Національний університет
«Одеська Юридична Академія»

Факультет прокуратури та слідства
(кримінальної юстиції)

Кафедра криміналістики, судових експертиз
та поліграфології

Національний центр судових експертиз
при Міністерстві юстиції
Республіки Молдова

Міжнародна громадська організація
«Конгрес Криміналістів»

Одеський науково-дослідний
Інститут судових експертиз
Міністерства юстиції України

ЗБІРНИК МАТЕРІАЛІВ

МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КРИМІНАЛІСТИКА МАЙБУТНЬОГО: ЦИФРОВІ ІННОВАЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, ГЛОБАЛЬНІ ВИКЛИКИ ТА ЗАГРОЗИ»

м. Одеса

05 червня 2026 року

КРИМІНАЛІСТИКА МАЙБУТНЬОГО: ЦИФРОВІ ІННОВАЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, ГЛОБАЛЬНІ ВИКЛИКИ ТА ЗАГРОЗИ

Матеріали Міжнародної науково-практичної конференції

5 червня 2026 р.

Одеса
2026

CRIMINALISTICS OF THE FUTURE: DIGITAL INNOVATIONS, ARTIFICIAL INTELLIGENCE, GLOBAL CHALLENGES AND THREATS

Proceedings of the International Scientific and Practical Conference

5 June 2026

Odesa
2026

УДК 343.98:004.8(062)

К823

Рекомендовано до друку рішенням кафедри криміналістики, судових експертиз та поліграфології НУ»ОЮА» (протокол № 20 від 12 червня 2026 року)
Рекомендовано до друку рішенням Вченої ради ОНДІСЕ (протокол №4 від 22 червня 2026 року)

Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози: збірник матеріалів міжнар. наук.–практ. конф. (м. Одеса, 5 черв. 2026 р.) / [орг. комітет: С. Ківалов, М. Аракелян, , О. Катарага, Д. Кішко, В. Шепітько, Д. Колодін, А. Колодіна Л. Аркуша, та ін.]; Нац. ун–т «Одеська юридична академія», кафедра криміналістики, судових експертиз та поліграфології; Національний центр судових експертиз при Міністерстві юстиції Республіки Молдова; Одеський науково–дослідний інститут судових експертиз Міністерства юстиції України, Міжнародна громадська організація «Конгрес криміналістів». Одеса: НУ «ОЮА», 2026. 564 с.

У збірнику викладено матеріали Міжнародної науково–практичної конференції «Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози», проведеної 5 червня 2026 року Національним університетом «Одеська юридична академія» за участю українських та іноземних науковців, судових експертів, представників правоохоронних органів, практиків, приватних експертів і здобувачів наукових ступенів. Матеріали присвячено криміналістичним інноваціям, цифровим технологіям, штучному інтелекту, розслідуванню злочинів у кіберпросторі, кримінально–правовим і кримінологічним викликам цифровізації, а також кримінально–процесуальним, оперативно–розшуковим та криміналістичним аспектам документування злочинів у цифровий час.

Висловлюємо вдячність усім авторам за активну участь, якісний науковий матеріал та дотримання принципів академічної доброчесності.

Матеріали викладені в авторській редакції.

Відповідальність за зміст, наукову новизну, коректність цитування та достовірність фактичного матеріалу несуть автори.

© НУ «Одеська юридична академія», 2026
© Автори статей, 2026

UDC 343.98:004.8(062)

К823

Recommended for publication by the decision of the Department of Criminalistics, Forensic Examinations and Polygraphology NU «OLA» (Pr. 20, June, 12, 2026)
Recommended for publication by the decision of the Academic Council of ONDISE (Pr. 4, June, 22, 2026)

Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats: Proceedings of the International Scientific and Practical Conference (Odesa, 5 June 2026) / [Organizing Committee: S. Kivalov, M. Arakelyan, O. Cataraga, D. Kishko, V. Shepitko, A. Kolodina, D. Kolodin, L. Arkusha, et al.]; National University «Odesa Law Academy», Department of Criminalistics, Forensic Examinations and Polygraphology; National Centre of Judicial Expertise of the Ministry of Justice of the Republic of Moldova; Odesa Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine; International Public Organization «Congress of Criminalists». Odesa: NU «OLA», 2026. 564 p.

The Proceedings contain papers presented at the International Scientific and Practical Conference «Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats», held on 5 June 2026 by the National University «Odesa Law Academy». The conference brought together Ukrainian and foreign scholars, forensic experts, representatives of law enforcement agencies, practitioners, private experts and postgraduate researchers. The materials cover criminalistics innovations, digital technologies, artificial intelligence, expert support for justice, investigation of crimes in cyberspace, criminal law and criminological challenges of digitalization, as well as criminal procedure, operational–search and criminalistics aspects of documenting crimes in the digital age.

We express our sincere gratitude to all authors for their active participation, high–quality academic contributions and adherence to academic integrity.

The materials are published in the authors' original versions.

Authors bear responsibility for the content, scientific novelty, accuracy of citations and reliability of factual information.

© National University «Odesa Law Academy», 2026
© Authors of articles, 2026

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ ПРОКУРАТУРИ ТА СЛІДСТВА
(КРИМІНАЛЬНОЇ ЮСТИЦІЇ)
КАФЕДРА КРИМІНАЛІСТИКИ, СУДОВИХ ЕКСПЕРТИЗ
ТА ПОЛІГРАФОЛОГІЇ
(м. Одеса, Україна)

NATIONAL UNIVERSITY «ODESA LAW ACADEMY»
FACULTY OF PROSECUTION AND INVESTIGATION
(CRIMINAL JUSTICE)
DEPARTMENT OF CRIMINALISTICS, FORENSIC EXAMINATIONS AND POLYGRAPHOLOGY
(Odesa, Ukraine)

НАЦІОНАЛЬНИЙ ЦЕНТР СУДОВИХ ЕКСПЕРТИЗ
ПРИ МІНІСТЕРСТВІ ЮСТИЦІЇ
РЕСПУБЛІКИ МОЛДОВА
(м. Кишинів, Республіка Молдова)
NATIONAL CENTRE OF JUDICIAL EXPERTISE
MINISTRY OF JUSTICE OF THE REPUBLIC OF MOLDOVA
(Chișinău, Republic of Moldova)

ОДЕСЬКИЙ НАУКОВО–ДОСЛІДНИЙ
ІНСТИТУТ СУДОВИХ ЕКСПЕРТИЗ
МІНІСТЕРСТВА ЮСТИЦІЇ УКРАЇНИ
(м. Одеса, Україна)
ODESA SCIENTIFIC RESEARCH INSTITUTE
OF FORENSIC EXAMINATIONS
MINISTRY OF JUSTICE OF UKRAINE
(Odesa, Ukraine)

МІЖНАРОДНА ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«КОНГРЕС КРИМІНАЛІСТІВ»
(Україна)
INTERNATIONAL PUBLIC ORGANIZATION
«CONGRESS OF CRIMINALISTS»
(Ukraine)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ:

ГОЛОВА ОРГКОМІТЕТУ:

Сергій КІВАЛОВ – Президент Національного університету «Одеська юридична академія», д.ю.н., академік;

ЗАСТУПНИКИ ГОЛОВИ ОРГКОМІТЕТУ:

Мінас АРАКЕЛЯН – проректор з наукової роботи Національного університету «Одеська юридична академія», д.ю.н., професор;

Денис КОЛОДІН – декан факультету прокуратури та слідства (кримінальної юстиції) Національного університету «Одеська юридична академія», д.ю.н., професор;

Лариса АРКУША – завідувач кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», д.ю.н., професор.

СПІВОРГАНІЗАТОРИ:

Ольга КАТАРАГА – директор Національного Центру судових експертиз Міністерства юстиції Республіки Молдова, судовий експерт вищої категорії, д.ю.н.;

Пьотр ПЄТКОВИЧ – заступник директора Національного Центру судових експертиз Міністерства юстиції Республіки Молдова, судовий експерт вищої категорії;

Дмитро КІШКО – директор Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України;

Антоніна ЧЕРЕМНОВА – вчений секретар Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України, к.ю.н., доцент;

Валерій ШЕПІТЬКО – президент Міжнародної громадської організації «Конгрес криміналістів», д.ю.н., професор.

ЧЛЕНИ ОРГКОМІТЕТУ:

Дар'я МІНЧЕНКО – начальник відділу міжнародних зв'язків Національного університету «Одеська юридична академія», к.ю.н., доцент;

Таїсія ІВАНІЙЧУК – директор наукової бібліотеки Національного університету «Одеська юридична академія», к.біол.н.;

Сергій СТАРОДУБОВ – декан факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія», к.ю.н., доцент;

Богдан ФАСІЙ – декан факультету судового та міжнародного права Національного університету «Одеська юридична академія», к.ю.н., доцент

Євген ХИЖНЯК – декан факультету цивільної та господарської юстиції Національного університету «Одеська юридична академія», к.ю.н., доцент

Віктор ЦИТРЯК – заступник декана факультету прокуратури та слідства (кримінальної юстиції) Національного університету «Одеська юридична академія», к.ю.н., доцент;

Юлія ГРЕСЬ – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», к.ю.н., доцент;

Анна КОЛОДІНА – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», к.ю.н., доцент;

Олександр ЧЕРНОВ – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», доктор філософії з галузі знань 08 «Право».

ГОЛОВА РОБОЧОЇ ГРУПИ:

Анна КОЛОДІНА – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», к.ю.н., доцент;

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Вікторія ГРИНЕВИЧ – в.о. директора Центру поліграфологічних досліджень та тестування, асистент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»;

Ірина ПИШНЕНКО – провідний фахівець відділу ліцензування, акредитації та забезпечення якості освіти, асистент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»;

Олександра СТАУРСЬКА – завідувач підготовчим відділенням, доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», доктор філософії з галузі знань 08 «Право».

ВІДПОВІДАЛЬНІ ЗА ВИПУСК / УКЛАДАЧІ:

Лариса АРКУША – завідувач кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», д.ю.н., професор;

Антоніна ЧЕРЕМНОВА – вчений секретар Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України, к.ю.н., доцент;

Пьотр ПІЄТКОВИЧ – заступник директора Національного Центру судових експертиз Міністерства юстиції Республіки Молдова, судовий експерт вищої категорії;

Валерій ШЕПІТЬКО – президент Міжнародної громадської організації «Конгрес криміналістів», д.ю.н., професор;

Юлія ГРЕСЬ – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», к.ю.н., доцент;

Анна КОЛОДІНА – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», к.ю.н., доцент;

Олександра СТАУРСЬКА – завідувач підготовчим відділенням, доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», доктор філософії з галузі знань 08 «Право».

Олександр ЧЕРНОВ – доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», доктор філософії з галузі знань 08 «Право».

ORGANIZING COMMITTEE OF THE CONFERENCE:

HEAD OF THE ORGANIZING COMMITTEE:

Sergiy KIVALOV – President of the National University «Odesa Law Academy», Doctor of Laws, Academician;

DEPUTY HEADS OF THE ORGANIZING COMMITTEE:

Minas ARAKELYAN – Vice–Rector for Scientific Work of the National University «Odesa Law Academy», Doctor of Laws, Professor;

Denys KOLODIN – Dean of the Faculty of Prosecution and Investigation (Criminal Justice) of the National University «Odesa Law Academy», Doctor of Laws, Professor;

Larisa ARKUSHA – Head of the Department of Forensics, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Doctor of Laws, Professor.

CO-ORGANIZERS:

Olga KATARAGA – Director of the National Center for Forensic Examinations of the Ministry of Justice of the Republic of Moldova, Judicial Expert of the Highest Category, Doctor of Laws;

Pyotr PETKOVYCH – Deputy Director of the National Center for Forensic Expertise of the Ministry of Justice of the Republic of Moldova, highest category forensic expert;

Dmytro KISHKO – Director of the Odesa Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine;

Antonina CHEREMNOVA – Scientific Secretary of the Odesa Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine, Candidate of Laws, Associate Professor;

Valerii SHEPITKO – President of the International Public Organization «Criminalists Congress», Doctor of Laws, Professor.

MEMBERS OF THE ORGANIZING COMMITTEE:

Darya MINCHENKO – Head of the International Relations Department of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Taisia IVANIYCHUK – Director of the Scientific Library of the National University «Odesa Law Academy», Candidate of Biology;

Serhiy STARODUBOV – Dean of the Faculty of Advocacy and Anti–Corruption Activities of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Bohdan FASIY – Dean of the Faculty of Judicial and International Law of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Yevhen KHYZHNYAK – Dean of the Faculty of Civil and Economic Justice of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Viktor TSYTRYAK – Deputy Dean of the Faculty of Prosecution and Investigation (Criminal Justice) of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Yulia HRES – Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Anna KOLODINA – Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Oleksandr CHERNOV – Associate Professor of the Department of Forensic, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Doctor of Philosophy in the field of knowledge 08 «Law».

HEAD OF THE WORKING GROUP:

Anna KOLODINA – Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

MEMBERS OF THE WORKING GROUP:

Viktoria HRYNEVYCH – Acting Director of the Center for Polygraph Research and Testing, Assistant Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy»;

Iryna PYSHNENKO – Leading Specialist of the Department of Licensing, Accreditation and Quality Assurance of Education, Assistant Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy»;

Oleksandra STAURSKA – Head of the Preparatory Department, Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Doctor of Philosophy in the field of knowledge 08 «Law».

RESPONSIBLE FOR THE PUBLICATION / COMPILERS:

Larysa ARKUSHA – Head of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Doctor of Law, Professor;

Antonina CHEREMNOVA – Scientific Secretary of the Odesa Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine, Candidate of Laws, Associate Professor;

Pyotr PETKOVYCH – Deputy Director of the National Center for Forensic Expertise of the Ministry of Justice of the Republic of Moldova, highest category forensic expert;

Valerii SHEPITKO – President of the International Public Organization «Criminalists Congress», Doctor of Laws, Professor.

Yulia HRES – Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Anna KOLODINA – Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Candidate of Laws, Associate Professor;

Oleksandra STAURSKA – Head of the Preparatory Department, Associate Professor of the Department of Forensic Science, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Doctor of Philosophy in the field of knowledge 08 «Law»;

Oleksandr CHERNOV – Associate Professor of the Department of Forensic, Forensic Examinations and Polygraphology of the National University «Odesa Law Academy», Doctor of Philosophy in the field of knowledge 08 «Law».

ЗМІСТ

Вступне слово С. Ківалова ……..…….36
Cuvânt de deschidere O. Cataraga ……...……40
Вступне слово Д. Кішка ……..…….44
Вступне слово В. Шепітька……..48

СЕКЦІЯ 1.
КРИМІНАЛІСТИЧНІ ІННОВАЦІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СТРАТЕГІЇ ПОДОЛАННЯ ГЛОБАЛЬНИХ ЗЛОЧИННИХ ЗАГРОЗ

ALIYEV Bakhtiyar Abdurahman ogly……..52
HISTORY AND DEVELOPMENT OF MODERN FORENSIC SCIENCE (CRIMINALISTICS) IN THE REPUBLIC OF AZERBAIJAN

CATARAGA Olga……...60
VIITORUL EXPERTIZEI JUDICIARE ÎN REPUBLICA MOLDOVA ŞI ÎN SPAȚIUL EUROPEAN

АРКУША Лариса……...64
ТЕОРЕТИКО–МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РОЗСЛІДУВАННЯ ДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ

БАСАЛЮК Наталія……..70
ЦИФРОВІ ТА СУДОВО–ЕКСПЕРТНІ ДОКАЗИ У ПРОЦЕДУРІ ЕКСТРАДИЦІЇ ОСІБ: ОКРЕМІ АСПЕКТИ

ВАРИНСЬКИЙ Владислав……..…74
ПРИНЦИП HUMAN OVERSIGHT У КРИМІНАЛЬНІЙ ЮСТИЦІЇ: АДАПТАЦІЯ СТАНДАРТІВ EU AI ACT В УКРАЇНІ

ГРЕСЬ Юлія……...79
ОСНОВИ ВИКОРИСТАННЯ МЕТОДОЛОГІЇ ПОВЕДІНКОВОГО ПРОФАЙЛІНГУ ТА ЦИФРОВОЇ АНАЛІТИКИ ПІД ЧАС РОЗСЛІДУВАННЯ КОРИСЛИВИХ ЗЛОЧИНІВ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

ЗАГОРОДНІЙ Андрій……...…84
ВЗАЄМОДІЯ СУБ'ЄКТІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА ВИКОРИСТАННЯ АНАЛІТИЧНОЇ ПІДТРИМКИ ШТУЧНОГО ІНТЕЛЕКТУ НА СТАДІЇ ДОСУДОВОГО РОЗСЛІДУВАННЯ

КАРАМАН Микола……...89
ОКРЕМІ ПИТАННЯ ОСОБЛИВОСТЕЙ ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОСУДДЯ ЩОДО ЗЛОЧИНІВ АГРЕСІЇ ТА ВОЄННИХ ЗЛОЧИНІВ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ

МИРОШНИЧЕНКО Юрій……...93
ЦИФРОВА ВІЗУАЛІЗАЦІЯ ЯК ЗАСІБ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ СУДОВОГО ПРОВАДЖЕННЯ

НЕДАШКІВСЬКА Ольга, ГУНЬКО Олександр……97
ЦИФРОВІЗАЦІЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ: ТРАНСФОРМАЦІЯ ДОКАЗУВАННЯ, НОВІ ТЕХНОЛОГІЧНІ МОЖЛИВОСТІ ТА ВИКЛИКИ ПРАВОСУДДЯ

ОСТАПЕНКО Артур……..102
ТЕХНІКО–КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

ПЛАТОВСЬКИЙ Сергій……106
ДОСЛІДЖЕННЯ КОЛЕКЦІЙНИХ ТА ІСТОРИЧНИХ АВТОМОБІЛІВ В ПРАКТИЦІ ОХОРОНИ КУЛЬТУРНОЇ СПАДЩИНИ РЕСПУБЛІКИ ПОЛЬША

САВЧУК Олена……110
ПОЧЕРКОЗНАВСТВО В ЦИФРОВУ ЕПОХУ: ВІД КЛАСИЧНИХ ОЗНАК ДО НОВИХ МОДЕЛЕЙ ІДЕНТИФІКАЦІЇ

САЛТИКОВ Олександр……..…114
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ: МОЖЛИВОСТІ ТА РИЗИКИ

СИДОРЧУК Інна…….117
РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ СУДОВОЇ ЕКСПЕРТИЗИ

СМИРНОВ Максим……...120
МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У РОЗСЛІДУВАННІ ЗЛОЧИНІВ В ДАРКНЕТ (DARKNET)

ТУЛЯКОВ Вячеслав……...124
ЄВРОПЕЙСЬКЕ ЗАКОНОДАВСТВО З ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ: НОВІ ВИКЛИКИ ДЛЯ УКРАЇНИ

УСЕНКО Олена……...128
ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ ЗАРУБІЖНИХ КРАЇН

ЧОРНОУС Юлія……..132
АКТУАЛЬНІ ПИТАННЯ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

ШЕВЧУК Віктор……..136
КРИМІНАЛІСТИКА МАЙБУТНЬОГО В ЕПОХУ ЦИФРОВІЗАЦІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ: ГЛОБАЛЬНІ ВИКЛИКИ Й ПЕРСПЕКТИВИ РОЗВИТКУ

ШЕПІТЬКО Валерій, ШЕПІТЬКО Михайло……142
ПРОБЛЕМИ ФОРМУВАННЯ ТА МІСЦЕ КРИМІНАЛІСТИЧНОЇ ІНЖЕНЕРІЇ В СТРУКТУРІ КРИМІНАЛІСТИКИ

СЕКЦІЯ 2.
ЦИФРОВІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОСУДДЯ

АФАНАСЕНКО Світлана……..148
ЦИФРОВІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОСУДДЯ

БАТІГ Андрій……..151
ЦИФРОВІ ТЕХНОЛОГІЇ PYTHON У СУДОВІЙ ЗАЛІЗНИЧНО–ТРАНСПОРТНІЙ ЕКСПЕРТИЗІ

БАЧИЛО Тетяна……..154
ПРОБЛЕМА ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

БІЛІНСЬКИЙ Маркіян……..158
ВИКОРИСТАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕХНІКО–КРИМІНАЛІСТИЧНОМУ ДОСЛІДЖЕННІ ДОКУМЕНТІВ

ВОЗОВИК Юрій……...161
ОСОБЛИВОСТІ ЦИФРОВОЇ ФІКСАЦІЇ СЛІДІВ ТЕРМІЧНОГО ВПЛИВУ В СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

VOZIAN Viorica……164
METODE DE CERCETARE ȘI ANALIZĂ A LIMBAJULUI INVECTIV ÎN CADRUL EXPERTIZEI JUDICIARE DE AUTOR

ГАЛАЙКО Марина……171
ІНТЕГРАЦІЯ ЦИФРОВИХ ІННОВАЦІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ В БУДІВЕЛЬНО–ТЕХНІЧНУ ЕКСПЕРТИЗУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

ГОЛОВАЧ Ростислав, ШЕРЕМЕТОВ Сергій……176
ЦИФРОВІ НОСІЇ ІНФОРМАЦІЇ ЯК ОБ'ЄКТИ СУДОВОЇ ВІЙСЬКОВОЇ ЕКСПЕРТИЗИ: ПРОБЛЕМИ МЕТОДОЛОГІЇ ТА НОРМАТИВНОГО РЕГУЛЮВАННЯ

GRECU Polixenia……180
CORELAREA DATELOR MEDICO–LEGALE ȘI A REZULTATELOR EXPERTIZEI BALISTICE ÎN RECONSTITUIREA MECANISMULUI MORȚILOR PRIN ÎMPUȘCARE

КРИВОНОЖКО Галина, СОБІН Олексій……..184
ШТУЧНИЙ ІНТЕЛЕКТ І СПЕЦІАЛІЗОВАНІ ЦИФРОВІ ІНСТРУМЕНТИ В ЕКСПЕРТНОМУ ЗАБЕЗПЕЧЕННІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ТА ЦИФРОВИХ ПРАВОПОРУШЕНЬ

ЛЯХОВЕЦЬКИЙ Сергій……...189
ІНСЦЕНУВАННЯ САМОГУБСТВА ЧЕРЕЗ ПОВІШАННЯ ДЛЯ ПРИХОВУВАННЯ УМИСНОГО ВБИВСТВА ТА МОЖЛИВОСТІ АНАЛІТИЧНОЇ ПІДТРИМКИ ШТУЧНОГО ІНТЕЛЕКТУ

PĂTRU Alina Daniela……...193
ABORDĂRI MODERNE PRIVIND UTILIZAREA ȘI VALORIFICAREA URMELOR CRIMINALISTICE ÎN IDENTIFICAREA AUTORILOR INFRACȚIUNILOR VIOLENTE

РИБАЛКО Андрій, КОВКІНА Євгенія……197
ІМПЛІЦИТНІ ТА ГІБРИДНІ СПОНУКАЛЬНІ ВИСЛОВЛЮВАННЯ У ЦИФРОВІЙ КОМУНІКАЦІЇ ЯК ОБ'ЄКТ СУДОВОЇ ПСИХОЛОГО–ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ

СТОЛЯРОВА Ірина, ПАГУРЕЦЬ Ольга, МАКАРОВА Олександра……203
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ДЛЯ РОЗШИФРУВАННЯ СПЕКТРІВ У СУДОВІЙ ЕКСПЕРТИЗІ МАТЕРІАЛІВ, РЕЧОВИН ТА ВИРОБІВ

ТКАЧЕНКО Наталія……..208
ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА РОЗВИТОК СУДОВО–ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ

ЦЕЛУЙКО Михайло, УСЕНКО Олена……..…212
ПЕРСПЕКТИВНІ НАПРЯМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ СУДОВОЇ ЕКСПЕРТИЗИ В УКРАЇНІ

ЦІЛЬМАК Олена…….216
КОГНІТИВНІ ВИКРИВЛЕННЯ У МЕХАНІЗМІ ФОРМУВАННЯ ЦИФРОВИХ СЛІДІВ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ

ШАНИГІН Антон, ВОЛОШИНА Владлена, АЛЬ–ФАЙЮМИ Халед……..221
ЦИФРОВІ ТЕХНОЛОГІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я: ВИКЛИКИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ МЕДИЧНИХ ДАНИХ

СЕКЦІЯ 3.
ЕКСПЕРТНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У КІБЕРПРОСТОРІ ТА ВИКОРИСТАННЯ ВІРТУАЛЬНИХ АКТИВІВ

ВЕЛИЧКО Юлія……..……225
ПЕРСПЕКТИВИ ПРОВЕДЕННЯ СУДОВИХ ЕКОНОМІЧНИХ ЕКСПЕРТИЗ ТА ДОСЛІДЖЕНЬ З ПИТАНЬ ДЕКЛАРУВАННЯ ТА ОПОДАТКУВАННЯ ДОХОДІВ ФІЗИЧНИХ ОСІБ, ОТРИМАНИХ ВІД ВІРТУАЛЬНИХ АКТИВІВ

ВОЗНЯК Олег……...230
ОСОБЛИВОСТІ ПРОВЕДЕННЯ КОМПЛЕКСНИХ ЕКСПЕРТИЗ ЗТП НА ПЕРЕЇЗДАХ: НОРМАТИВНО–ТЕХНІЧНИЙ ПОГЛЯД ЕКСПЕРТА–ЗАЛІЗНИЧНИКА

ГОЛОВА Інна, МЕНЗУЛ Оксана…….236
ВИЗНАЧЕННЯ ВАРТОСТІ ПОСЛУГ У СУДОВІЙ ЕКСПЕРТИЗІ

ДЕРЕЧА Андрій, АБРОСІМОВ Тарас……..…240
СУЧАСНІ ПРОБЛЕМИ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У СУДОВОМУ ДОСЛІДЖЕННІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

ДИКИЙ Олег……..…245
КІБЕРКРИМІНАЛІСТИКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ФАХОВОЇ ПІДГОТОВКИ СУЧАСНОГО ФАХІВЦЯ З БЕЗПЕКИ

ЄВСЮКОВ Олександр……...249
ЦИФРОВІ ОБ'ЄКТИ В СУДОВО–ЕКСПЕРТНИХ ДОСЛІДЖЕННЯХ

KIOSE Michael……..253
PROSPECTS OF USING ARTIFICIAL INTELLIGENCE IN RESEARCHING TITANIUM, ALUMINUM AND MAGNESIUM ALLOY POWDER AS DUAL–USE GOODS

ЛУЩИК Ігор, ТЯПКІН Анатолій……..…258
ШЛЯХИ ВЗАЄМОДІЇ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ І СУДОВОЇ ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ

МІНЯЙЛО Анатолій, ДМИТРЕНКО Людмила, МІНЯЙЛО Надія……..263
ІНЖЕНЕРНО–ЕКОЛОГІЧНА ЕКСЕРТИЗА – ВАЖЛИВА ЛАНКА ПРОТИДІЇ ЕКОЛОГІЧНИМ ПРАВОПОРУШЕННЯМ

ПІРОГ Олександр……268
ОСОБЛИВОСТІ ВИЛУЧЕННЯ ВОЛАТИЛЬНИХ ДАНИХ З ІОТ–ПРИСТРОЇВ

РАДЕЦЬКИЙ Сергій……..273
ОСОБЛИВОСТІ ОГЛЯДУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ, РОЗМІЩЕНИХ У ВІДКРИТОМУ ДОСТУПІ

СТАУРСЬКА Олександра……..278
АВТОМАТИЗАЦІЯ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ У КРИМІНАЛІСТИЦІ: ВІД КЛАСИЧНИХ МЕТОДИК ДО ІНТЕЛЕКТУАЛЬНИХ АЛГОРИТМІВ

ХАМУЛА Дмитро……283
ДО ПИТАННЯ АТРИБУЦІЇ КАХЕЛЬНОЇ КАМІНО–ПЕЧІ З ГРИФОНАМИ В БУДИНКУ М. ПІДГОРСЬКОГО В КИЄВІ

ЧАБАНЕЦЬ Тетяна, МАКАРЕЦЬ Альбіна……287
НАТУРНЕ ДОСЛІДЖЕННЯ У СУДОВО–ТОВАРОЗНАВЧІЙ ЕКСПЕРТИЗІ ЯК ОСНОВА ІДЕНТИФІКАЦІЇ, ДЕФЕКТОСКОПІЇ ТА ПАРАМЕТРИЧНОГО ПІДБОРУ АНАЛОГІВ

ЧЕРЕМНОВА Антоніна……..……293
СУДОВА ЕКСПЕРТИЗА В СИСТЕМІ ДОКАЗУВАННЯ: РОЛЬ, ФУНКЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

ЧЕРНОВ Олександр……298
ОСОБЛИВОСТІ ПРОВЕДЕННЯ ПОЧЕРКОЗНАВЧОЇ ЕКСПЕРТИЗИ ПІДПИСІВ У ЦИФРОВИХ КОПІЯХ ДОКУМЕНТІВ

ЮСУПОВ Володимир, КИСІЛЬ Наталія……303
ІНТЕГРАЦІЯ МЕТОДІВ КРИМІНАЛІСТИКИ У ПРАКТИКУ ПРОВЕДЕННЯ СУДОВИХ ЕКСПЕРТИЗ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

СЕКЦІЯ 4.
КРИМІНАЛЬНО–ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ВИКЛИКИ ЦИФРОВІЗАЦІЇ: ВІД КІБЕРТЕРОРИЗМУ ДО АВТОНОМНИХ СИСТЕМ ОЗБРОЄННЯ

АРТЮХ Надія, КОЗАЧЕНКО Віталій……308
КІБЕРБУЛІНГ У СИСТЕМІ ДЕТЕРМІНАНТ ДЕВІАНТНОЇ ПОВЕДІНКИ МОЛОДІ

БЕРШАВСЬКА Анастасія……313
ОРГАНІЗАЦІЙНО–ТАКТИЧНІ ОСОБЛИВОСТІ ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ ІЗ ПОСОБНИЦТВОМ ДЕРЖАВІ–АГРЕСОРУ

ГОРБАЧОВА Ірина……316
ІНФОРМАЦІЙНІ ВКИДИ ТА ЦИФРОВА ДЕЗІНФОРМАЦІЯ ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ

ЄРОФЕЄВА Ольга……...321
МОТИВИ ЗЛОЧИННОГО ПОСЯГАННЯ У КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЯХ, ПОВ'ЯЗАНИХ ІЗ ЗАВОЛОДІННЯМ СПАДКОВИМ МАЙНОМ

КЛИМЕНКО Дар'я, КОЗАЧЕНКО Віталій……324
ЦИФРОВІ ФОРМИ НАСИЛЬСТВА ЩОДО ОСІБ ПОХИЛОГО ВІКУ: КРИМІНОЛОГІЧНІ АСПЕКТИ

КОЗАЧЕНКО Віталій……329
ПРОБЛЕМА ВЕРБАЛЬНОЇ АГРЕСІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ: КРИМІНОЛОГІЧНИЙ АНАЛІЗ

КУБАЄНКО Андрій……334
ЕФЕКТИВНІСТЬ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНИХ ЗАГРОЗ

ЛУКАЩУК Каріна……338
ЦИФРОВІЗАЦІЯ ВИКОНАННЯ ПОКАРАНЬ, НЕ ПОВ'ЯЗАНИХ ІЗ ПОЗБАВЛЕННЯМ ВОЛІ: МІЖНАРОДНИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

ЛУЦЮК Павло……342
ПРОБЛЕМИ ВИЗНАЧЕННЯ ВЧИНЕННЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ ВПЕРШЕ У КРИМІНАЛЬНОМУ ПРАВІ ТА СУДОВІЙ ПРАКТИЦІ

СИДОРЧУК Владислав, СИДОРЧУК Інна……348
КІБЕРТЕРОРИЗМ: ПОНЯТТЯ, ОЗНАКИ ТА НАПРЯМКИ ПРОТИДІЇ

СТЕПАНЕНКО Оксана……353
КІБЕРНАСИЛЬСТВО ЯК САМОСТІЙНА ФОРМА ДОМАШНЬОГО НАСИЛЬСТВА

ТІТУНІНА Катерина……..358
ПРОТИДІЯ РАДИКАЛІЗАЦІЇ ТА ГІБРИДНИМ ЗАГРОЗАМ В УСТАНОВАХ ВИКОНАННЯ ПОКАРАНЬ В УМОВАХ ВОЄННОГО СТАНУ

ЦЕХАН Дмитро……362
ІДЕОЛОГІЯ ФОРМУВАННЯ ТА ФУНКЦІОНУВАННЯ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

ЦИТРЯК Віктор……..…367
ЕФЕКТИВНІСТЬ ОПЕРАТИВНО–РОЗШУКОВОЇ ДІЯЛЬНОСТІ ЯК ЗАСОБУ ЗАБЕЗПЕЧЕННЯ ПРАВОПОРЯДКУ В ПЕНІТЕНЦІАРНИХ УСТАНОВАХ

СЕКЦІЯ 5.
КРИМІНАЛЬНО–ПРОЦЕСУАЛЬНІ, ОПЕРАТИВНО–РОЗШУКОВІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ У ЦИФРОВИЙ ЧАС

АЛБУЛ Сергій…….……..…372
КРИМІНАЛЬНА РОЗВІДКА ЯК СИСТЕМНИЙ ЕЛЕМЕНТ КОМПЛЕКСНОЇ МОДЕЛІ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ

ВАЩУК Олеся…….…377
ПРОБЛЕМИ ДОСТОВІРНОСТІ ФОТО– ТА ВІДЕОДОКАЗІВ ВОЄННИХ ЗЛОЧИНІВ В УМОВАХ РОЗВИТКУ DEEPFAKE–ТЕХНОЛОГІЙ

ВОЛОС Владислав……..381
ОСОБЛИВОСТІ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

ВОЛОШИНА Владлена……..…384
ПРОЦЕСУАЛЬНИЙ ПОРЯДОК ОТРИМАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОБЛЕМИ ПРАВОЗАСТОСУВАННЯ

ГОНЧАРУК Владислава……387
СОЦІАЛЬНІ МЕРЕЖІ ЯК ДЖЕРЕЛО КРИМІНАЛІСТИЧНИХ СЛІДІВ: ІННОВАЦІЙНІ МЕТОДИ РОЗСЛІДУВАННЯ ТРАФІКІНГУ

ГРЕБЕНЮК Сергій, КУШНІРЕНКО Наталія……...391
СУДОВО–ДАКТИЛОСКОПІЧНА ІДЕНТИФІКАЦІЯ НЕВПІЗНАНИХ ТРУПІВ ТА ЇХ ОСТАНКІВ ЗА ЦИФРОВИМИ ЗОБРАЖЕННЯМИ ВІДБИТКІВ ПАЛЬЦІВ РУК ІЗ БІОМЕТРИЧНИХ ДОКУМЕНТІВ

ГРИНЕВИЧ Вікторія……..…397
МІЖ ЕФЕКТИВНІСТЮ ТА ВЕРХОВЕНСТВОМ ПРАВА: ПРАВОВІ Й ЕТИЧНІ МЕЖІ ЗАСТОСУВАННЯ НЕТРАДИЦІЙНИХ МЕТОДІВ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

ДРИГА Єлизавета……401
ВЗАЄМОДІЯ СЛІДЧИХ ТА ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ПІД ЧАС ПРОВЕДЕННЯ ТАКТИЧНИХ ОПЕРАЦІЙ ПРИ РОЗСЛІДУВАННІ НЕЗАКОННОГО ОБІГУ ЗБРОЇ ТА БОЄПРИПАСІВ В УМОВАХ ВОЄННОГО СТАНУ

ЗАВТУР Віктор……406
ЦИФРОВИЙ ОБШУК У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ОКРЕМІ ПИТАННЯ НОРМАТИВНОЇ МОДЕЛІ

ЗАГОРОДНІЙ Ігор……..412
АЛГОРИТМІЗАЦІЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ З МОЖЛИВОСТЯМИ ВИКОРИСТАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ОСНОВА ЕФЕКТИВНОГО РОЗКРИТТЯ ТЯЖКИХ ТА ОСОБЛИВО ТЯЖКИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

ЗАГОРОДНІЙ Віктор……..…419
МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ПРОКУРОРА ЯК ПРОЦЕСУАЛЬНОГО КЕРІВНИКА НА ЗАВЕРШАЛЬНОМУ ЕТАПІ ДОСУДОВОГО РОЗСЛІДУВАННЯ

ЗГОДА Юлія……..……423
ОБСТАНОВКА ВЧИНЕННЯ КОРИСЛИВИХ ЗЛОЧИНІВ В УМОВАХ ВОЄННОГО АБО НАДЗВИЧАЙНОГО СТАНУ

КІЛІМІЧЕНКО Сергій……...428
ОБСТАВИНИ, ЯКІ ПІДЛЯГАЮТЬ ВСТАНОВЛЕННЮ ПІД ЧАС ВИЯВЛЕННЯ ОЗНАК ПРОТИДІЇ РОЗСЛІДУВАННЮ

КІЛІМІЧЕНКО Христина……434
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТАКТИЧНИХ ОПЕРАЦІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ВЧИНЕНИХ ЖІНКАМИ

КОВИРШИН Віктор……...439
СПЕЦИФІКА ЗАТРИМАННЯ АДВОКАТА У КРИМІНАЛЬНОМУ ПРОЦЕСІ

КОЛОДІН Денис, КОЛОДІНА Анна……442
ДО ПИТАННЯ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ НА СИСТЕМУ ЗАСОБІВ КРИМІНАЛІСТИЧНОЇ ТАКТИКИ

КУЗНЕЦОВА Людмила…….……446
ЩОДО ДОЦІЛЬНОСТІ ЗГАДКИ ЕКОНОМІЧНОГО ДОБРОБУТУ У ВИПАДКАХ ВИНЕСЕННЯ РІШЕННЯ ПРО СКЛАДАННЯ ДОСУДОВОЇ ДОПОВІДІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

КРИВДА Людмила……450
ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У РОЗСЛІДУВАННІ НАСИЛЬНИЦЬКИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

МАКСИМЧУК Іван……453
ВПЛИВ ПРЕДМЕТА КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ НА ФОРМУВАННЯ СТАТИСТИЧНИХ ПОКАЗНИКІВ ЗА ОКРЕМИМИ ВИДАМИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

МУНТЯНУ Юліан……458
АНАЛІЗ ВІДКРИТИХ ДЖЕРЕЛ У ДІЯЛЬНОСТІ З РОЗСЛІДУВАННЯ ЗАХОПЛЕННЯ ТА УМИСНОГО ВБИВСТВА ЗАРУЧНИКІВ

НЕЧИПОРУК Володимир……461
ДИСТАНЦІЙНІ ДОПИТИ УЧАСНИКІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ У ФОКУСІ ПРАВОВИХ ПОЗИЦІЙ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

ПАВЗЮК Анатолій……465
ПСИХОЛОГІЧНИЙ ПРОФІЛЬ ОСОБИ, ЯКА ВЧИНИЛА ПРОТИПРАВНЕ ДІЯННЯ: МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛІСТИЧНОМУ АНАЛІЗІ ПОВЕДІНКИ

ПАЛАМАРЧУК Олексій……470
ОБСТАНОВКА ВЧИНЕННЯ КВАРТИРНИХ КРАДІЖОК, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ УГРУПОВАННЯМИ

ПАТРЕЛЮК Дмитро……..475
ЩОДО ЗАСОБІВ КРИМІНАЛЬНОГО ПЕРЕСЛІДУВАННЯ

ПЕТРОСЯН Айк……..478
РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, УЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ ГРУПАМИ У СФЕРІ ІНВЕСТИЦІЙНОЇ ДІЯЛЬНОСТІ: ТЕОРЕТИКО–ПРАВОВІ ЗАСАДИ

ПИШНЕНКО Ірина……483
ІНСЦЕНУВАННЯ ЯК ЗАСІБ МАСКУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ: МЕТОДИ МОДЕЛЮВАННЯ ТА ВИЯВЛЕННЯ

ПОЖАР Вадим……..…488
ПРОБЛЕМАТИКА ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ПРАВ І ЗАКОННИХ ІНТЕРЕСІВ ПОТЕРПІЛОГО ПІД ЧАС ЗАСТОСУВАННЯ ДО ОСОБИ ТРИМАННЯ ПІД ВАРТОЮ

РУБЕЦЬ Катерина……..492
КРИМІНАЛЬНО–ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ ЗАСАДИ ВИКОРИСТАННЯ ПОЧЕРКОЗНАВЧОЇ ЕКСПЕРТИЗИ ПІД ЧАС ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

САМОЙЛЕНКО Олена……..496
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ЕЛЕМЕНТ СУЧАСНИХ КРИМІНАЛІСТИЧНИХ МЕТОДИК

СТАРОДУБОВ Олександр……499
ОСОБЛИВОСТІ ВИКОРИСТАННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС ПРОВЕДЕННЯ ТАКТИЧНИХ ОПЕРАЦІЙ З УРАХУВАННЯМ СУЧАСНИХ УМОВ

ТІЩЕНКО Валерій, БЄЛІК Лариса…….504
СЛІДЧА СИТУАЦІЯ ЯК ОСНОВА ТАКТИЧНИХ І СТРАТЕГІЧНИХ РІШЕНЬ У ДОСУДОВОМУ РОЗСЛІДУВАННІ

ТОРБАС Олександр……509
ДО ПОНЯТТЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

ФЕДОРОВ Владислав…….512
ОБСТАНОВКА ВЧИНЕННЯ РОЗБІЙНИХ НАПАДІВ ІЗ ЗАСТОСУВАННЯМ ВОГНЕПАЛЬНОЇ ЗБРОЇ У ВОЄННИЙ ТА ПОСТВОЄННИЙ ПЕРІОД

ФЕДОРЧУК Олександр…….516
КОРЕЛЯЦІЙНІ ЗАЛЕЖНОСТІ СТРУКТУРНИХ ЕЛЕМЕНТІВ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ПОСАДОВИХ ОСІБ ТА ВПЛИВ ЇХ ПІЗНАННЯ НА ПРОЦЕС РОЗСЛІДУВАННЯ

ХИЖНЯК Євген……..521
СУТНІСТЬ КООРДИНАЦІЇ ТА ВЗАЄМОДІЇ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ З РІЗНИМИ СУБ'ЄКТАМИ ПІД ЧАС ОПЕРАТИВНО–РОЗШУКОВОГО ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЗА ФАКТОМ ВЧИНЕННЯ УМИСНИХ ВБИВСТВ

ЧИГРИНА Галина……..526
КЛЮЧОВІ ФОРМИ КРИМІНАЛІСТИЧНОГО СУПРОВОДУ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: СВІТОВИЙ ДОСВІД ДЛЯ УКРАЇНИ

ЧІПКО Наталія……531
СУЧАСНЕ ШАХРАЙСТВО У СФЕРІ ПЛАТІЖНИХ СИСТЕМ

ЧЕРНИШ Юрій……536
ТИПОВІ СИТУАЦІЇ ПОДАЛЬШОГО ЕТАПУ РОЗСЛІДУВАННЯ КОНТРАБАНДИ КУЛЬТУРНИХ ЦІННОСТЕЙ

ЧУМАК Сергій……..…539
ЦИФРОВІЗАЦІЯ СУДОВОЇ ФОТОГРАФІЇ У ЗБИРАННІ ДОКАЗІВ

ШЕРЕМЕТОВ Сергій……543
КАДРОВЕ ЗАБЕЗПЕЧЕННЯ НДУСЕ ЯК СКЛАДОВА ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У ВІЙСЬКОВІЙ СФЕРІ

ШЕРШЕНЬКОВА Вікторія……555
ЗБІР ДОКАЗІВ СТОСОВНО ВІЙСЬКОВИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

ЯЦКЕВИЧ Руслан……...559
СКЛАДОВІ ПРОФЕСІЙНОЇ КОМПЕТЕНЦІЇ ПРАЦІВНИКІВ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ, ЯКІ ЗАБЕЗПЕЧУЮТЬ ПРОТИДІЮ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

CONTENT

Introductory speech by S. Kivalov……..…36
Introductory speech by O. Cataraga……..40
Introductory speech by D. Kishko……..44
Introductory speech by V. Shepitko……48

SECTION 1.
CRIMINALISTICS INNOVATIONS AND ARTIFICIAL INTELLIGENCE IN THE STRATEGY FOR OVERCOMING GLOBAL CRIMINAL THREATS

ALIYEV Bakhtiyar Abdurahman ogly……..52
HISTORY AND DEVELOPMENT OF MODERN FORENSIC SCIENCE (CRIMINALISTICS) IN THE REPUBLIC OF AZERBAIJAN

CATARAGA Olga……60
THE FUTURE OF JUDICIAL EXPERTISE IN THE REPUBLIC OF MOLDOVA AND IN THE EUROPEAN AREA

ARKUSHA Larysa…….……..64
THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF THE USE OF ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF ORGANIZED CRIMINAL GROUPS

BASALYUK Natalia.…….…....70
DIGITAL AND FORENSIC EVIDENCE IN EXTRADITION PROCEDURES: SELECTED ASPECTS

VARYNSKYI Vladyslav…….....74
THE PRINCIPLE OF HUMAN OVERSIGHT IN CRIMINAL JUSTICE: ADAPTATION OF EU AI ACT STANDARDS IN UKRAINE

HRES Yuliia……..79
FUNDAMENTALS OF USING BEHAVIOURAL PROFILING METHODOLOGY AND DIGITAL ANALYTICS IN THE INVESTIGATION OF PROFIT-MOTIVATED CRIMES UNDER CONDITIONS OF DIGITAL TRANSFORMATION

ZAHORODNII Andrii……..…84
INTERACTION OF PRE–TRIAL INVESTIGATION SUBJECTS AND THE USE OF ARTIFICIAL INTELLIGENCE ANALYTICAL SUPPORT AT THE STAGE OF PRE–TRIAL INVESTIGATION

KARAMAN Mykola……89
SPECIFIC ISSUES OF THE FEATURES OF EXPERT PROVISION OF JUSTICE IN RELATION TO CRIMES OF AGGRESSION AND WAR CRIMES IN THE ERA OF DIGITAL TECHNOLOGIES

MYROSHNYCHENKO Yurii……93
DIGITAL VISUALIZATION AS A MEANS OF FORENSIC SUPPORT OF JUDICIAL PROCEEDINGS

NEDASHKIVSKA Olga, GUNKO Olekxandr……..…97
DIGITIZATION AND ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ACTIVITY: TRANSFORMATION OF EVIDENCE, NEW TECHNOLOGICAL CAPABILITIES, AND CHALLENGES TO JUSTICE

OSTAPENKO Artur……..102
TECHNICAL AND CRIMINALISTICS SUPPORT FOR THE INVESTIGATION OF CRIMINAL OFFENSES IN THE CONDITIONS OF DIGITAL TRANSFORMATION

PLATOVSKIY Serhiy…..……106
RESEARCH ON COLLECTIBLE AND HISTORICAL AUTOMOBILES IN THE PRACTICE OF CULTURAL HERITAGE PROTECTION IN THE REPUBLIC OF POLAND

SAVCHUK Olena……..……110
FORENSIC HANDWRITING IN THE DIGITAL ERA: FROM CLASSICAL FEATURES TO NEW IDENTIFICATION MODELS

SALTYKOV Oleksandr……114
THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ACTIVITY: OPPORTUNITIES AND RISKS

SYDORCHUK Inna……..……117
THE ROLE OF DIGITAL TECHNOLOGIES IN IMPROVING THE EFFICIENCY OF FORENSIC EXPERT EXAMINATION

SMIRNOV Maksym……....120
INTERNATIONAL COOPERATION IN THE INVESTIGATION OF CRIMES IN THE DARKNET

TULIAKOV Viacheslav……124
EU ANTI–MONEY LAUNDERING LEGISLATION: NEW CHALLENGES FOR UKRAINE

USENKO Olena……..……128
APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN FORENSIC EXPERT ACTIVITY OF FOREIGN COUNTRIES

CHORNOUS Yuliia……...……132
CURRENT ISSUES OF FORENSIC SUPPORT FOR THE INVESTIGATION OF WAR CRIMES

SHEVCHUK Viktor……..…136
FUTURE CRIMINALISTICS IN THE ERA OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE: GLOBAL CHALLENGES AND DEVELOPMENT PROSPECTS

SHEPITKO Valerii, SHEPITKO Mykhailo……142
PROBLEMS OF FORMATION AND THE PLACE OF FORENSIC ENGINEERING IN THE STRUCTURE OF CRIMINALISTICS

SECTION 2.
DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF EXPERT SUPPORT FOR JUSTICE

AFANASENKO Svitlana……...……148
DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF EXPERT SUPPORT FOR JUSTICE

BATIG Andriy……151
APPLICATION OF PYTHON DIGITAL TECHNOLOGIES IN FORENSIC RAILWAY TRANSPORT EXPERTISE

BACHYLO Tetiana……154
THE PROBLEM OF LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ACTIVITY

BILINSKYI Markiyan……...…..158
APPLICATION OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN TECHNICAL FORENSIC EXAMINATION OF DOCUMENTS

VOZOVYK Yurii……...……161
FEATURES OF DIGITAL RECORDING OF TRACES OF THERMAL IMPACT IN FORENSIC EXPERTISE

VOZIAN Viorica……164
METHODS FOR RESEARCHING AND ANALYZING INVECTIVE LANGUAGE IN FORENSIC AUTHORSHIP

HALAYKO Marina……..…..…171
INTEGRATION OF DIGITAL INNOVATIONS AND ARTIFICIAL INTELLIGENCE IN CONSTRUCTION AND TECHNICAL EXPERTISE: CHALLENGES AND DEVELOPMENT PROSPECTS

HOLOVACH Rostislav, SHEREMETOV Serhii…….……176
DIGITAL DATA MEDIA AS OBJECTS OF FORENSIC MILITARY EXPERT EXAMINATION: METHODOLOGICAL AND REGULATORY ISSUES

GRECU Polixenia……..……180
CORRELATION OF FORENSIC MEDICAL FINDINGS AND BALLISTIC EXPERTISE RESULTS IN RECONSTRUCTING THE MECHANISM OF FIREARM DEATHS

KRYVONOZHKO Halyna, SOBIN Oleksii……184
ARTIFICIAL INTELLIGENCE AND SPECIALIZED DIGITAL TOOLS IN EXPERT SUPPORT FOR THE INVESTIGATION OF CYBERCRIMES AND DIGITAL OFFENCES

LIAKHOVETSKYI Serhii……189
STAGING SUICIDE BY HANGING TO CONCEAL INTENTIONAL HOMICIDE AND THE POSSIBILITIES OF ANALYTICAL SUPPORT BY ARTIFICIAL INTELLIGENCE

PĂTRU Alina Daniela……193
MODERN APPROACHES TO THE USE AND EXPLOITATION OF FORENSIC TRACES IN THE IDENTIFICATION OF VIOLENT CRIME OFFENDERS

RYBALKO Andrii, KOVKINA Yevheniia……...…197
IMPLICIT AND HYBRID DIRECTIVE UTTERANCES IN DIGITAL COMMUNICATION AS AN OBJECT OF FORENSIC PSYCHOLOGICAL AND LINGUISTIC EXAMINATION

STOLIAROVA Irina, PAHURETS Olha, MAKAROVA Oleksandra……..203
ARTIFICIAL INTELLIGENCE AS A TOOL FOR SPECTRUM DECODING IN FORENSIC EXAMINATION OF MATERIALS, SUBSTANCES AND PRODUCTS

TKACHENKO Nataliia……208
THE IMPACT OF DIGITAL TECHNOLOGIES ON THE DEVELOPMENT OF FORENSIC EXPERT ACTIVITY

TSELUYKO Mykhailo, USENKO Olena……212
THEORETICAL AND LEGAL FOUNDATIONS OF THE ORGANIZATION OF REMUNERATION FOR FORENSIC EXPERTS IN UKRAINE

TSILMAK Olena……...…216
COGNITIVE BIASES IN THE MECHANISM OF FORMING DIGITAL TRACES OF CRIMINAL ACTIVITY

SHANYHIN Anton, VOLOSHYNA Vladlena, AL-FAIYUMI Khaled……..…221
DIGITAL TECHNOLOGIES IN PUBLIC HEALTH: CHALLENGES OF CYBERSECURITY AND PROTECTION OF MEDICAL DATA

SECTION 3.
EXPERT SUPPORT FOR THE INVESTIGATION OF CRIMES IN CYBERSPACE AND THE USE OF VIRTUAL ASSETS

VELYCHKO Yuliia…….....225
PROSPECTS FOR CONDUCTING FORENSIC ECONOMIC EXPERTISE AND RESEARCH ON THE ISSUES OF DECLARING AND TAXING INCOME OF INDIVIDUALS OBTAINED FROM VIRTUAL ASSETS

VOZNYAK Oleh…….....230
FEATURES OF CONDUCTING COMPREHENSIVE FORENSIC EXAMINATIONS OF RAILWAY ACCIDENTS AT CROSSINGS: A REGULATORY AND TECHNICAL PERSPECTIVE OF A RAILWAY EXPERT

HOLOVA Inna, MENZUL Oksana…….....237
DETERMINING THE COST OF SERVICES IN FORENSIC EXPERTISE

DERECHA Andrii, ABROSIMOV Taras……240
CURRENT PROBLEMS OF USING SPECIAL KNOWLEDGE IN COURT EXAMINATION OF COMPUTER CRIMES UNDER CONDITIONS OF DIGITALIZATION

DYKYI Oleg…….....245
CYBERFORENSICS AS A KEY COMPONENT OF THE PROFESSIONAL TRAINING OF MODERN SECURITY SPECIALISTS

YEVSIUKOV Oleksandr…….....249
DIGITAL OBJECTS IN FORENSIC RESEARCH

KIOSE Michael…….....253
PROSPECTS OF USING ARTIFICIAL INTELLIGENCE IN RESEARCHING TITANIUM, ALUMINUM AND MAGNESIUM ALLOY POWDER AS DUAL-USE GOODS

LUSHCHYK Ihor, TIAPKIN Anatolii…….....258
WAYS IN WHICH LARGE LANGUAGE MODELS INTERACT WITH FORENSIC LINGUISTIC EXPERTISE

MINIAILO Anatolii, DMITRENKO Liudmyla, MINIAILO Nadia……263
ENGINEERING ENVIRONMENTAL EXPERTISE – AN IMPORTANT LINK IN COMBATING ENVIRONMENTAL OFFENSE

PIROH Oleksandr…….....268
FEATURES OF VOLATILE DATA ACQUISITION FROM IOT DEVICES

RADETSKYI Serhii…….....273
SPECIFIC FEATURES OF THE EXAMINATION OF ELECTRONIC DOCUMENTS AVAILABLE IN OPEN ACCESS

STAURSKA Oleksandra…….....278
«AUTOMATION OF EXPERT RESEARCH IN CRIMINALISTICS: FROM CLASSICAL METHODS TO INTELLIGENT ALGORITHMS»

KHAMULA Dmytro…….....283
ON THE QUESTION OF THE ATTRIBUTION OF THE GRIFFIN–TILED FIREPLACE STOVE FROM M. PIDHORSKYI'S HOUSE IN KYIV

CHABANETS Tetiana, MAKARETS Albina…….……287
IN–SITU EXAMINATION IN FORENSIC COMMODITY EXPERTISE AS A BASIS FOR IDENTIFICATION, DEFECT DETECTION AND PARAMETRIC SELECTION OF ANALOGUES

CHEREMNOVA Antonina…….....293
FORENSIC EXPERTISE IN THE EVIDENTIARY SYSTEM: ROLE, FUNCTIONS AND PROSPECTS FOR DEVELOPMENT

CHERNOV Oleksandr…….....298
FEATURES OF CONDUCTING HANDWRITING ANALYSIS OF SIGNATURES IN DIGITAL COPIES OF DOCUMENTS

YUSUPOV Volodymyr, KISIL Nataliia……303
INTEGRATION OF CRIMINALISTICS METHODS INTO THE PRACTICE OF CONDUCTING FORENSIC EXPERT EXAMINATIONS OF INTELLECTUAL PROPERTY OBJECTS

SECTION 4.
CRIMINAL LAW AND CRIMINOLOGICAL CHALLENGES OF DIGITALIZATION: FROM CYBERTERRORISM TO AUTONOMOUS WEAPONS SYSTEMS

ARTIUKH Nadiia, KOZACHENKO Vitalii……308
CYBERBULLYING IN THE SYSTEM OF DETERMINANTS OF YOUTH DEVIANT BEHAVIOR

BERSHAVSKA Anastasiia…….....313
ORGANIZATIONAL AND TACTICAL FEATURES OF COUNTERING CRIMES RELATED TO AIDING THE AGGRESSOR

GORBACHOVA Iryna…….....316
INFORMATION INJECTIONS AND DIGITAL DISINFORMATION AS AN ELEMENT OF HYBRID WARFARE

YEROFEIEVA Olha…….....321
MOTIVES OF CRIMINAL ENCOURAGEMENT IN CRIMINAL OFFENSES RELATED TO THE CONFISCATION OF INHERITABLE PROPERTY

KLYMENKO Daria, KOZACHENKO Vitalii……324
DIGITAL FORMS OF VIOLENCE AGAINST ELDERLY PERSONS: CRIMINOLOGICAL ASPECTS

KOZACHENKO Vitalii…….....329
VERBAL AGGRESSION IN SOCIAL MEDIA AS A CRIMINOLOGICAL PROBLEM

KUBAIENKO Andrii…….....334
EFFICIENCY OF POLICE ACTIVITY IN THE CONDITIONS OF DIGITALIZATION OF CRIMINAL THREATS

LUKASHCHUK Karina…….....338
DIGITALIZATION OF NON–CUSTODIAL SENTENCES: INTERNATIONAL EXPERIENCE AND PROSPECTS FOR UKRAINE

LUTSIUK Pavlo…….....342
PROBLEMS OF DEFINING THE FIRST–TIME COMMISSION OF A CRIMINAL OFFENSE IN CRIMINAL LAW AND JUDICIAL PRACTICE

SYDORCHUK Vladyslav, SYDORCHUK Inna…….……348
CYBERTERRORISM: CONCEPT, SIGNS AND DIRECTIONS OF COUNTERACTION

STEPANENKO Oksana…….....353
CYBERVIOLENCE AS AN INDEPENDENT FORM OF DOMESTIC VIOLENCE

TITUNINA Kateryna…….....358
COUNTERING RADICALIZATION AND HYBRID THREATS IN PENITENTIARY INSTITUTIONS UNDER MARTIAL LAW

TSEKHAN Dmytro…….....362
IDEOLOGY OF THE FORMATION AND FUNCTIONING OF ORGANIZED CRIMINAL GROUPS IN CONDITIONS OF ARMED CONFLICT

TSITRYAK Viktor…….....367
THE EFFECTIVENESS OF OPERATIONAL AND INVESTIGATIVE ACTIVITIES AS A MEANS OF ENSURING LAW AND ORDER IN PRISON

SECTION 5. CRIMINAL PROCEDURAL, OPERATIONAL-SEARCH AND CRIMINALISTICS ASPECTS OF DOCUMENTING CRIMES IN THE DIGITAL AGE

ALBUL Serhii…….....372
CRIMINAL INTELLIGENCE AS A SYSTEMIC ELEMENT OF A COMPREHENSIVE MODEL OF POLICE ACTIVITIES

VASHCHUK Olesia…….....377
PROBLEMS OF THE RELIABILITY OF PHOTO AND VIDEO EVIDENCE OF WAR CRIMES IN THE CONTEXT OF THE DEVELOPMENT OF DEEPFAKE TECHNOLOGIES

VOLOS Vladyslav…….....
FEATURES OF DETECTION AND RECORDING OF DIGITAL TRACES IN THE INVESTIGATION OF CRIMES COMMITTED BY ORGANIZED GROUPS

VOLOSHYNA Vladlena…….....384
PROCEDURAL ORDER FOR OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: PROBLEMS OF LAW ENFORCEMENT

HONCHARUK Vladyslava…….....387
SOCIAL NETWORKS AS A SOURCE OF FORENSIC TRACES: INNOVATIVE METHODS FOR INVESTIGATING TRAFFICKING

HREBENIUK Serhii, KUSHNIRENKO Nataliia……...……391
FORENSIC FINGERPRINT IDENTIFICATION OF UNIDENTIFIED CORPSES AND THEIR REMAINS USING DIGITAL IMAGES OF FINGERPRINTS FROM BIOMETRIC DOCUMENTS

HRYNEVYCH Viktoria…….....397
BETWEEN EFFICIENCY AND THE RULE OF LAW: LEGAL AND ETHICAL LIMITS OF THE APPLICATION OF NON–TRADITIONAL METHODS IN LAW ENFORCEMENT ACTIVITIES

DRYHA Yelyzaveta…….....401
COOPERATION BETWEEN INVESTIGATIVE AND OPERATIONAL UNITS DURING TACTICAL OPERATIONS IN THE INVESTIGATION OF THE ILLEGAL TRAFFICKING OF WEAPONS AND AMMUNITION UNDER MARTIAL LAW

ZAVTUR Viktor…….....406
DIGITAL SEARCH IN CRIMINAL PROCEEDINGS: SELECTED ISSUES OF THE REGULATORY MODEL

ZAHORODNII Ihor…….....412
ALGORITHMISATION OF PRE-TRIAL INVESTIGATION WITH THE POSSIBILITY OF USING ARTIFICIAL INTELLIGENCE ELEMENTS AS A BASIS FOR EFFECTIVE SOLVING OF SERIOUS AND ESPECIALLY SERIOUS CRIMINAL OFFENCES

ZAHORODNII Viktor…….....419
POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF A PROSECUTOR AS A PROCEDURAL SUPERVISOR AT THE FINAL STAGE OF PRE–TRIAL INVESTIGATION

ZHODA Yuliia…….....423
THE SETTING OF COMMITTING ACQUISITIVE CRIMES UNDER MARTIAL LAW OR STATE OF EMERGENCY

KILIMICHENKO Serhii…….....428
CIRCUMSTANCES TO BE ESTABLISHED UPON DETECTION OF INVESTIGATION OBSTRUCTION

KILIMICHENKO Khrystyna…….....434
PECULIARITIES OF APPLYING TACTICAL OPERATIONS DURING THE INVESTIGATION OF CRIMES AGAINST NATIONAL SECURITY COMMITTED BY WOMEN

KOVYRSHYN Viktor…….....439
SPECIFICS OF DETENTION OF AN ATTORNEY IN CRIMINAL PROCEEDINGS

KOLODIN Denys, KOLODINA Anna…….....442
ON THE ISSUE OF THE IMPACT OF DIGITAL TECHNOLOGIES ON THE SYSTEM OF FORENSIC TACTICS TOOLS

KUZNETSOVA Liudmyla…….....446
ON THE EXPEDIENCY OF MENTIONING ECONOMIC WELL–BEING IN CASES OF MAKING A DECISION TO DRAW UP A PRE–TRIAL REPORT IN CRIMINAL PROCEEDINGS

KRYVDA Liudmyla…….....450
THE USE OF SPECIAL KNOWLEDGE IN THE INVESTIGATION OF VIOLENT CRIMES: CURRENT STATE AND PROSPECTS FOR DEVELOPMENT

MAKSYMCHUK Ivan…….....453
THE INFLUENCE OF THE SUBJECT OF FORENSIC RESEARCH ON THE FORMATION OF STATISTICAL INDICATORS FOR CERTAIN TYPES OF CRIMINAL OFFENSES

MUNTIANU Yulian…….....458
OPEN SOURCE INTELLIGENCE IN THE INVESTIGATION OF HOSTAGE-TAKING AND INTENTIONAL MURDER

NECHYPORUK Volodymyr…….....461
REMOTE EXAMINATION OF PARTICIPANTS IN CRIMINAL PROCEEDINGS IN THE FOCUS OF THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

PAVZIUK Anatolii…….....465
PSYCHOLOGICAL PROFILE OF A PERSON WHO COMMITTED AN UNLAWFUL ACT: POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN FORENSIC BEHAVIORAL ANALYSIS

PALAMARCHUK Oleksii…….....470
THE SITUATION REGARDING BURGLARIES COMMITTED BY ORGANISED CRIMINAL GANGS

PATRELUK Dmytro…….....475
REGARDING MEANS OF CRIMINAL PROSECUTION

PETROSIAN Aik…….....478
INVESTIGATION OF CRIMINAL OFFENSES COMMITTED BY ORGANIZED CRIME GROUPS IN THE SPHERE OF INVESTMENT ACTIVITIES: THEORETICAL AND LEGAL PRINCIPLES

PYSHNENKO Iryna…….....483
STAGING AS A MEANS OF CONCEALING CRIMINAL ACTIVITY: METHODS OF MODELLING AND DETECTION

POZHAR Vadym…….....488
ISSUES OF THE PRINCIPLE OF ENSURING THE RIGHTS AND LEGITIMATE INTERESTS OF THE VICTIM WHEN APPLYING DETENTION TO A PERSON

RUBETS Kateryna…….....492
CRIMINAL PROCEDURAL AND FORENSIC PRINCIPLES OF THE USE OF HANDWRITING EXAMINATION IN THE DOCUMENTATION OF CRIMES IN THE CONDITIONS OF DIGITALIZATION

SAMOILENKO Olena…….....496
CRIMINAL ANALYSIS AS AN ELEMENT OF MODERN CRIMINALISTIC METHODOLOGIES

STARODUBOV Oleksandr…….....499
FEATURES OF THE USE OF COVERT INVESTIGATIVE (INTELLIGENCE–GATHERING) MEASURES DURING TACTICAL OPERATIONS, TAKING CURRENT CONDITIONS INTO ACCOUNT

TISHCHENKO Valerii, BIELIK Larysa…….504
INVESTIGATIVE SITUATION AS THE BASIS FOR TACTICAL AND STRATEGIC DECISIONS IN PRE–TRIAL INVESTIGATION

TORBAS Oleksandr…….……509
THE CONCEPT OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEDURE

FEDOROV Vladyslav…….....512
THE SITUATION REGARDING ROBBERIES INVOLVING THE USE OF FIREARMS DURING THE WAR AND IN THE POST–WAR PERIOD

FEDORCHUK Oleksandr…….....516
CORRELATION DEPENDENCES OF STRUCTURAL ELEMENTS OF CRIMINAL ACTIVITY OF OFFICIALS AND THE INFLUENCE OF THEIR KNOWLEDGE ON THE INVESTIGATION PROCESS

KHYZHNIAK Yevhen…….....521
THE ESSENCE OF COORDINATION AND INTERACTION BETWEEN CRIMINAL POLICE UNITS AND VARIOUS SUBJECTS DURING THE OPERATIONAL–SEARCH SUPPORT OF CRIMINAL PROCEEDINGS REGARDING INTENTIONAL HOMICIDES

CHYHRYNA Halyna…….....526
KEY FORMS OF FORENSIC SUPPORT OF LAW ENFORCEMENT ACTIVITIES: WORLD EXPERIENCE FOR UKRAINE

CHIPKO Nataliia…….....531
MODERN FRAUD IN THE SPHERE OF PAYMENT SYSTEMS

CHERNYSH Yuriy...…….....536
TYPICAL SITUATIONS OF THE SUBSEQUENT STAGE OF INVESTIGATING THE SMUGGLING OF CULTURAL PROPERTY

CHUMAK Serhiy...…….....539
DIGITALIZATION OF FORENSIC PHOTOGRAPHY IN EVIDENCE COLLECTION

SHEREMETOV Sergii…….....543
STAFFING OF RESEARCH INSTITUTIONS OF FORENSIC EXAMINATION AS A COMPONENT OF EXPERT SUPPORT FOR THE INVESTIGATION OF CRIMES IN THE MILITARY SPHERE

SHERSHENKOVA Viktoriia…….....555
COLLECTION OF EVIDENCE REGARDING MILITARY CRIMINAL OFFENSES UNDER MARTIAL STATE IN UKRAINE

YATSKEVICH Ruslan…….....559
COMPONENTS OF PROFESSIONAL COMPETENCE OF EMPLOYEES OF OPERATIONAL UNITS THAT PROVIDE COMBAT TO ORGANIZED CRIME

Шановні учасники конференції, дорогі колеги, науковці, практики, представники судово-експертних установ, правоохоронної спільноти та молоді дослідники!

Проведення Міжнародної науково-практичної конференції «Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози» є важливою подією не лише для Національного університету «Одеська юридична академія», а й для всієї професійної спільноти, яка працює у сфері криміналістики, судової експертизи, кримінального судочинства та забезпечення правової безпеки. Ця конференція стала результатом послідовної наукової роботи, спрямованої на осмислення тих змін, які сьогодні відбуваються у праві, технологіях, доказуванні та практиці протидії злочинності.

Криміналістика завжди була наукою практичної дії. Її цінність полягає не лише в теоретичних положеннях, а в здатності давати відповіді на конкретні питання розслідування: як виявити слід, як правильно його зафіксувати, як перевірити інформацію, як побудувати доказову версію, як відокремити достовірне від штучно створеного, випадкове від закономірного, правдиве від маніпулятивного. Саме тому кожна епоха ставить перед криміналістикою власні виклики, а сучасна цифрова епоха робить ці виклики особливо складними.

Сьогодні злочинність дедалі частіше виходить за межі традиційного матеріального простору. Вона використовує цифрові платформи, зашифровані канали комунікації, криптовалютні механізми, штучний інтелект, технології анонімізації, deepfake-інструменти, транскордонні інформаційні потоки та складні способи приховування цифрової активності. Водночас і доказова інформація змінює свою природу: вона може існувати у вигляді цифрового сліду, метаданих, електронного документа, зображення, аудіо- чи відеофайлу, результату автоматизованого аналізу або інформаційного зв’язку між різними джерелами.

У таких умовах криміналістика вже не може сприйматися тільки як сукупність усталених технічних, тактичних і методичних засобів. Вона поступово перетворюється на складну міждисциплінарну систему знань, у якій поєднуються правова доктрина, судово-експертні методики, цифрова аналітика, кібербезпека, кримінальний аналіз, інформаційні технології, штучний інтелект і міжнародна взаємодія. Однак технологічне оновлення не повинно витісняти головного - наукової обґрунтованості, процесуальної коректності, об’єктивності та поваги до прав людини.

Особливе значення ця проблематика має для України. В умовах воєнного стану, документування воєнних злочинів, протидії гібридним загрозам, кібератакам, інформаційним операціям, злочинам проти основ національної безпеки та транснаціональній організованій злочинності криміналістика набуває не лише наукового, а й державного значення. Від якості криміналістичних рішень сьогодні залежить не тільки ефективність окремого кримінального провадження, а й здатність держави захищати правопорядок, фіксувати злочини, забезпечувати справедливість і зберігати довіру до правосуддя.

Саме тому важливо, що ця конференція об'єднала представників різних наукових шкіл, освітніх установ, судово-експертних інституцій, правоохоронних органів і практичних середовищ. Такий формат дозволяє не просто обмінятися науковими позиціями, а побачити криміналістику в її реальному розвитку - на перетині теорії, експертної практики, кримінального процесу, цифрових технологій і міжнародного досвіду.

Матеріали, представлені у збірнику, засвідчують широту й глибину сучасного криміналістичного пошуку. У них порушуються питання використання штучного інтелекту в судово-експертній діяльності, допустимості та достовірності електронних доказів, виявлення й фіксації цифрових слідів, застосування OSINT-інструментів, протидії deepfake-технологіям, кримінального аналізу, документування злочинів у цифровому просторі, розвитку експертних методик і формування нових підходів до доказування.

Цінність цього збірника полягає не тільки в актуальності тематики. Його значення ширше: він фіксує момент переходу криміналістики до нового етапу розвитку. Це етап, коли класичні наукові положення не втрачають свого значення, але потребують осмислення в умовах цифрової доказової реальності. Це етап, коли науковець, експерт, слідчий, прокурор, адвокат і суддя мають говорити спільною професійною мовою, щоб технології служили правосуддю, а не створювали нові загрози для нього.

Окремо слід відзначити міжнародний характер конференції. Партнерство з інституціями Республіки Молдова, участь представників Азербайджану, Румунії, Польщі та інших професійних середовищ підтверджують, що криміналістика майбутнього не може розвиватися у вузьких національних межах. Цифрові докази, кіберзлочини, експертні стандарти, алгоритмічні технології та транснаціональні способи злочинної діяльності потребують відкритого міжнародного діалогу, узгодження підходів і взаємного професійного посилення.

Переконаний, що цей збірник буде корисним для науковців, викладачів, аспірантів, студентів, судових експертів, слідчих, прокурорів, адвокатів, суддів і всіх, хто працює у сфері кримінальної юстиції. Він може стати не лише джерелом наукової інформації, а й підґрунтям для подальших досліджень, методичних розробок, професійних дискусій та практичних рішень.

Щиро дякую організаційному комітету, співорганізаторам, авторам і всім учасникам конференції за активну наукову позицію, професійну відповідальність, доброчесність і готовність працювати над питаннями, від яких залежить майбутнє криміналістики та якість правосуддя в цифрову епоху.

Президент Національного університету
«Одеська юридична академія»,
Заслужений юрист України,
доктор юридичних наук, професор,
академік НАПрН України,
м. Одеса, Україна
Сергій Ківалов



Dear participants of the conference, esteemed colleagues, scholars, practitioners, representatives of judicial expertise institutions, the law enforcement community and young researchers!

The holding of the International Scientific and Practical Conference «Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats» is an important event not only for the National University «Odesa Law Academy», but also for the entire professional community working in the fields of criminalistics, judicial expertise, criminal justice and the legal protection of state security. This conference is the result of consistent scholarly work aimed at understanding the changes currently taking place in law, technology, evidence, and the practice of counteracting crime.

Criminalistics has always been a science of practical action. Its value lies not only in theoretical propositions, but also in its ability to provide answers to specific investigative questions: how to detect a trace, how to record it properly, how to verify information, how to construct an evidentiary version, how to distinguish the reliable from the artificially created, the accidental from the закономірного, and the truthful from the manipulative. For this reason, every historical period poses its own challenges to criminalistics, while the contemporary digital era makes these challenges particularly complex.

Today, crime is increasingly moving beyond the boundaries of the traditional material environment. It uses digital platforms, encrypted communication channels, cryptocurrency mechanisms, artificial intelligence, anonymization technologies, deepfake tools, cross-border information flows and sophisticated methods of concealing digital activity. At the same time, evidentiary information itself is changing its nature: it may exist as a digital trace, metadata, an electronic document, an image, an audio or video file, the result of automated analysis, or an informational connection between different sources.

Under such conditions, criminalistics can no longer be perceived solely as a set of established technical, tactical and methodological means. It is gradually transforming into a complex interdisciplinary system of knowledge that combines legal doctrine, judicial expertise methodologies, digital analytics, cybersecurity, criminal analysis, information technologies, artificial intelligence and international cooperation. However, technological renewal must not displace what is essential: scientific validity, procedural correctness, objectivity and respect for human rights.

This set of issues is of particular significance for Ukraine. Under martial law, in the context of documenting war crimes, counteracting hybrid threats, cyberattacks, information operations, crimes against the foundations of national security and transnational organized crime, criminalistics acquires not only scholarly but also state-level importance. The quality of criminalistic solutions today determines not only the effectiveness of an individual criminal proceeding, but also the ability of the state to protect legal order, document crimes, ensure justice and preserve public trust in the judiciary.

It is therefore especially important that this conference has brought together representatives of different scientific schools, educational institutions, judicial expertise bodies, law enforcement agencies and practical professional environments. Such a format allows participants not merely to exchange scholarly positions, but to observe criminalistics

in its real development - at the intersection of theory, expert practice, criminal procedure, digital technologies and international experience.

The materials presented in this collection demonstrate the breadth and depth of contemporary criminalistic inquiry. They address issues concerning the use of artificial intelligence in judicial expertise, the admissibility and reliability of electronic evidence, the detection and recording of digital traces, the application of OSINT tools, counteraction to deepfake technologies, criminal analysis, the documentation of crimes in the digital environment, the development of expert methodologies and the formation of new approaches to proof.

The value of this collection lies not only in the relevance of its subject matter. Its significance is broader: it records the moment of criminalistics' transition to a new stage of development. This is a stage at which classical scientific principles do not lose their importance, but require rethinking in the context of digital evidentiary reality. It is also a stage at which the scholar, expert, investigator, prosecutor, advocate and judge must speak a common professional language so that technologies serve justice rather than create new threats to it.

The international character of the conference deserves special emphasis. Partnership with institutions of the Republic of Moldova, as well as the participation of representatives of Azerbaijan, Romania, Poland and other professional communities, confirms that criminalistics of the future cannot develop within narrow national boundaries. Digital evidence, cybercrime, expert standards, algorithmic technologies and transnational forms of criminal activity require open international dialogue, the harmonization of approaches and mutual professional reinforcement.

I am convinced that this collection will be useful for scholars, lecturers, postgraduate students, students, judicial experts, investigators, prosecutors, advocates, judges and all those working in the field of criminal justice. It may become not only a source of scholarly information, but also a foundation for further research, methodological developments, professional discussions and practical solutions.

I sincerely thank the Organizing Committee, the co-organizers, the authors, and all conference participants for their active scholarly engagement, professional responsibility, integrity, and commitment to addressing the issues that will shape the future of criminalistics and the quality of justice in the digital age.

President of the National University
«Odesa Law Academy»,
Honoured Lawyer of Ukraine,
Doctor of Law, Professor,
Academician of the National Academy
of Legal Sciences of Ukraine
Odesa, Ukraine
Serhiy Kivalov



Stimați colegi, distinși participanți, reprezentanți ai mediului academic, ai instituțiilor de expertiză judiciară și ai comunității profesionale internaționale!

Conferința internațională științifico–practică «Criminalistica viitorului: inovații digitale, inteligență artificială, provocări și amenințări globale» constituie un prilej deosebit de important pentru consolidarea dialogului științific și profesional într–un domeniu aflat astăzi într–un proces profund de transformare. Criminalistica și expertiza judiciară nu mai pot fi analizate exclusiv prin prisma metodelor tradiționale de cercetare, deoarece realitățile contemporane impun o regândire substanțială a instrumentelor, procedurilor și standardelor aplicate în activitatea de identificare, examinare și valorificare a probelor.

Digitalizarea accelerată a relațiilor sociale, dezvoltarea inteligenței artificiale, extinderea comunicării online, apariția unor noi forme de criminalitate și utilizarea tehnologiilor avansate în comiterea, ascunderea sau simularea faptelor ilicite modifică în mod esențial conținutul activității criminalistice și expertale. În prezent, informația relevantă pentru procesul de probare poate exista sub forma urmelor digitale, a documentelor electronice, a metadatelor, a imaginilor, a înregistrărilor audio–video, a datelor tehnice, a comunicărilor electronice sau a rezultatelor generate prin sisteme algoritmice complexe.

Pentru instituțiile de expertiză judiciară, aceste schimbări nu reprezintă doar o temă de reflecție teoretică, ci o realitate profesională cotidiană. Expertul contemporan este chemat să lucreze cu volume mari de date, cu obiecte complexe, cu informații volatile, ușor de modificat, copiat, ascuns sau manipulat. În asemenea condiții, activitatea expertală presupune nu numai competențe tehnice avansate, ci și o înțelegere profundă a valorii probatorii a informației, a integrității acesteia, a originii datelor analizate și a limitelor metodologice ale instrumentelor utilizate.

Modernizarea expertizei judiciare nu poate fi redusă la simpla introducere a unor tehnologii noi în activitatea de cercetare. Ea presupune, înainte de toate, consolidarea cadrului metodologic, dezvoltarea unor proceduri clare și verificabile, acreditarea laboratoarelor, formarea profesională continuă a experților, respectarea independenței expertale și asigurarea trasabilității fiecărei etape a examinării. Calitatea unei concluzii expertale nu este determinată doar de performanța tehnică a instrumentului folosit, ci de rigoarea metodei, competența specialistului și posibilitatea verificării rezultatului obținut.

O atenție deosebită trebuie acordată utilizării inteligenței artificiale și a instrumentelor algoritmice în activitatea de expertiză judiciară. Acestea pot contribui la prelucrarea unor volume mari de informații, la identificarea unor corelații, la clasificarea preliminară a datelor sau la eficientizarea anumitor etape ale cercetării. Totuși, ele nu trebuie să substituie raționamentul expertului, analiza profesională și responsabilitatea umană. Controlul uman asupra procesului de cercetare rămâne o condiție esențială pentru menținerea obiectivității, transparenței și credibilității concluziilor expertale.

În acest context, protejarea integrității probelor capătă o importanță fundamentală. Orice intervenție asupra datelor digitale, orice prelucrare algoritmică, orice transfer sau

stocare a informației trebuie să fie realizată cu respectarea cerințelor de autenticitate, securitate, trasabilitate și reproductibilitate. În caz contrar, chiar și cele mai moderne instrumente tehnologice pot genera riscuri pentru procesul de probare, pentru drepturile persoanelor implicate și pentru încrederea în actul de justiție.

Cooperarea internațională reprezintă, de asemenea, o dimensiune indispensabilă a dezvoltării criminalisticii și expertizei judiciare contemporane. Criminalitatea digitală, circulația transfrontalieră a datelor, utilizarea platformelor online, mecanismele de anonimizare și apariția unor noi forme de manipulare informațională impun schimbul constant de experiență între instituții, cercetători, experți și practicieni. Numai printr–un dialog profesional deschis pot fi formulate standarde comune, metode comparabile și soluții eficiente pentru provocările actuale.

Conferința organizată de Universitatea Națională «Academia Juridică din Odesa», în cooperare cu instituțiile partenere, oferă o platformă necesară pentru acest schimb de idei, experiențe și abordări profesionale. Ea permite apropierea dintre cercetarea științifică și practica expertală, dintre mediul universitar și instituțiile aplicative, dintre tradiția criminalistică și necesitatea adaptării la noile realități digitale.

Materialele publicate în prezentul volum demonstrează diversitatea temelor abordate, nivelul științific al cercetărilor prezentate și deschiderea comunității profesionale către inovație, responsabilitate și cooperare. Ele reflectă preocuparea comună pentru dezvoltarea expertizei judiciare, perfecționarea standardelor de probare, consolidarea metodologiilor de cercetare și adaptarea practicilor naționale la exigențele spațiului juridic european.

Exprim recunoștință organizatorilor, autorilor și tuturor participanților pentru contribuția adusă la consolidarea dialogului științific internațional. Sunt convinsă că rezultatele acestei conferințe vor avea o valoare reală nu doar pentru mediul academic, ci și pentru instituțiile de expertiză judiciară, organele de drept și întreaga comunitate profesională preocupată de calitatea probării, de protecția drepturilor omului și de dezvoltarea justiției într–o societate digitală.

Directorul Centrului Național de Expertize Judiciare
al Ministerului Justiției din Republica Moldova
dr. Olga CATARAGA



Esteemed colleagues, distinguished participants, representatives of the academic community, judicial expertise institutions and the international professional community!

The International Scientific and Practical Conference «Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats» constitutes a particularly important occasion for strengthening scientific and professional dialogue in a field that is currently undergoing profound transformation. Criminalistics and judicial expertise can no longer be examined exclusively through the prism of traditional research methods, since contemporary realities require a substantial reconsideration of the instruments, procedures and standards applied in the identification, examination and evidentiary use of proof.

The accelerated digitalization of social relations, the development of artificial intelligence, the expansion of online communication, the emergence of new forms of crime and the use of advanced technologies in the commission, concealment or simulation of unlawful acts are fundamentally changing the content of criminalistic and expert activity. At present, information relevant to the process of proof may exist in the form of digital traces, electronic documents, metadata, images, audio and video recordings, technical data, electronic communications or results generated by complex algorithmic systems.

For judicial expertise institutions, these changes are not merely a subject of theoretical reflection, but an everyday professional reality. The contemporary expert is required to work with large volumes of data, complex objects and volatile information that can easily be altered, copied, concealed or manipulated. Under such conditions, expert activity requires not only advanced technical competence, but also a profound understanding of the evidentiary value of information, its integrity, the origin of the data analysed and the methodological limits of the instruments used.

The modernization of judicial expertise cannot be reduced to the mere introduction of new technologies into research activity. It presupposes, above all, the strengthening of the methodological framework, the development of clear and verifiable procedures, the accreditation of laboratories, the continuous professional training of experts, respect for expert independence and the assurance of traceability at every stage of the examination. The quality of an expert conclusion is determined not only by the technical performance of the instrument employed, but by the rigour of the method, the competence of the specialist and the possibility of verifying the result obtained.

Particular attention must be paid to the use of artificial intelligence and algorithmic instruments in judicial expertise. Such tools may contribute to the processing of large volumes of information, the identification of correlations, the preliminary classification of data or the optimization of certain stages of research. However, they must not replace expert reasoning, professional analysis or human responsibility. Human control over the research process remains an essential condition for maintaining the objectivity, transparency and credibility of expert conclusions.

In this context, the protection of the integrity of evidence acquires fundamental importance. Any intervention in digital data, any algorithmic processing, any transfer or storage of information must be carried out in compliance with the requirements of authenticity, security, traceability and reproducibility. Otherwise, even the most advanced technological instruments may generate risks for the process of proof, for the rights of the persons involved and for public confidence in the administration of justice.

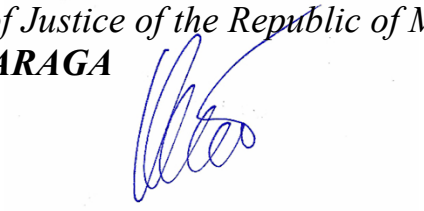
International cooperation is likewise an indispensable dimension of the development of contemporary criminalistics and judicial expertise. Digital crime, the cross–border circulation of data, the use of online platforms, anonymization mechanisms and the emergence of new forms of informational manipulation require a constant exchange of experience among institutions, researchers, experts and practitioners. Only through open professional dialogue can common standards, comparable methods and effective solutions to current challenges be formulated.

The conference organized by the National University «Odesa Law Academy», in cooperation with partner institutions, provides a necessary platform for this exchange of ideas, experience and professional approaches. It facilitates closer interaction between scientific research and expert practice, between the university environment and applied institutions, between the criminalistic tradition and the need to adapt to new digital realities.

The materials published in this volume demonstrate the diversity of the topics addressed, the scientific level of the research presented and the openness of the professional community to innovation, responsibility and cooperation. They reflect a shared concern for the development of judicial expertise, the improvement of standards of proof, the strengthening of research methodologies and the adaptation of national practices to the requirements of the European legal area.

I express my gratitude to the organizers, authors and all participants for their contribution to the consolidation of international scientific dialogue. I am convinced that the results of this conference will have genuine value not only for the academic community, but also for judicial expertise institutions, law enforcement bodies and the entire professional community concerned with the quality of proof, the protection of human rights and the development of justice in a digital society.

Director National Center for Judicial Expertise
of the Ministry of Justice of the Republic of Moldova
PhD Olga CATARAGA



Шановні колеги, учасники конференції, представники наукової, судово–експертної та правозастосовної спільноти!

Судова експертиза завжди працює там, де загальні припущення вже не мають значення, а вирішальними стають точність, методика, перевірюваність і відповідальність за кожне сформульоване положення. Саме тому тема цієї конференції є для експертної спільноти не віддаленою науковою перспективою, а частиною щоденної професійної роботи. Цифрові носії, електронні документи, віртуальні активи, дані з мобільних пристроїв, онлайн–комунікації, штучно створені зображення, відео– та аудіоматеріали вже стали звичайними об'єктами експертного дослідження.

У цій новій реальності змінюється не лише перелік об'єктів, з якими працює експерт. Змінюється сама логіка експертного пізнання. Якщо раніше значна частина досліджень була пов'язана переважно з матеріальними слідами, документами, предметами та фізичними властивостями об'єктів, то сьогодні все частіше доводиться працювати з інформацією, яка існує у цифровій формі, швидко змінюється, легко копіюється, може бути прихована, спотворена або штучно згенерована. Це вимагає від експерта не тільки технічної підготовки, а й здатності критично оцінювати походження, цілісність і доказове значення такої інформації.

Для Одеського науково–дослідного інституту судових експертиз Міністерства юстиції України розвиток науково–практичної взаємодії з університетами, правоохоронними органами, судами та іншими експертними установами має принципове значення. Жодна експертна установа не може ефективно відповідати на сучасні виклики ізольовано. Нові види об'єктів, складність цифрових доказів, потреба в оновленні методик і високі вимоги судової практики потребують постійного професійного діалогу між наукою та практикою.

Особливо важливо, щоб цифровізація судової експертизи не перетворилася на просте накопичення технічних засобів. Наявність програмного забезпечення, аналітичних платформ або алгоритмічних інструментів сама по собі ще не гарантує якості експертного дослідження. Якість забезпечують методологія, компетентність експерта, дотримання процедури, наукова обґрунтованість висновків і можливість перевірити шлях, яким експерт дійшов до результату.

Тому питання використання штучного інтелекту та цифрових технологій у судово–експертній діяльності слід розглядати не з позиції безумовного захоплення новизною, а з позиції професійної відповідальності. Алгоритм може допомагати у виявленні закономірностей, обробці великих масивів даних, попередній класифікації інформації чи пошуку зв'язків. Але остаточне експертне судження має залишатися результатом фахового аналізу, а не механічного прийняття машинного результату.

Сучасна експертиза також дедалі частіше виходить за межі одного вузького виду дослідження. У багатьох провадженнях цифрові сліди поєднуються з економічною інформацією, документами, мовними матеріалами, відеозаписами, товарами, зброєю, вибуховими речовинами, об'єктами військового походження та

іншими доказовими джерелами. Саме тому майбутнє судово–експертної діяльності полягає не лише в розвитку окремих методик, а й у здатності до комплексного, міждисциплінарного бачення доказової картини.

Матеріали цього збірника демонструють, що професійна спільнота вже не просто констатує появу нових викликів, а шукає практичні відповіді на них. У поданих працях порушуються питання цифрових слідів, експертного аналізу кіберзлочинів, дослідження електронних документів, використання штучного інтелекту, кримінального аналізу, судово–експертного забезпечення розслідування воєнних, економічних та інших категорій кримінальних правопорушень. Цінність таких матеріалів полягає в тому, що вони поєднують наукове бачення з реальними потребами практики.

Для української експертної спільноти ця тематика має ще один вимір. В умовах війни, масового документування злочинів, кібератак, інформаційних операцій і зростання складності кримінальних проваджень експертний висновок часто стає одним із ключових елементів доказування. Від його якості залежить не лише процесуальна перспектива конкретної справи, а й довіра до правосуддя загалом.

Переконаний, що ця конференція є важливою не лише як науковий захід, а як простір професійної звірки позицій: що ми вже вміємо, чого ще бракує, які методики потребують оновлення, які ризики не можна ігнорувати та якою має бути судова експертиза в умовах цифрового майбутнього.

Висловлюю повагу організаторам конференції, авторам і всім учасникам за фахову роботу, змістовні дослідження та готовність вести відверту професійну розмову про складні питання. Бажаю, щоб цей збірник став не формальним підсумком конференції, а корисним джерелом для подальших наукових досліджень, методичних розробок і практичних рішень, які посилюватимуть судово–експертну діяльність і доказову основу правосуддя.

Директор Одеського науково-дослідного
інституту судових експертиз
Міністерства юстиції України,
м. Одеса, Україна
Дмитро Кішко



Dear colleagues, conference participants, representatives of the scientific, judicial expertise and law enforcement communities!

Judicial expertise has always operated in the sphere where general assumptions no longer suffice, and where precision, methodology, verifiability and responsibility for every formulated conclusion become decisive. That is why the theme of this conference is not a remote scientific prospect for the expert community, but an integral part of its everyday professional work. Digital media, electronic documents, virtual assets, data from mobile devices, online communications, artificially generated images, video and audio materials have already become ordinary objects of expert examination.

In this new reality, it is not only the range of objects examined by experts that is changing. The very logic of expert cognition is also being transformed. Whereas previously a significant part of expert research was primarily associated with material traces, documents, objects and their physical properties, today experts increasingly have to work with information that exists in digital form, changes rapidly, can be easily copied, concealed, distorted or artificially generated. This requires from the expert not only technical competence, but also the ability to critically assess the origin, integrity and evidentiary value of such information.

For the Odesa Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine, the development of scientific and practical cooperation with universities, law enforcement agencies, courts and other expert institutions is of fundamental importance. No expert institution can respond effectively to contemporary challenges in isolation. New types of objects, the complexity of digital evidence, the need to update methodologies and the high demands of judicial practice require constant professional dialogue between science and practice.

It is particularly important that the digitalization of judicial expertise should not be reduced to the mere accumulation of technical tools. The availability of software, analytical platforms or algorithmic instruments does not in itself guarantee the quality of an expert examination. Quality is ensured by methodology, expert competence, adherence to procedure, the scientific validity of conclusions and the possibility of verifying the path by which the expert arrived at the result.

Therefore, the use of artificial intelligence and digital technologies in judicial expertise should be considered not from the standpoint of unconditional fascination with novelty, but from the standpoint of professional responsibility. An algorithm may assist in identifying patterns, processing large datasets, preliminarily classifying information or detecting connections. However, the final expert judgement must remain the result of professional analysis, not the mechanical acceptance of a machine–generated outcome.

Contemporary expertise also increasingly goes beyond the limits of a single narrow type of examination. In many proceedings, digital traces are combined with economic information, documents, linguistic materials, video recordings, goods, weapons, explosives, military–origin objects and other evidentiary sources. For this reason, the future of judicial expertise lies not only in the development of individual

methodologies, but also in the ability to form a comprehensive, interdisciplinary vision of the evidentiary picture.

The materials of this collection demonstrate that the professional community is no longer merely acknowledging the emergence of new challenges, but is seeking practical responses to them. The submitted papers address issues of digital traces, expert analysis of cybercrime, examination of electronic documents, the use of artificial intelligence, criminal analysis, and judicial expertise support for the investigation of war crimes, economic offences and other categories of criminal offences. The value of these materials lies in the fact that they combine scientific vision with the real needs of practice.

For the Ukrainian expert community, this topic has an additional dimension. In the context of war, the mass documentation of crimes, cyberattacks, information operations and the increasing complexity of criminal proceedings, an expert opinion often becomes one of the key elements of proof. Its quality determines not only the procedural prospects of a particular case, but also public trust in justice as a whole.

I am convinced that this conference is important not only as a scientific event, but also as a space for professional alignment of positions: what we already know how to do, what is still lacking, which methodologies require updating, which risks must not be ignored, and what judicial expertise should be in the conditions of the digital future.

I express my respect to the organizers of the conference, the authors and all participants for their professional work, substantive research and readiness to engage in an open professional discussion of complex issues. I hope that this collection will become not merely a formal outcome of the conference, but a useful source for further scientific research, methodological developments and practical solutions that will strengthen judicial expertise and the evidentiary foundation of justice.

Director of the Odesa
Scientific Research Institute
of Forensic Examinations
Ministry of Justice of Ukraine
Dmytro Kishko



Шановні колеги, учасники конференції, представники наукової, освітньої, судово–експертної та правоохоронної спільноти!

Криміналістика завжди була наукою, яка першою відчуває зміну характеру злочинності. Там, де змінюються способи підготовки, вчинення та приховування кримінальних правопорушень, неминуче змінюються і засоби їх виявлення, фіксації та дослідження. Саме тому розмова про криміналістику майбутнього сьогодні є не прогнозом на віддалену перспективу, а професійною необхідністю, з якою вже працюють слідчі, прокурори, судові експерти, науковці та суди.

Міжнародна науково–практична конференція «Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози» піднімає питання, які виходять далеко за межі звичайного оновлення криміналістичної техніки. Йдеться про більш глибоку зміну – про трансформацію самої доказової реальності. Доказова інформація дедалі частіше виникає, зберігається, передається і змінюється у цифровому середовищі. Вона може бути фрагментарною, розподіленою між різними платформами, прихованою за технічними механізмами анонімізації або штучно змодельованою за допомогою алгоритмічних технологій.

За таких умов криміналістика вже не може обмежуватися лише пошуком матеріального сліду у його класичному розумінні. Вона має працювати з новими формами слідової інформації – цифровими слідами, електронними доказами, метаданими, результатами автоматизованого аналізу, інформаційними зв’язками, віртуальними активами, даними відкритих джерел, зображеннями, аудіо– та відеоматеріалами, які можуть бути як джерелом істини, так і результатом складної маніпуляції.

Водночас технологічний розвиток не скасовує фундаментальних засад криміналістики. Навпаки, він робить їх ще більш значущими. Будь–який цифровий інструмент, яким би сучасним він не був, має оцінюватися крізь призму наукової обґрунтованості, перевірюваності, процесуальної допустимості, об’єктивності та можливості відтворення результатів. Штучний інтелект, автоматизовані системи аналізу, технології розпізнавання, OSINT–інструменти та інші цифрові рішення не повинні підміняти криміналістичне мислення. Вони можуть посилювати його, але не замінювати професійну оцінку, досвід і відповідальність людини.

Саме в цьому, на моє переконання, полягає один із головних викликів сучасності: криміналістика має не просто прийняти нові технології, а навчитися керувати ними в інтересах правосуддя. Не технологія повинна диктувати логіку доказування, а науково обґрунтована криміналістична методологія має визначати межі, умови та критерії використання технологій у кримінальному провадженні.

Ці питання є актуальними як для України, так і для світової спільноти. Воєнні злочини, кібератаки, інформаційні операції, злочини проти основ національної безпеки, транснаціональна організована злочинність і використання цифрового простору для приховування кримінальної активності потребують не

загальних декларацій, а точних, дієвих і процесуально надійних криміналістичних рішень. Сьогодні від якості фіксації доказової інформації залежить не лише результат окремого провадження, а й здатність держави документувати злочини, захищати права людини та забезпечувати справедливість.

Матеріали цього збірника показують, що наукова спільнота уважно реагує на ці зміни. У працях авторів розглядаються проблеми цифрових слідів, електронних доказів, штучного інтелекту, судово–експертної діяльності, кіберзлочинності, кримінального аналізу, інформаційної безпеки, міжнародної взаємодії та нових стандартів доказування. Важливо, що ці питання подані не ізольовано, а як частини єдиного процесу оновлення криміналістичної науки.

Міжнародний характер конференції також має принципове значення. Сучасна злочинність не обмежується державними кордонами, а цифрові докази часто мають транскордонну природу. Саме тому розвиток криміналістики майбутнього неможливий без професійного діалогу між науковими школами, експертними установами, освітніми центрами та практиками різних держав. Такий діалог дозволяє не лише обмінюватися досвідом, а й поступово формувати спільні підходи до якості, достовірності та використання доказової інформації.

Висловлюю щиру повагу організаторам конференції, авторам наукових праць і всім учасникам за внесок у розвиток сучасної криміналістичної думки. Переконаний, що цей збірник стане не просто відображенням проведеного наукового заходу, а важливим джерелом для подальших досліджень, професійних дискусій і практичних рішень у сфері криміналістики, судової експертизи та кримінального судочинства.

Криміналістика майбутнього формується вже сьогодні. І від того, наскільки відповідально наукова та професійна спільнота осмислить цифрові виклики, залежить не лише розвиток науки, а й якість правосуддя в нову цифрову епоху.

Президент Міжнародної громадської
організації «Конгрес криміналістів»,
м. Харків, Україна
Валерій Шепітько



Dear colleagues, participants of the conference, representatives of the scientific, educational, judicial expertise and law enforcement communities!

Criminalistics has always been a science that is among the first to sense changes in the nature of crime. Wherever the methods of preparing, committing and concealing criminal offences change, the means of detecting, recording and proving them inevitably change as well. That is why the discussion of criminalistics of the future today is not a forecast for a distant perspective, but a professional necessity already faced by investigators, prosecutors, judicial experts, scholars and courts.

The International Scientific and Practical Conference «Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats» raises issues that go far beyond the ordinary renewal of criminalistic techniques. It concerns a much deeper change – the transformation of evidentiary reality itself. Evidentiary information increasingly emerges, is stored, transmitted and modified in the digital environment. It may be fragmented, distributed across different platforms, hidden behind technical mechanisms of anonymization, or artificially modelled through algorithmic technologies.

Under such conditions, criminalistics can no longer be limited to the search for a material trace in its classical understanding. It must work with new forms of trace information – digital traces, electronic evidence, metadata, results of automated analysis, informational links, virtual assets, open–source data, images, audio and video materials, which may serve both as a source of truth and as the result of complex manipulation.

At the same time, technological development does not abolish the fundamental principles of criminalistics. On the contrary, it makes them even more significant. Any digital tool, however advanced it may be, must be assessed through the prism of scientific validity, verifiability, procedural admissibility, objectivity and the reproducibility of results. Artificial intelligence, automated analytical systems, recognition technologies, OSINT tools and other digital solutions must not replace criminalistic thinking. They may strengthen it, but they cannot substitute professional assessment, experience and human responsibility.

In my view, this is one of the main challenges of the present stage: criminalistics must not merely accept new technologies, but learn to manage them in the interests of justice. Technology should not dictate the logic of proof; rather, scientifically grounded criminalistic methodology must determine the limits, conditions and criteria for the use of technologies in criminal proceedings.

These issues are of particular importance for Ukraine. War crimes, cyberattacks, information operations, crimes against the foundations of national security, transnational organized crime and the use of digital space to conceal criminal activity require not general declarations, but precise, effective and procedurally reliable criminalistic solutions. Today, the quality of recording evidentiary information determines not only the outcome of a particular proceeding, but also the ability of the state to document crimes, protect human rights and ensure justice.

The materials of this collection show that the scientific community responds attentively to these changes. The works of the authors address the problems of digital traces, electronic evidence, artificial intelligence, judicial expertise, cybercrime, criminal analysis, information security, international cooperation and new standards of proof. It is important that these issues are presented not in isolation, but as parts of a unified process of renewal of criminalistic science.

The international character of the conference is also of fundamental importance. Modern crime is not confined within state borders, and digital evidence often has a cross–border nature. That is why the development of criminalistics of the future is impossible without professional dialogue among scientific schools, expert institutions, educational centres and practitioners from different states. Such dialogue makes it possible not only to exchange experience, but also gradually to develop common approaches to the quality, reliability and use of evidentiary information.

I express my sincere respect to the organizers of the conference, the authors of scientific papers and all participants for their contribution to the development of modern criminalistic thought. I am convinced that this collection will become not merely a reflection of the scientific event held, but an important source for further research, professional discussions and practical solutions in the field of criminalistics, judicial expertise and criminal justice.

Criminalistics of the future is being shaped today. The development of science, as well as the quality of justice in the new technological era, depends on how responsibly the scientific and professional community understands and addresses digital challenges.

President of the International Public
Organization «Criminalists Congress»,
Kharkiv, Ukrain
Valerii Shepitko



Секція 1.
КРИМІНАЛІСТИЧНІ ІННОВАЦІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СТРАТЕГІЇ ПОДОЛАННЯ ГЛОБАЛЬНИХ ЗЛОЧИННИХ ЗАГРОЗ

DOI https://doi.org/10.32837/11300.33524

Aliyev Bakhtiyar Abdurahman ogly
candidate of law sciences (Ph.D.), associate professor,
Editor–in–chief of the scientific and practical journal
«Antiterror and Security Problems» (Azerbaijan),
Baku, Azerbaijan
ORCID: https://orcid.org/0000–0003–0104–4921
e–mail: bakhtiyaraliyev69@gmail.com

HISTORY AND DEVELOPMENT OF MODERN FORENSIC SCIENCE (CRIMINALISTICS) IN THE REPUBLIC OF AZERBAIJAN

In the modern life it is increasing importance of the lawyers' specialty, conditions of the Azerbaijan society and developing in this direction. Also, it is action formalizing general conception about importance of the preparation and creation the new, wide and special lawyers' knowledge. Such experts should have the following qualities: based on logical activity; highly developed, special and seriously preparing on own professional activity; quick adapting to the hard conditions of implementations of the law. Professional development and skills in using information technology are necessary to have for modern lawyers in Azerbaijan in this case, existing three stepped high educational system in our country has such specific experts' features.

In this article reader could be interested in conducting of criminalistic education, especially, in preparation of high qualified criminalists and forensic experts, and also development in educational sphere.

Key words: criminalistics, legal knowledge, professional training, teaching, skill, practical activity.

The significant increase in the social importance of legal professions in modern Azerbaijan, driven by the strengthening role of law in all spheres of our society and state, and the considerable expansion of areas for the practical application of legal knowledge at a proper level, on one hand, and, on the other hand, a certain decline in the professionalism of lawyers within the state apparatus and other bodies, especially in the detection and investigation of crimes during the transitional period, have necessitated corresponding improvements in the training of lawyers, including specialists in the field of criminalistics. Undoubtedly, such improvement will not be able to solve all issues in the fight against crime but will positively impact further solutions.

Adjustments to the nature and level of professional training of lawyers in any field are part of the nationwide task of improving higher and postgraduate professional

education, stemming from the requirements of the Law of the Azerbaijan Republic «On Education»[5]

Currently, considering the increasing importance of legal professions, the state and trends of development in Azerbaijani society, and the provisions of the Law «On Education,» there is a general consensus on the need to train modern lawyers of both broad and narrow specializations of a new type. Such specialists must possess the following qualities: a well–developed need for logically precise cognitive activity and creative implementation of tasks in their professional activities based on fundamental general legal and solid specialized training; the ability to adapt relatively quickly in complex situations of any law enforcement activity; the capacity for professional growth and mobility in the context of computerization and information society.

In this regard, the three–level higher education system in Azerbaijan also acquires its own specifics.

For criminalists, the primary concern is what changes should be made to the teaching of criminalistics and the training of specialists in this field, what guidelines should be followed, and what is needed to achieve this.

The teaching of criminalistics in Azerbaijani law schools, like the science itself, has its own history. The first criminalistics course was introduced at the Faculty of Law of Azerbaijan State University (now Baku State University) in the late 1920s. This course was naturally based on educational literature and systems predominantly focused on criminal tactics (characteristics of criminals and their activities, investigative tactics, and scientific methods of crime investigation).

With the development of criminalistic theory and the study and generalization of investigative practice, certain adjustments were made to the course system, curricula, and educational materials, aimed at expanding the range of issues addressed in the university course of criminalistics.

In the mid–1930s, with the publication of the first two–volume university textbook (1935–1936), criminalistics became one of the mandatory disciplines in law schools and other legal educational institutions of the former USSR. The publication of textbooks in 1938–1939 and in 1950, 1952 further strengthened the importance of criminalistics as a mandatory discipline in higher legal education.

The teaching of criminalistics in Azerbaijan (as in other republics of the former USSR) according to its division into three components – criminalistic technique, tactics, and investigation methods – practically began in the mid–1950s. Since then, the general criminalistics course has been taught within this system in all law schools of the country.

During this time, the textbook «Criminalistic Technique» was published in Azerbaijani, co–authored by K.G. Saridjalinskaya and D.G. Movsumov (Azerbaijan Publishing House, 1975) [1, p.8].

The exchange of experience in teaching criminalistics within this system and information received from investigative authorities indicate that students, even those specializing in criminalistics, gained knowledge through modern teaching methods and

technical support, enabling them to work as investigators, although not as easily as students specializing in this field.

At the same time, new systems for the criminalistics course were sought, taking into account modern trends. After the collapse of the USSR, in 1989, the Department of Criminalistics and Forensic Expertise of Baku State University, under the leadership of Prof. K.G. Saridjalinskaya, prepared and published a textbook on criminalistics in Azerbaijani («Criminalistics,» Textbook for Universities, «Hüquq Ədəbiyyatı,» 1999), which was based on the division of criminalistics into four parts, and accordingly, the course and curriculum were reorganized [2, p. 14] .

A fundamentally new approach to the presentation of material was adopted in the collective course on criminalistics in Russian, edited by Doctor of Law D.G. Suleymanov («Criminalistics,» Textbook, «Ishyg,» 2000).

A more traditional approach to the system of criminalistics was taken by Candidates of Law B.A. Aliyev and A.M. Makhmudov in the educational and methodological manual in Azerbaijani («Criminalistics: Schemes, Commentary, Terms,» Baku, «Ganun,» 2003) [3, p. 183].

It should be noted that, in our opinion, the course of criminology should not be confused with a monographic course of criminology, which does not claim to be recognized as an academic course and is essentially a theoretical work.

Considering the modern trends in the training of lawyers, it is necessary to determine in which direction it is most appropriate to adjust the preparation of specialists in the field of criminology.

It is known that the key figure of specialization in many law schools preparing lawyers of broad and narrow profiles is the investigator. According to their functions and nature, they must be a researcher and thinker, a specialist with good logical and criminological thinking, capable of conducting a continuous search for necessary information with effective use of the entire technical, tactical, and methodological arsenal of criminology, and able to make quick and correct decisions in any investigative and especially problematic situations. They must also interact correctly with operational–search bodies, primarily in the «hot pursuit» of crimes. The investigator must be clearly oriented towards solving crimes «on hot pursuit» rather than conducting investigations with an unknown outcome.

Therefore, such a specialist needs to possess a wide range of knowledge in criminology, related sciences of the criminological cycle, and the basics of operational–search activity, as well as many other sciences, both humanitarian and natural. This is precisely what distinguishes the profession of an investigator among other legal specialties.

It is no coincidence that Hans Gross, in his famous work, which laid the foundation of criminology as a science and academic discipline, devoted significant attention to reflections on what an investigator should be like, considering them the most important element of the «general staff in the fight against crime.» Gross called the work of an investigator an artful activity based on extensive legal knowledge, the study of

people, the ability to communicate with them, and the capacity to solve questions in all fields of human knowledge without exception. The investigator must master the art of penetrating the criminological essence of crimes, revealing the methods of their commission, knowing the tricks of criminals, and much more necessary for effective crime investigation.

To train criminology specialists with such knowledge and skills, it is primarily necessary to study not only the fundamental theoretical and methodological issues of criminology, criminal law, and criminal procedure but also the main problems of all parts of criminology, the basics of operational–search activity, issues of interaction, the use of special knowledge, and data from information centers of law enforcement agencies.

At the same time, lectures and classes should be designed in such a way as to encourage students to creatively solve criminological tasks, contribute to the formation of a broad legal and criminological outlook, awaken their interest in creative problem–solving in investigations, and use the recommendations of all structural parts of criminology, especially in interaction with operatives and various specialists.

If the investigator does not acquire sufficient practical skills in applying all the means of forensic investigative techniques during their university education but is well–versed in the possibilities of their application and capable of supervising the actions of specialists using these techniques, this may not be the most serious shortcoming in their training. Moreover, forensic literature constantly emphasizes the need to improve forensic support for investigations, meaning ongoing assistance to investigators and forensic experts.

Furthermore, focusing on developing practical skills in investigator training appears to be a simplified approach that does not meet modern requirements for the preparation of forensic specialists. The necessary level of skills in applying fundamental principles of forensic science can only be acquired through practice.

Unfortunately, the preparation of investigators does not always follow this approach, often placing more emphasis on developing isolated practical skills in forensic activities (usually without much success but with a considerable expenditure of study hours) rather than fostering a creative attitude toward forensic recommendations, an inclination for intellectual, search–analytical activities, and the ability to consider all the features of each investigated crime. This should be done in close and skillful cooperation with the actions of specialists and operational search officers.

The absence of a genuinely creative approach to investigations, the inability to interact correctly with operational search agencies, and the failure to use data from law enforcement information centers are precisely the shortcomings affecting most of today's investigators.

To determine which areas of forensic knowledge are particularly necessary for investigative specialists and how the systematic courses of forensic science should be taught, it is first necessary to understand the correlation between the concepts of the system of forensic science as a discipline and the system of forensic science as an academic course. These are different yet closely related concepts.

The system of forensic science as a discipline consists of a set of its component parts, united by an internal content unity determined by the objects of study and interconnected in an inseparable organic structure that reflects the overall structure of this science. As is known, this system has developed from the four parts previously mentioned. It should be noted that the system of any science, including forensic science, cannot be created or fundamentally changed overnight. The system of forensic science is the result of the long–term development of the science and possesses considerable stability over time. However, this does not mean that it cannot be improved.

On the other hand, the system of the forensic science academic course, based on the system of forensic science, is more flexible, subject to didactic interpretation, and relatively easily adaptable to modern life, innovations in higher legal education, the crime–fighting environment, and the specifics of the higher educational institution where forensic science is taught.

Therefore, the system of the forensic science academic course, and consequently the curriculum in each law school preparing broad–profile lawyers, as well as in specialized departmental legal institutions (such as the Police Academy of the Ministry of Internal Affairs of the Republic of Azerbaijan and the Heydar Aliyev Academy of the State Security Service of the Republic of Azerbaijan), not only can but must have its own justified and necessary specificity, taking into account various factors.

However, when addressing issues of improving the system of the forensic science academic course and developing it based on the curriculum, it is necessary each time to ensure that the proposed innovations do not contradict the existing system of science, do not disrupt its structure, and guarantee the study of the fundamentals of all its structural parts.

As is known, the adjustment of the curriculum and programs can be diverse. Thus, the specific adjustment of the curriculum and educational programs aimed at the targeted training of investigators, inquirers, and operational–search workers should also be carried out within the framework of the forensic science system and should mainly consist of the appropriate selection of topics on investigation methodology, forensic tactics, and especially the specific topics of special courses. In training on topics dedicated to investigation methodology, emphasis should be placed on the methodology of investigating crimes «hot on the trail».

In the preparation of forensic experts, such specificity should obviously be reflected in the topics of forensic techniques, forensic tactics, and the content of special courses. Regarding the question of where to start studying forensic science, the majority of forensic science teachers are unanimous. They believe that since criminal procedure and criminal law have a basic, fundamental nature in relation to forensic science, its study (including technical and forensic issues) should be preceded by the student’s mastery of the main provisions of these sciences. In this case, the beginning of forensic science studies and the completion of criminal procedure studies may coincide in time.

However, some forensic experts, based on the fact that forensic information about the investigated crime objectively serves as the starting point for making not only

forensic but also procedural and criminal law decisions, consider forensic science to be, to a certain extent, the basic informational foundation for the aforementioned sciences. Therefore, they believe that its study can be conducted in the early courses.

The assertion that forensic information on the case is primary is correct, but the opinion about its fundamental role is quite controversial. After all, primary and any other information by forensic means without knowledge of criminal procedure and criminal law and outside the framework of criminal procedural norms cannot be properly and purposefully collected, evaluated, and used in the interests of the investigation. Consequently, it is impossible to speak about the basic informational role of forensic science in relation to the noted sciences without convincing evidence.

For this or another reason, the study of forensic science in some universities begins in the second or third year without knowledge of the fundamental provisions of criminal procedure. Such a practice can hardly be considered successful since in this case, the teaching of forensic science will proceed only by developing students' skills in performing certain practical operations without a proper conscious understanding of the goals and significance of such operations [6, p.231] .

Taking into account the modern requirements for the training of forensic specialists, as well as the certain lag of textbooks and teaching aids due to rapidly changing legislation and the criminal situation in the country, the role of lectures, seminars, practical classes, and independent work of students significantly increases.

It is lectures and classes that should primarily contribute to the formation of a broad forensic outlook in students, a creative approach to solving procedural and forensic tasks, and the creative, rather than template, application of forensic recommendations. The changes occurring in the country should also be taken into account and analyzed during teaching.

A significant role in such training of specialists is played by the wide and appropriate use of all modern teaching tools (video films, computer technologies, role–playing, business games, active discussions, round tables, and other teaching technologies depending on its goal, form, type, and level). During teaching, it is advisable to more actively use techniques that create situations provoking students to freely express their opinions on the discussed issues and contribute to the formation of reasoning skills in a reflective way not only for themselves but also for the opposing side. It is very important to ensure the involvement of all students in the group (in one form or another) in the discussion of the raised issue.

It is necessary to skillfully select problematic questions and put them up for group discussion, expanding the potential of each question as much as possible, even if it can be answered with a yes or no. It is desirable to practice techniques of collective brainstorming of these questions during group discussions to develop at least basic skills in analyzing available information in problematic work situations of the investigation (for example, interaction between investigators and operational workers within the framework of the investigative–operational group or investigative brigade). According to teaching practice, all this develops the creative potential of forensic specialists.

It is necessary to think about how to make the most rational use of the time allocated for independent work of students. Thoughtful organization of industrial and especially pre–diploma practice, the work of scientific and practical student circles, and scientific supervision of the preparation of term papers and theses by students on relevant topics also significantly help to solve the specified task.

Proper forensic training can also be facilitated by the creation of educational and scientific–practical complexes by departments on a contractual basis with interested law enforcement agencies, where the opportunities and potential of the university and the mentioned bodies would be used.

As the experience of the Department of Forensic Science of the Law Faculty of Baku State University (BSU) shows, scientific and practical conferences summarizing students' scientific activities also serve these goals. Such conferences are held annually at BSU. They show that students specializing in the department in their speeches often demonstrate elements of a serious creative approach to studying forensic science.

The teaching of forensic science at Baku State University (BSU), as well as in departmental specialized law universities of the Republic of Azerbaijan, is mainly built on the desire to form in students a broad forensic outlook and the need for a creative approach to solving procedural and forensic tasks in various typical forensic situations.

Of course, as far as possible, the department's teachers teach students elementary skills of practical investigative work. However, having received good theoretical and special training at the department, graduates of the faculty (according to reviews of the heads of practical bodies) quickly enough master other necessary skills and successfully perform the functions of an investigator.

Currently, there are three levels of higher legal education in our country: 4–year, preparing a Bachelor of Jurisprudence; 5–year, graduating a certified specialist lawyer (in departmental specialized law universities); 6–year, preparing a Master of Jurisprudence. A Bachelor of Jurisprudence, in our opinion, can work as an investigator if he has studied forensic science in the full hourly and thematic volume of the general course taught at the second (5–year) level of education, using the previously mentioned modern technologies of regular teaching and the necessary material and technical base. Naturally, he is less prepared for investigative work than a specialist lawyer, but with such preparation, the basic forensic knowledge necessary for it should be present in the bachelor [5].

Certified specialist lawyers who choose investigative, operational, or forensic expert work as their profession, along with the general course of forensic science (in the required standard volume and using all necessary teaching technologies), must necessarily undergo additional specialized training at the department in departmental specialized law universities (in the form of special courses). Therefore, they are usually better prepared than bachelors for investigative, operational work, or expert–forensic activities.

Especially wide opportunities for deep specialization in the field of forensic science are created by master's training. Lawyers–masters of jurisprudence in the

forensic profile of training within 2 years undergo additional advanced general theoretical and specialized training not only in forensic science but also in other disciplines of the criminal law cycle. Therefore, they possess knowledge that allows them to engage in both investigative and scientific–research activities or work in law enforcement agencies in positions requiring sufficiently high professional forensic training. The specificity of master's training lies in the fact that it usually has a purely individual («piece») character with greater creative freedom in teaching methods [6, p. 294] .

The list and content of special courses in forensic science for the training of specialists and masters should be determined by the graduating department, taking into account the targeted forensic orientation of graduates, the peculiarities of the corresponding region, and the staffing and material–technical capabilities of the departments. Recommended lists of special courses may be used in this case. However, they must necessarily include special courses on the tactics of inspection, crime scene examination, on the tactics and methodology of interaction between investigators and operational–search workers, including issues of forensic examination, and on the methodology of investigating the most dangerous crimes.

Undoubtedly, the level of training of forensic specialists largely depends on the material and technical base. However, currently, for example, civilian universities training lawyers, certified specialists of a broad profile, are in a more difficult situation than departmental universities of the Republic of Azerbaijan. Each university tries to solve this problem taking into account the prevailing circumstances, without relying too much on state support.

References:

1. Sarijalinskaya K., Movsumov D. Criminalistic tenniques: textbook [Sarijalinskaya K., Mövsümov D. Kriminalistika texnikası: dərslik]. Baku, 1975, 178 p.
2. Criminalistics: textbook [Kriminalistika, dərslik]. Ed. By K.Sarijalinskaya. Baku, 1999, 548 p.
3. Criminalistics: textbook [Kriminalistika, dərslik]. Ed. By D.Suleymanov, Baku. 2000, 732 p.
4. Aliyev B., Makhmudov A. Criminalistics: schemes, commentaries, terms. Baku, 2003, 278 p.
5. Law of the Republic of Azerbaijan «On Education», 2011.
6. Aliyev B. Special legal fight against terrorism: criminalistic and operational–search aspects (monograph). Baku, «Chirag» publishing house, 2017, 344 p. (Əliyev B. Terrorçuluğa qarşı xüsusi hüquqi mübarizə: kriminalistik və əməliyyat–axtarış aspektləri (monoqrafiya). Bakı, «Çıraq» nəşriyyatı, 2017, 344 s.)

DOI https://doi.org/10.32837/11300.33525

Cataraga Olga
Doctor în ştiinţe juridice, formator la Institutul Naţional al Justiţiei,
director al Centrului Naţional de Expertize Judiciare al Ministerului Justiţiei,
Chişinău, Republica Moldova
ORCID: https://orcid.org/0000-0003-4257-8049
e–mail: olga.cataraga@justice.gov.md

VIITORUL EXPERŢIZEI JUDICIARE ÎN REPUBLICA MOLDOVA ŞI ÎN SPAŢIUL EUROPEAN

Articolul analizează viitorul expertizei judiciare în Republica Moldova în contextul digitalizării, al utilizării inteligenței artificiale și al alinierii la standardele europene. Textul urmărește să evidențieze modul în care transformarea tehnologică modifică evaluarea probelor, organizarea activității expertale și cerințele de modernizare a cadrului normativ și instituțional. Sunt relevate avantajele instrumentelor digitale și ale tehnologiilor Big Data, în special reducerea duratei examinării și sporirea preciziei concluziilor, concomitent cu necesitatea validării științifice a metodelor și a verificării continue a fiabilității software–ului. Articolul subliniază că utilizarea inteligenței artificiale în domeniul judiciar implică riscuri ridicate, astfel încât algoritmii opaci nu pot constitui temei exclusiv pentru concluziile expertale, iar controlul uman trebuie menținut permanent. De asemenea, sunt prezentate standardizarea procedurilor și acreditarea laboratoarelor conform ISO/IEC 17025, ISO/IEC 17020 și orientărilor ENFSI ca premise ale credibilității, cooperării judiciare și recunoașterii transfrontaliere a rezultatelor expertale. Concluzia autorului este că modernizarea expertizei judiciare trebuie să combine tehnologia cu rigoarea științifică, independența profesională și formarea continuă a expertului, pentru a garanta protecția drepturilor fundamentale și compatibilitatea sistemului moldovenesc cu exigențele justiției europene.

Cuvinte–cheie: expertiză judiciară, digitalizare expertiză judiciară; digitalizare; inteligență artificială; criminalistică digitală; acreditarea laboratoarelor; standarde ISO/ENFSI; Republica Moldova.

Kataraga Olga
Doctor of Law, Director of the National Center of Judicial Expertise,
Ministry of Justice,
Chisinau, Republic of Moldova

THE FUTURE OF JUDICIAL EXPERTISE IN THE REPUBLIC OF MOLDOVA AND IN THE EUROPEAN AREA

The article analyzes the future of forensic expertise in the Republic of Moldova in the context of digitalization, the use of artificial intelligence, and alignment with European standards. It seeks to show how technological transformation reshapes

evidence assessment, the organization of expert work, and the need to modernize the legal and institutional framework. The text highlights the benefits of digital tools and Big Data technologies, especially shorter examination times and greater precision of conclusions, together with the need for scientific validation of methods and continuous verification of software reliability. The article emphasizes that the use of artificial intelligence in the judicial field entails high risks, so opaque algorithms cannot serve as the exclusive basis for expert conclusions and human oversight must be maintained at all times. It also presents the standardization of procedures and the accreditation of laboratories under ISO/IEC 17025, ISO/IEC 17020, and ENFSI standards as prerequisites for credibility, judicial cooperation, and cross–border recognition of expert results. The author concludes that the modernization of forensic expertise must combine technology with scientific rigor, professional independence, and the expert's continuous training in order to safeguard fundamental rights and ensure the compatibility of Moldova's system with the requirements of European justice.

Keywords: Forensic expertise; digitalization; artificial intelligence; digital forensics; laboratory accreditation; ISO/ENFSI standards; Republic of Moldova

Expertiza judiciară reprezintă unul dintre cele mai importante instrumente de susținere a actului de justiție contemporan. Evoluția tehnologiilor informaționale, creșterea volumului de date și apariția noilor forme de criminalitate au determinat transformarea profundă a practicii expertale. În prezent, metodele empirice clasice sunt completate de algoritmi de analiză, instrumente digitale și sisteme automatizate capabile să proceseze volume considerabile de informații într–un timp redus.

Această transformare este esențială și pentru Republica Moldova, unde presiunea asupra sistemului de expertiză judiciară este în continuă creștere. În lipsa unor mecanisme moderne de gestionare și analiză a probelor, există riscul diminuării eficienței și credibilității actului de justiție. În acest context, viitorul expertizei judiciare depinde de capacitatea instituțiilor de a integra tehnologii moderne fără a compromite principiile fundamentale ale independenței și imparțialității expertului judiciar [1, p. 12].

Integrarea tehnologiilor digitale în activitatea de expertiză judiciară a modificat atât procedurile tehnice, cât și paradigma metodologică a evaluării probelor. Sistemele informatice moderne permit procesarea automată a datelor, compararea caracteristicilor și identificarea unor corelații imposibil de observat prin metode tradiționale.

În criminalistica digitală, expertul judiciar gestionează astăzi probe provenite din cloud computing, dispozitive inteligente, active virtuale și rețele informatice globale. Utilizarea tehnologiilor Big Data contribuie la reducerea timpului de examinare și la creșterea gradului de precizie a concluziilor. Totodată, această evoluție generează obligația validării științifice a metodelor utilizate și a verificării continue a fiabilității software–ului aplicat [3, p. 25].

Pentru Republica Moldova, digitalizarea expertizei judiciare trebuie privită drept un obiectiv strategic. Implementarea sistemelor moderne de management al probelor și

a platformelor electronice de gestiune poate reduce considerabil riscul depășirii termenelor procesuale și poate contribui la sporirea eficienței instituțiilor expertale.

Inteligența Artificială (IA) reprezintă una dintre cele mai importante direcții de dezvoltare ale expertizei judiciare moderne. Algoritmii de analiză automată sunt capabili să proceseze volume enorme de informații și să identifice tipare complexe într–un timp foarte scurt. În expertiza digitală și financiară, aceste instrumente permit detectarea conexiunilor dintre persoane, tranzacții și fluxuri informaționale ascunse.

Cu toate acestea, utilizarea IA în justiție implică riscuri semnificative. Regulamentul european privind Inteligența Artificială clasifică sistemele utilizate în domeniul judiciar ca fiind de «risc înalt», ceea ce impune condiții stricte privind transparența și controlul uman [5, p. 7]. Algoritmii de tip «black box», a căror logică nu poate fi explicată, nu trebuie să constituie fundament exclusiv pentru concluziile expertale.

Expertul judiciar trebuie să rămână factorul central al procesului de interpretare a datelor. Responsabilitatea profesională și juridică pentru concluziile formulate aparține exclusiv expertului, iar tehnologia trebuie utilizată doar ca instrument auxiliar. Automatizarea excesivă poate genera erori judiciare grave, în special atunci când rezultatele generate de software sunt acceptate fără analiză critică.

Credibilitatea expertizei judiciare moderne depinde în mod direct de standardizarea procedurilor și acreditarea laboratoarelor conform normelor internaționale ISO/IEC 17025 și ISO/IEC 17020. Aceste standarde garantează faptul că activitatea laboratoarelor se desfășoară în condiții controlate, prin utilizarea unor metode validate și reproductibile [6, p. 9].

Rapoartele internaționale NRC și PCAST au demonstrat că metodele expertale insuficient validate pot conduce la erori judiciare și la contestarea concluziilor în instanță [3, p. 41; 4, p. 52]. Din această perspectivă, acreditarea nu reprezintă doar o formalitate administrativă, ci o garanție a protecției drepturilor fundamentale și a legalității procesului judiciar.

Pentru Republica Moldova, extinderea acreditării laboratoarelor și armonizarea metodologiilor cu standardele ENFSI constituie o condiție indispensabilă pentru integrarea în Spațiul European de Științe Criminalistice. Totodată, standardizarea contribuie la consolidarea cooperării judiciare internaționale și la recunoașterea transfrontalieră a rezultatelor expertale.

În contextul transformării digitale, expertul judiciar nu își pierde relevanța profesională, ci dimpotrivă, devine principalul garant al validității și fiabilității concluziilor științifice. Rolul său depășește simpla utilizare a instrumentelor tehnice și presupune evaluarea critică a rezultatelor generate de algoritmi și software specializat.

Un risc major al epocii digitale îl reprezintă dependența excesivă de automatizare. Așa–numitul «bias de automatizare» poate determina acceptarea necritică a rezultatelor generate de sistemele informatice. Din acest motiv, expertul trebuie să posede competențe interdisciplinare care să combine cunoștințele juridice, tehnice și metodologice.

Independența profesională a expertului trebuie protejată prin mecanisme instituționale și normative clare. Expertul judiciar nu reprezintă interesele uneia dintre părți, ci servește exclusiv adevărului științific și obiectivității procesului judiciar. În acest sens, formarea profesională continuă și dezvoltarea competențelor digitale devin elemente indispensabile ale profesiei.

Viitorul expertizei judiciare în Republica Moldova depinde de capacitatea sistemului expertal de a integra tehnologiile digitale și de a menține, în același timp, controlul uman asupra procesului de analiză și interpretare a probelor. Modernizarea instituțională, digitalizarea proceselor și acreditarea conform standardelor internaționale reprezintă direcții esențiale pentru consolidarea credibilității actului de justiție.

Inteligența Artificială și instrumentele digitale trebuie privite ca mecanisme de sprijin al activității expertului judiciar, nu ca substituenți ai raționamentului uman. Numai prin îmbinarea tehnologiei cu rigoarea științifică și independența profesională poate fi garantată protecția drepturilor fundamentale și realizarea unui act de justiție echitabil.

În perspectiva integrării europene, Republica Moldova trebuie să accelereze armonizarea cadrului normativ și instituțional cu standardele ENFSI și ISO, pentru a crea un sistem expertal modern, transparent și compatibil cu exigențele contemporane ale justiției europene.

Lista Sursei Utilizate:

1. Republica Moldova. Legea nr. 68 din 14.04.2016 cu privire la expertiza judiciară și statutul expertului judiciar. Chișinău, 2016.
2. Republica Moldova. Hotărârea Guvernului nr. 441 din 16.06.2017 pentru aprobarea Regulamentului privind Centrul Național de Expertize Judiciare. Chișinău, 2017.
3. National Research Council. Strengthening Forensic Science in the United States: A Path Forward. Washington, 2009.
4. PCAST. Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature–Comparison Methods. Washington, 2016.
5. Council of the European Union. Council Conclusions on the Action Plan for the European Forensic Science Area 2.0. Brussels, 2023.
6. ILAC. ILAC–G19:06/2022 Modules in a Forensic Science Process. New South Wales, 2022.
7. ENFSI. Policy on Accreditation and Maintaining of Accreditation. Wiesbaden, 2025.

DOI https://doi.org/10.32837/11300.33430

Аркуша Лариса
доктор юридичних наук, професор,
завідувач кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–0422–6416
E–mail: larisa_arkusha@ukr.net

ТЕОРЕТИКО–МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РОЗСЛІДУВАННЯ ДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ

В тезах проаналізовано вплив ШІ на трансформацію організованої злочинності та роботу слідчих. Розглянуто «розрив швидкостей» між злочинцями та правоохоронцями. Досліджено правові засади застосування ШІ згідно з EU AI Act, проблеми доказування, алгоритмічну упередженість та необхідність розвитку експертиз на базі пояснюваного ШІ.

Ключові слова: штучний інтелект, цифрові докази, аналіз соціальних мереж, розслідування, злочин, судова експертиза, організовані злочинні угруповання.

Arkusha Larysa
Doctor of Law, Professor,
Head of the Department of Criminalistics, Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF THE USE OF ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF ORGANIZED CRIMINAL GROUPS

The theses analyze the impact of AI on the transformation of organized crime and the work of investigators. The «speed gap» between criminals and law enforcement is examined. The paper explores the legal framework for AI application under the EU AI Act, evidentiary issues, algorithmic bias, and the need for developing forensics based on explainable AI.

Key words: artificial intelligence, digital evidence, social network analysis, investigation, crime, forensic science, organized crime groups.

Стрімке впровадження технологій штучного інтелекту в різні сфери життєдіяльності людини докорінно трансформує архітектуру сучасної

злочинності, висуваючи безпрецедентні виклики перед органами досудового розслідування та судовими експертами. Організовані злочинні угруповання (ОЗУ) дедалі частіше відмовляються від жорстких ієрархічних моделей на користь гнучких, децентралізованих цифрових мереж, що функціонують у транскордонному віртуальному просторі. За таких умов традиційні криміналістичні методи виявляються малоефективними, оскільки електронні докази – листування у шифрованих месенджерах, транзакції у блокчейн–мережах, дані геолокації та записи інтелектуальних систем відеоспостереження – сьогодні становлять основу доказової бази у кожному другому кримінальному провадженні.

Проблема ускладнюється виникненням так званого «розриву швидкостей» між технологічним оснащенням транснаціональних кримінальних синдикатів та можливостями державних правоохоронних інституцій. Маючи у своєму розпорядженні значні фінансові ресурси, організована злочинність оперативно залучає провідних фахівців у галузі комп'ютерних наук та блокчейну, отримуючи доступ до передових інструментів автоматизації кримінальних процесів значно раніше за органи державної влади. Водночас рівень загальної кібербезпеки в державному та приватному секторах залишається незадовільним. За результатами окремих досліджень, близько 70% українських компаній у 2024 році не здійснювали інвестицій у кібербезпеку [4], що свідчить про низький рівень кіберзахисту бізнес–середовища (водночас такі дані мають обмежений характер, оскільки базуються на вибіркових опитуваннях і не відображають повною мірою реальну існуючу ситуацію у всіх секторах економіки). Це створює сприятливе середовище для масштабних кібератак та цифрового шахрайства.

У зв'язку з цим виникає об'єктивна потреба в інтенсифікації використання ШІ правоохоронними органами для обробки великих масивів інформації, подолання ризику «інформаційного перевантаження» та прогнозування злочинної діяльності. Проте впровадження алгоритмічних систем у сферу кримінального судочинства потребує ретельного теоретичного обґрунтування та розв'язання низки процесуальних проблем, пов'язаних із забезпеченням допустимості доказів, усуненням алгоритмічної упередженості та захистом фундаментальних прав людини.

Теоретико–правові та практичні засади інтеграції штучного інтелекту в криміналістичну науку та практику досудового розслідування досліджували у своїх працях як вітчизняні, так і зарубіжні автори. Загальні перспективи та ризики застосування технологій штучного інтелекту у криміналістиці висвітлено у наукових розвідках Д. Черваньової та О. Курман [11, С. 211–215]. Питання впровадження штучного інтелекту у кримінальне провадження з урахуванням необхідності дотримання процесуальних гарантій та збереження контролю людини над прийняттям рішень обґрунтовано у працях А. Піддубної та К. Божук [7, С. 234–238]. Окремі аспекти використання інтелектуальних систем у виявленні та аналізі злочинної діяльності, зокрема у сфері цифрових доказів, досліджувалися

О. Шевчуком та Н. Моргун [6, С. 95–100]. На особливу увагу заслуговують праці Г. Кучинської, присвячені розвитку цифрової криміналістичної експертизи та застосуванню штучного інтелекту в експертній діяльності [5, С. 126–131].

Водночас питання процесуального забезпечення допустимості цифрових доказів, отриманих за допомогою алгоритмів ШІ, в умовах вітчизняного кримінального процесу та прецедентної практики Європейського суду з прав людини (ЄСПЛ) залишаються дискусійними і потребують додаткової систематизації.

Для формування єдиного наукового підходу необхідно чітко визначити сутність ШІ в межах правового поля України. Згідно з Концепцією розвитку штучного інтелекту в Україні, схваленою розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556–р [9], штучний інтелект визначається як організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів, досліджень і алгоритмів обробки інформації. Реалізація зазначеної Концепції, розрахована на період до 2030 року, передбачає створення сприятливих умов для використання ШІ в пріоритетних галузях економіки та державного управління. Цей курс було деталізовано у Концепції Державної цільової науково–технічної програми з використання технологій штучного інтелекту на період до 2026 року, схваленій розпорядженням Кабінету Міністрів України від 13 квітня 2024 р. № 320–р. [8], яка спрямована на системне впровадження технологій штучного інтелекту у наукову, економічну та безпекову діяльність держави.

У контексті міжнародно–правових стандартів ключовим орієнтиром для адаптації національного законодавства є Регламент Європейського Парламенту і Ради (ЄС) 2024/1689 від 13 червня 2024 року про встановлення гармонізованих правил щодо штучного інтелекту (EU AI Act), який набрав чинності 1 серпня 2024 року [10]. Цей документ визначає ШІ як машинобудовану систему, розроблену для функціонування з різними рівнями автономності, яка може демонструвати адаптивність після розгортання та генерувати вихідні дані (прогнози, рекомендації або рішення), що впливають на фізичне чи віртуальне середовище.

Регламент запроваджує ризик–орієнтований підхід, класифікуючи системи ШІ за чотирма рівнями ризику. Сфера правоохоронної діяльності підпадає під дію найсуворіших обмежень. Зокрема, з 2 лютого 2025 року Регламентом повністю заборонено використання систем ШІ, що несуть неприйнятний ризик для фундаментальних прав громадян [1].

Окрему процесуальну складність становить використання дозволених систем дистанційної біометричної ідентифікації (RBI) в реальному часі за винятковими обставинами. Відповідно до статті 5(1)(h) EU AI Act, таке застосування можливе лише за наявності попереднього дозволу судового органу (або незалежного адміністративного органу за умови підтвердження судом протягом 24 годин в екстрених випадках), обов’язкового проведення

фундаментальної оцінки впливу на права людини (FRIA) згідно зі статтею 27 та реєстрації системи в офіційній базі даних ЄС (стаття 71). При цьому застосування ШІ–технологій правоохоронними органами має будуватися на неухильному дотриманні принципів законності, справедливості, прозорості та обмеження цілей збору даних.

Розвиток інструментів генеративного ШІ після виходу моделі ChatGPT у листопаді 2022 року кардинально змінив тактичний арсенал ОЗУ. Маючи значний фінансовий потенціал, кримінальні мережі успішно впроваджують інноваційні моделі злочинного бізнесу, що дозволяє низькокваліфікованим кіберзлочинцям отримувати доступ до високотехнологічних інструментів проведення атак, що значно розширює коло потенційних зловмисників.

За даними Оцінки загроз серйозній та організованій злочинності в ЄС (EU–SOCTA 2025 [2]) та Оцінки загроз інтернет–організованій злочинності (IOCTA 2026 [3]), підготовлених Європолом, найшвидше зростаючим сегментом організованої злочинності є кібершахрайство. Тільки в межах ЄС сукупні збитки від таких схем у 2025 році сягали десятків мільярдів доларів США. При цьому штучний інтелект суттєво підвищує ефективність таких злочинів, забезпечуючи масштабованість, автоматизацію та персоналізацію шахрайських кампаній. Організовані злочинні угруповання дедалі активніше інтегрують цифрові інструменти, перетворюючи кіберзлочинність на високоприбуткову індустрію.

Крім того, технічний інструментарій сучасних ОЗУ включає: інтегровані програмно–апаратні комплекси, керовані алгоритмами ШІ, які дозволяють автоматично генерувати й надсилати тисячі повідомлень та здійснювати масові дзвінки з метою викрадення персональних даних, функціонуючи як транснаціональні ланцюги постачання; портативні технічні засоби, які імітують вишки мобільного зв’язку для несанкціонованого підключення мобільних пристроїв жертв та перехоплення трафіку й конфіденційної інформації; програми–вимагачі, де ШІ використовується для автоматичного сканування цифрових ланцюгів постачання, виявлення вразливостей і психологічного тиску на жертв без шифрування даних; автономні ШІ–агенти, здатні самостійно, без участі людини–оператора, вести повний цикл кримінальної діяльності – від пошуку вразливості системи до відмивання викрадених коштів через криптовалютні міксери.

Найбільш гострою доктринальною та практичною проблемою використання ШІ у кримінальному процесуальному доказуванні є проблема «чорної скриньки». Оскільки алгоритми глибокого навчання оперують мільйонами нелінійних параметрів у багатовимірних просторах, ні слідчий, ні прокурор, ні сторона захисту чи суддя не можуть простежити логіку формування кінцевого висновку машини. Це нівелює засади безпосередності дослідження доказів та обмежує право обвинуваченого на ефективний захист і справедливий судовий розгляд.

Перспективи подальших наукових досліджень полягають у розробці детальних методичних рекомендацій щодо проведення судових цифрових експертиз із використанням пояснюваного штучного інтелекту, а також у

створенні вітчизняного спеціалізованого програмного забезпечення кримінального аналізу, адаптованого до вимог кримінального процесуального законодавства України.

Перелік використаних джерел:

1. European Commission. AI Act: Regulatory framework for artificial intelligence. Shaping Europe's digital future. 2025. URL: https://digital–strategy.ec.europa.eu/en/policies/regulatory–framework–ai.

2. Europol. European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime (EU–SOCTA 2025). Luxembourg : Publications Office of the European Union, 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU–SOCTA–2025.pdf.

3. Europol. The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026. Luxembourg: Publications Office of the European Union, 2026. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA–2026.pdf.

4. Кібератаки на бізнес України 2025: нові вектори загроз та захист. URL: https://synchron.ua/cyberattacks–on–ukrainian–business–2025–uk/.

5. Кучинська Г. Аналіз та оцінка доказів штучним інтелектом у кримінальному процесі. Судова експертиза. 2025. № 1. С. 126–131. DOI: https://doi.org/10.32782/forensic.science.2025.1.17. URL: https://journal.srcif.com.ua/index.php/main/article/view/20

6. Моргун Н.С., Шевчук О.О. Використання штучного інтелекту в оперативно–розшуковій діяльності. Аналітично–порівняльне правознавство. 2026. Т. 3, № 1. С. 95–100. URL: https://app–journal.in.ua/wp–content/uploads/2026/02/17–2.pdf DOI: https://doi.org/10.24144/2788–6018.2026.01.3.15 .

7. Піддубна А. В., Божук К. О. Штучний інтелект у кримінальному провадженні: сучасні виклики та правові перспективи. Аналітично–порівняльне правознавство. 2025. Т. 3. № 5. С. 234–238. URL: https://journal–app.uzhnu.edu.ua/article/view/342787. DOI: https://doi.org/10.24144/2788–6018.2025.05.3.36.

8. Про схвалення Концепції Державної цільової науково–технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : розпорядження Кабінету Міністрів України від 13.04.2024 № 320–р. URL: https://zakon.rada.gov.ua/laws/show/320–2024–р#Text .

9. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556–р. URL: https://zakon.rada.gov.ua/laws/show/1556–2020–р.#Text.

10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial

Intelligence Act). Official Journal of the European Union. 2024. URL: https://eur–lex.europa.eu/eli/reg/2024/1689/oj.

11. Черваньова Д.А., Курман О.В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. Аналітично–порівняльне правознавство. 2025. Т. 3, № 3. С. 211–215. URL: https://journal–app.uzhnu.edu.ua/article/view/334719/323667 DOI: https://doi.org/10.24144/2788–6018.2025.03.3.31

DOI https://doi.org/10.32837/11300.33431

Басалюк Наталія
доктор філософії з галузі знань 08 – «Право», провідний фахівець науково–дослідної частини, доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–2429–6964
e–mail: basalyk@ukr.net

ЦИФРОВІ ТА СУДОВО–ЕКСПЕРТНІ ДОКАЗИ У ПРОЦЕДУРІ ЕКСТРАДИЦІЇ ОСІБ: ОКРЕМІ АСПЕКТИ

У тезах досліджено сучасні тенденції трансформації процедури екстрадиції у механізм міжнародного кримінального процесуального доказування. Проаналізовано роль цифрових, криміналістичних та судово–експертних доказів у міжнародному розшуку та екстрадиції осіб, особливості використання електронних доказів, результатів негласних слідчих (розшукових) дій і судових експертиз у провадженнях щодо транснаціональних економічних та корупційних злочинів.

Ключові слова: екстрадиція, міжнародне кримінальне співробітництво, міжнародний розшук, цифрові докази, електронні докази, криміналістичне забезпечення, судова експертиза, судово–експертні докази.

Basalyuk Natalia
PhD in Law (Field of Knowledge 08 – Law),
Senior Specialist at the Research Department,
Associate Professor at the Department of Criminalistics, Forensic Expertise and Polygraphology, National University «Odesa Law Academy»,
Odesa, Ukraine

DIGITAL AND FORENSIC EVIDENCE IN EXTRADITION PROCEDURES: SELECTED ASPECTS

The theses examine current trends in the transformation of extradition into a mechanism of international criminal procedural proof. The role of digital, criminalistic, and forensic evidence in international search and extradition procedures is analyzed, along with the use of electronic evidence, covert investigative measures, and forensic examinations in cases involving transnational economic and corruption crimes.

Key words: extradition, international criminal cooperation, international search, digital evidence, electronic evidence, criminalistic support, forensic examination, forensic evidence.

Сучасний розвиток транснаціональної злочинності, цифровізація суспільних відносин та активізація міжнародного кримінального співробітництва держав зумовлюють суттєву трансформацію інституту екстрадиції. У XXI столітті екстрадиція поступово виходить за межі класичного розуміння міждержавної процедури передачі особи для кримінального переслідування або виконання вироку та набуває ознак складного механізму міжнародного кримінального процесуального доказування. Якщо раніше ефективність екстрадиції переважно залежала від наявності міжнародно–правових підстав видачі особи та формального дотримання процедурних вимог, то сучасний етап розвитку кримінального провадження свідчить про істотне зростання ролі доказів криміналістичного та судово–експертного характеру, які фактично визначають можливість міжнародного розшуку особи, обґрунтованість екстрадиційного запиту та перспективи подальшого кримінального переслідування.

Екстрадиція за своєю правовою природою є комплексним міжгалузевим інститутом, що функціонує на перетині міжнародного, кримінального та кримінального процесуального права. У сучасних умовах її зміст охоплює не лише передачу особи від однієї держави до іншої, а й складну систему процесуальної перевірки доказової інформації, оцінки ризиків порушення прав людини, встановлення меж кримінального переслідування та аналізу достатності доказів для міжнародного співробітництва. Саме тому сучасна процедура екстрадиції дедалі більше трансформується у специфічну форму міжнародного доказування, у межах якої держави фактично здійснюють оцінку належності, допустимості, достовірності та переконливості доказів, отриманих у різних юрисдикціях.

Особливого значення у цих умовах набувають саме докази криміналістичного та судово–експертного характеру. Розвиток цифрових технологій та транснаціональний характер сучасної злочинності зумовили істотне розширення кола доказових джерел, які використовуються у процедурах міжнародного розшуку та екстрадиції. Йдеться, зокрема, про результати комп’ютерно–технічних, економічних, портретних, фоноскопічних, почеркознавчих, лінгвістичних та інших судових експертиз, матеріали негласних слідчих (розшукових) дій, телекомунікаційні дані, цифрові сліди, інформацію з електронних реєстрів, електронне листування, повідомлення у месенджерах, результати аналізу банківських транзакцій та відомості з міжнародних інформаційних систем Interpol і Europol. Саме такі докази дедалі частіше формують основу для оголошення особи у міжнародний розшук, підтвердження її місцезнаходження, встановлення ролей учасників організованої злочинної діяльності та обґрунтування екстрадиційного запиту.

Показовим у цьому контексті є кримінальне провадження щодо заволодіння державним майном та маніпуляцій із договорами державного підприємства аграрного сектору, у межах якого судом досліджувалися численні докази цифрового та криміналістичного характеру. Аналіз встановлених судом фактичних обставин свідчить, що доказування у таких категоріях справ вже не

обмежується дослідженням письмових договорів або показань учасників провадження. Натомість ключове значення набуває комплексний аналіз цифрової комунікації між учасниками, результатів негласних слідчих (розшукових) дій, телекомунікаційних з'єднань, повідомлень у месенджерах, аудіоконтролю та електронної координації дій між особами, причетними до організації злочинної схеми.

Так, у межах зазначеного кримінального провадження [1] суд досліджував зафіксовані результати зняття інформації з транспортних телекомунікаційних мереж, листування у месенджері WhatsApp, цифрові комунікації між учасниками господарських операцій, а також аудіозаписи переговорів щодо погодження договорів, зміни їх умов та координації фінансових розрахунків. Саме ці цифрові докази дозволили встановити фактичний розподіл ролей між учасниками схеми, підтвердити координацію їх дій, виявити приховані механізми управління фінансово–господарською діяльністю та довести обізнаність учасників щодо штучного завищення вартості робіт і маніпуляцій із документацією. Фактично суд здійснював фактично здійснював реконструкцію злочинної схеми на основі аналізу цифрових слідів та електронної взаємодії між учасниками провадження.

Особливого значення набуває і те, що сучасні транснаціональні економічні та корупційні злочини дедалі частіше мають складний цифровий характер. Крім того, особи, підозрювані у вчиненні корупційних чи економічних злочинів, намагаються уникнути кримінальної відповідальності шляхом виїзду за межі держави. У таких випадках ефективність міжнародного переслідування напряму залежить від здатності правоохоронних органів сформувати належний цифровий доказовий масив, придатний для міжнародної процесуальної комунікації та подальшого використання у процедурі екстрадиції.

Про актуальність цієї проблематики свідчить і сучасна практика екстрадиції осіб, підозрюваних у заволодінні державними коштами, незаконному відчуженні земель державної та комунальної власності, участі в організованих корупційних схемах та інших економічних злочинах. Зокрема, у 2025 році з Федеративної Республіки Німеччина в Україну було екстрадовано оцінювачку, обвинувачену у кримінальному провадженні щодо незаконного продажу за заниженою вартістю земельної ділянки комунальної власності площею понад 3 гектари на Закарпатті [2]. За даними слідства, особа за попередньою змовою з іншими учасниками схеми підробила звіт про експертну грошову оцінку земельної ділянки, штучно занизивши її вартість, що призвело до збитків територіальній громаді на суму понад 81 млн грн. Вказане кримінальне провадження є показовим прикладом того, що у сучасних процедурах екстрадиції визначального значення набувають саме докази судово–експертного характеру, оскільки предметом доказування фактично виступають результати оцінювальних, економічних та документознавчих досліджень, які дозволяють встановити механізм штучного заниження вартості майна, обсяг завданих збитків та роль конкретних учасників організованої схеми. Крім того, сама екстрадиція стала можливою завдяки комплексній міжнародній

взаємодії між компетентними органами Німеччини, Польщі, Офісом Генерального прокурора України та українським бюро Interpol, що додатково підтверджує трансформацію екстрадиції у форму міжнародної криміналістичної кооперації.

Водночас розвиток цифрового кримінального провадження породжує нові виклики для процедури екстрадиції. Особливої актуальності набувають питання допустимості електронних доказів, їх автентичності, процесуального порядку отримання та можливості використання доказової інформації, здобутої за межами національної юрисдикції. Крім того, використання цифрових доказів у міжнародному співробітництві вимагає належного рівня криміналістичного та судово–експертного забезпечення, оскільки саме судова експертиза забезпечує перевірку достовірності електронної інформації, встановлення відсутності втручання у цифрові дані та підтвердження їх належності конкретним особам.

У цьому контексті особливого значення набуває принцип подвійної кримінальності, який традиційно виступає гарантією захисту особи від видачі за діяння, що не визнаються злочинними у запитуваній державі. Проте розвиток кіберзлочинності, цифрових фінансових схем та нових форм транснаціональної злочинної діяльності істотно ускладнює застосування цього принципу, оскільки кримінально–правові моделі різних держав не завжди однаково реагують на новітні форми суспільно небезпечної поведінки. Саме тому сучасна міжнародна практика дедалі більше орієнтується не на буквальне співставлення складів злочинів, а на аналіз фактичної сутності діяння та його суспільної небезпечності.

Таким чином, екстрадиція перестає бути виключно технічною процедурою передачі особи між державами та трансформується у складний механізм міжнародного кримінального процесуального доказування, у якому ключову роль відіграють цифрові, криміналістичні та судово–експертні докази. Саме вони забезпечують можливість міжнародного розшуку осіб, доведення їх причетності до організованої злочинної діяльності, обґрунтування екстрадиційних запитів та подальше кримінальне переслідування.

Перелік використаних джерел:

1. Вирок Вищого антикорупційного суду від 11.12.2025 у справі № 991/1307/25, провадження № 1–кп/991/12/25. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/132536122

2. Продаж за безцінь землі на Закарпатті: екстрадовано обвинувачену з Німеччини. Національне антикорупційне бюро 15.09.2025. URL: https://nabu.gov.ua/news/prodazh–za–beztcin–zemli–na–zakarpatti–ekstradovano–obvynuvachenu–z–nimechchyny–1/

DOI https://doi.org/10.32837/11300.33432

Варинський Владислав
кандидат політичних наук, доцент,
доцент кафедри філософії та україністики
Національного університету «Одеська морська академія»
м.Одеса, Україна
ORCID: https://orcid.org/0000–0001–5837–6201
e–mail: vlad.varinskiy@gmail.com

ПРИНЦИП HUMAN OVERSIGHT У КРИМІНАЛЬНІЙ ЮСТИЦІЇ: АДАПТАЦІЯ СТАНДАРТІВ EU AI ACT В УКРАЇНІ

У тезах досліджено адаптацію стандартів EU AI Act до системи кримінальної юстиції України крізь призму принципу human oversight. Обґрунтовано необхідність формування єдиного правового режиму використання високоризикових систем ШІ на всіх етапах кримінального провадження – від діяльності правоохоронних органів до здійснення правосуддя. Доведено, що модель human–in–the–loop є мінімально допустимим стандартом легітимного використання ШІ у кримінальній юстиції, оскільки забезпечує збереження визначального людського контролю, процесуальних гарантій та принципу верховенства права.

Ключові слова: штучний інтелект; високоризикові системи ШІ; human oversight; кримінальна юстиція; EU AI Act; правоохоронні органи; правосуддя.

Varynskyi Vladyslav
Candidate of Political Sciences, Associate Professor;
Associate Professor of the Department of Philosophy and Ukrainian Studies
National University «Odesa Maritime Academy»
Odesa, Ukraine

THE PRINCIPLE OF HUMAN OVERSIGHT IN CRIMINAL JUSTICE: ADAPTATION OF EU AI ACT STANDARDS IN UKRAINE

The theses examine the adaptation of the EU AI Act standards to the criminal justice system of Ukraine through the prism of the principle of human oversight. The study substantiates the necessity of establishing a unified legal framework for the use of high–risk AI systems at all stages of criminal proceedings – from the activities of law enforcement agencies to the administration of justice. It is argued that the human–in–the–loop model constitutes the minimum acceptable standard for the legitimate use of AI in criminal justice, as it ensures the preservation of decisive human control, procedural safeguards, and the principle of the rule of law.

Keywords: artificial intelligence; high–risk AI systems; human oversight; criminal justice; EU AI Act; law enforcement agencies; justice.

Стрімка цифровізація кримінальної юстиції та впровадження систем штучного інтелекту (ШІ) формують новий комплекс правових викликів, пов'язаних із допустимими межами автономізації алгоритмічного прийняття рішень як на стадії досудового розслідування правоохоронними органами, так і в процесі здійснення правосуддя. В умовах інтеграції алгоритмічних систем у діяльність правоохоронних органів, прокуратури та суду забезпечення цілісності кримінальної процедури вимагає формування уніфікованого правового режиму застосування ШІ та єдиних вимог до його прозорості, пояснюваності й контрольованості на всіх етапах кримінального провадження незалежно від суб'єкта використання відповідних технологій.

В умовах повномасштабної війни це питання набуває для України стратегічного значення, зокрема у зв'язку з використанням ШІ для фіксації воєнних злочинів, розпізнавання осіб, аналізу кримінальної розвідки та обробки великих масивів даних (Big Data). Перехід від суто допоміжної обробки інформації до безпосереднього впливу алгоритмічних систем на аналітичне прогнозування, оцінку ризиків і підготовку процесуально значущих рішень актуалізує потребу у формуванні єдиних правових стандартів використання ШІ та посилює значення європейського досвіду нормативного обмеження високоризикових систем.

Сучасна модель регулювання ШІ в Європейському Союзі ґрунтується на ризико–орієнтованому підході, закріпленому в Регламенті (ЄС) 2024/1689 (EU AI Act) [1]. Відповідно до його архітектури системи ШІ, що використовуються у сфері правосуддя та кримінальної юстиції, віднесено до категорії високого ризику. Водночас окремі практики –зокрема дистанційна біометрична ідентифікація (п. e ч. 1 ст. 5), біометрична категоризація (п. g ч. 1 ст. 5) та соціальний скоринг (п. c ч. 1 ст. 5) – визнані несумісними з фундаментальними цінностями ЄС через непропорційне втручання у права людини та ризик масового цифрового нагляду.

Особливу специфіку має регулювання винятків щодо використання ШІ правоохоронними органами у випадках, передбачених пп. i–iii п. h абз. 1 ст. 5 Регламенту, а також обмеження щодо умов застосування та оцінки наслідків такого використання. Так, частина 2 статті 5 визначає оціночні категорії, які безпосередньо впливають на допустимість застосування систем біометринчної ідентифікації у режимі реального часу в загальнодоступних місцях. Оцінка правомірності використання таких систем здійснюється на основі аналізу двох взаємопов'язаних критеріїв:

а) характеру ситуації (ї. «à» ÷. 2 ñò. 5) – з урахуванням серйозності, ймовірності та масштабу потенційної шкоди, яка може настати в разі незастосування систем біометричної ідентифікації в конкретних обставинах;

б) наслідків використання (ї. «b» ÷. 2 ñò. 5) – шляхом оцінки прогнозованого впливу системи ШІ на права, свободи та законні інтереси всіх зацікавлених осіб, зважаючи на серйозність, ймовірність і масштаб таких наслідків.

Щодо високоризикових систем ШІ EU AI Act встановлює не лише критерії їх оцінки, а й комплекс спеціальних вимог до контрольованого використання таких технологій у межах цілісної моделі кримінальної юстиції. AI Act визначає загальні критерії віднесення систем ШІ до високоризикових у ст. 6, відповідно до якої такими визнаються системи, що створюють значну загрозу здоров'ю, безпеці або основоположним правам людини, зокрема у зв'язку з ризиком дискримінації, свавільного втручання у приватність чи необґрунтованого обмеження прав особи. Саме це обґрунтовує встановлення підвищених вимог до якості даних, прозорості, людського контролю, простежуваності та систем управління ризиками на всіх етапах використання ШІ – від діяльності правоохоронних органів до здійснення правосуддя.

Подібний суворий підхід європейського законодавця до систем ШІ у сфері правопорядку обумовлений внутрішньою специфікою технології та її безпосереднім впливом на кримінальний процес і правосуддя. Оскільки матеріали, сформовані правоохоронними органами за допомогою алгоритмічних систем, у подальшому можуть набувати статусу процесуальних джерел доказів, особливої деструктивності набуває так званий black box effect. Цей феномен гносеологічної непрозорості ШІ, за якого логіка формування алгоритмічного висновку залишається недоступною для зовнішньої перевірки та інтерпретації, створює спільні виклики як для стадії досудового розслідування, так і для судового розгляду.

Використання подібних «закритих» моделей у кримінальному судочинстві здатне нівелювати принцип належної правової процедури (due process) та право на справедливий суд, гарантоване ст. 6 Конвенції про захист прав людини і основоположних свобод [2]. За таких умов особливої актуальності набуває проблема збереження автономного людського судового розсуду та недопустимості фактичного делегування юридично значущих рішень алгоритмічним системам

Саме тому сучасні правові стандарти пов'язують допустимість використання ШІ у сфері правосуддя з вимогами пояснюваності (explainability), простежуваності (traceability) та обов'язкового людського контролю. Відповідні підходи відображені, зокрема, у Європейській етичній хартії щодо використання ШІ в судових системах (CEPEJ, 2018) [3], яка визначає принцип «під контролем користувача» (under user control) одним із базових орієнтирів функціонування судових ШІ–систем

Водночас це не виключає можливості інтеграції алгоритмічних систем у діяльність суду як допоміжного інструменту аналізу та обробки інформації. Саме тому у правничому середовищі триває дискусія щодо допустимих меж використання ШІ в судочинстві, зокрема у контексті розробки нормативних актів, придатних для машинного зчитування (machine–readable legislation).

Дійсно, завдяки здатності до обробки великих масивів даних ШІ відкриває значні перспективи для оптимізації судочинства. До його очевидних переваг

належать автоматизація рутинних технічних процесів, мінімізація помилок, пов'язаних із людським фактором, швидкий пошук релевантної нормативної бази, аналіз судової практики та акумуляція доказової інформації з відкритих джерел (OSINT).

Водночас межі такого використання чітко окреслені як міжнародними, так і національними етичними стандартами. Так, відповідно до ст. 16 Кодексу суддівської етики [5] використання суддею технологій штучного інтелекту є допустимим лише за умови, що це не впливає на незалежність та неупередженість судді, не стосується оцінки доказів і процесу ухвалення судових рішень та не порушує вимог законодавства. Таким чином, національний підхід остаточно закріплює статус ШІ як допоміжного інструменту, функціонування якого можливе виключно за умов збереження людського контролю та персональної відповідальності судді–людини.

За таких обставин принцип human oversight трансформується з технічного механізму безпеки у фундаментальний критерій легітимності використання штучного інтелекту в кримінальній юстиції. Саме збереження визначального людського контролю дозволяє забезпечити персоналізацію юридичної відповідальності, критичну оцінку алгоритмічних висновків та дотримання базових гарантій верховенства права на всіх етапах кримінального провадження – від діяльності правоохоронних органів до здійснення правосуддя.

У зв'язку з цим ШІ у сфері кримінальної юстиції має функціонувати виключно як допоміжний інструмент підтримки прийняття рішень (decision support system), інтегрований у єдиний процесуальний механізм людського контролю. Використання автономних моделей human–out–of–the–loop у правоохоронній та судовій діяльності суперечить принципам людиноцентричного правопорядку, тоді як концепція human–in–the–loop фактично виступає мінімально допустимою моделлю легітимного застосування високоризикових систем ШІ у кримінальній юстиції.

Проведена оцінка європейських регуляторних трендів та національних правових реалій дає підстави констатувати, що адаптація стандартів EU AI Act в Україні має ґрунтуватися на безкомпромісному дотриманні принципу human oversight на всіх етапах кримінального провадження як єдиного цілісного процесу реалізації кримінальної юстиції.

По–перше, у діяльності правоохоронних органів на стадії досудового розслідування використання високоризикових систем ШІ, зокрема для біометричної ідентифікації чи кримінального прогнозування, має суворо обмежуватися критеріями необхідності й пропорційності та виключати автономні моделі »human–out–of–the–loop».

По–друге, на стадії судового розгляду конституційні імперативи (ст. 127 Конституції України) та стандарти професійної етики (ст. 16 Кодексу суддівської етики) [5] повністю нівелюють можливість надання ШІ статусу суб'єкта владних

повноважень чи самостійної оцінки доказів, остаточно закріплюючи здійснення правосуддя як виключну прерогативу людини.

Відтак, єдиним легітимним стандартом для вітчизняної кримінальної юстиції є модель human–in–the–loop, яка виключає можливість автономного ухвалення юридично значущих рішень алгоритмічними системами та зберігає визначальну роль людини на всіх етапах кримінального провадження.

DOI https://doi.org/10.32837/11300.33435

Гресь Юлія
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія», м. Одеса,
Україна
ORCID: https://orcid.org/0000-0002-8670-9779
e–mail: julia.bayderina@gmail.com

ОСНОВИ ВИКОРИСТАННЯ МЕТОДОЛОГІЇ ПОВЕДІНКОВОГО ПРОФАЙЛІНГУ ТА ЦИФРОВОЇ АНАЛІТИКИ ПІД ЧАС РОЗСЛІДУВАННЯ КОРИСЛИВИХ ЗЛОЧИНІВ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

У тезах доповіді розглянуто основи використання методології поведінкового профайлінгу у поєднанні із засобами цифрової аналітики під час розслідування корисливих кримінальних правопорушень, охарактеризовано трансформацію джерел інформації про особу злочинця в умовах цифровізації та визначено види злочинних дій, унаслідок яких цифрові сліди виникають на етапах підготовки, безпосереднього вчинення і приховування злочину. Обґрунтовано значення комплексного аналізу електронних комунікацій, цифрових профілів, метаданих, транзакційної активності та мережевих зв’язків для встановлення поведінкових закономірностей, формування слідчих версій, виявлення серійності злочинної діяльності й визначення перспективних напрямів досудового розслідування.

Ключові слова: поведінковий профайлінг; криміналістичний профайлінг; цифрова аналітика; корисливі злочини; цифрові сліди; цифровий профіль; транзакційна активність; слідчі версії; досудове розслідування; цифрові трансформації.

Hres Yuliia
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminalistics, Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

FUNDAMENTALS OF USING BEHAVIOURAL PROFILING METHODOLOGY AND DIGITAL ANALYTICS IN THE INVESTIGATION OF PROFIT-MOTIVATED CRIMES UNDER CONDITIONS OF DIGITAL TRANSFORMATION

The conference abstracts examine the fundamentals of applying behavioral profiling methodology in combination with digital analytics tools in the investigation of acquisitive criminal offenses. The transformation of sources of information concerning an offender's personality in the context of digitalization is characterized, and the types of criminal actions that generate digital traces at the stages of preparation, direct commission, and concealment of a crime are identified. The significance of the comprehensive analysis of electronic communications, digital profiles, metadata, transactional activity, and network connections for identifying behavioral patterns, developing investigative versions, detecting the serial nature of criminal activity, and determining promising directions for pre-trial investigation is substantiated.

Keywords: behavioral profiling; criminal profiling; digital analytics; acquisitive crimes; digital traces; digital profile; transactional activity; investigative versions; pre-trial investigation; digital transformation.

Сучасний етап розвитку суспільства характеризується не лише стрімким упровадженням цифрових технологій у фінансову, господарську та комунікаційну сфери, а й зростанням кількості корисливих кримінальних правопорушень, механізм учинення яких постійно ускладнюється. Прагнення до незаконного заволодіння чужим майном, грошовими коштами, цифровими активами або майновими правами залишається одним із найбільш поширених мотивів злочинної діяльності. Водночас корисливі злочини дедалі рідше обмежуються традиційними способами безпосереднього вилучення майна, оскільки правопорушники активно використовують можливості електронних платіжних систем, соціальних мереж, месенджерів, онлайн-платформ, криптовалютних сервісів та засобів дистанційної ідентифікації. Цифровізація суспільних відносин не лише створила нові об'єкти злочинного посягання, а й надала злочинцям додаткові засоби для пошуку потенційних потерпілих, установлення з ними контакту, маніпулювання їхньою поведінкою, переміщення та приховування незаконно отриманих активів. У результаті цього корислива злочинність набуває технологічно організованого, дистанційного та нерідко транскордонного характеру, що істотно ускладнює своєчасне виявлення відповідних кримінальних правопорушень і встановлення причетних до них осіб.

Адаптація злочинців до умов цифрових трансформацій виявляється не лише у використанні новітніх технічних засобів, а й у постійному вдосконаленні моделей злочинної поведінки, способів соціальної інженерії, алгоритмів конспірації та механізмів протидії розслідуванню. Правопорушники вивчають типові реакції потерпілих, підбирають переконливі сценарії комунікації, створюють фіктивні цифрові профілі, використовують підмінені номери телефонів, анонімні облікові записи, мережі підставних осіб і багаторівневі транзакції, що дозволяє їм мінімізувати ризик викриття та ускладнити простеження злочинних зв'язків. За таких умов традиційного аналізу матеріальних слідів та окремих обставин кримінального правопорушення часто

виявляється недостатньо для формування цілісного уявлення про особу злочинця, його мотивацію, спосіб мислення та закономірності вибору об'єкта посягання.

Окрім того, враховуючи, що процес розслідування є доволі складним та динамічним явищем, провадження ефективного досудового розслідування вимагає впровадження у слідчу та оперативно-розшукову діяльність нових методів пізнання [2, с.159], які б дозволяли правоохоронним органам своєчасно реагувати на тенденції злочинної діяльності та адаптувати наявний криміналістичний інструментарій до змін у способах підготовки, вчинення і приховування кримінальних правопорушень. У світлі цього перспективним є запровадження у практику правоохоронних органів методології поведінкового профайлінгу у поєднанні із засобами цифрової аналітики, що дозволить на основі комплексного дослідження поведінкових закономірностей, цифрових слідів, інформаційних зв'язків і транзакційної активності формувати обґрунтовані слідчі версії, звужувати коло осіб, причетних до вчинення корисливих злочинів, та визначати найбільш ефективні напрями їх розслідування.

Л.І. Аркуша, О.В. Чернов та Є.С. Хижняк слушно відзначають, що криміналістичний профайлінг виступає важливим аналітичним інструментом, який здатний суттєво посилити ефективність пізнавальної діяльності слідчого [1, с.1033]. Традиційними джерелами під час профілювання невідомого злочинця виступає матеріальна обстановка місця події, свідчення потерпілих осіб та свідків, результати експертних досліджень та віктимологічна інформація. Проте перенесення різних суспільних відносин у кіберпростір трансформує і джерела інформації про поведінкові особливості злочинця та його потенційної жертви. Надзвичайно актуальною дана теза є саме для різних видів корисливої злочинності, коли як окремі дії з підготовки, так і безпосереднє вчинення та приховування переносяться у цифровий простір, що зумовлює необхідність дослідження електронних комунікацій, цифрових профілів, транзакційної активності, метаданих, мережевих зв'язків та інших цифрових слідів як джерел відомостей про спосіб мислення, поведінкові закономірності, рівень технічної підготовки й роль конкретної особи у механізмі злочинної діяльності.

Під час учинення корисливих злочинів цифрові сліди можуть виникати на різних етапах реалізації злочинного задуму. На етапі підготовки вони утворюються внаслідок пошуку та відбору потенційних потерпілих у соціальних мережах, на торговельних платформах і в інформаційних системах, збирання відомостей про їхній майновий стан, професійну діяльність, коло контактів, фінансові звички та особливості поведінки. До утворення відповідних слідів призводять також реєстрація фіктивних облікових записів, створення підроблених вебсайтів і сторінок, придбання доменних імен, використання електронних поштових скриньок, віртуальних номерів, засобів анонімізації та спеціального програмного забезпечення. Зазначені дії залишають відомості про IP-адреси, ідентифікатори пристроїв, час і тривалість мережевих з'єднань, історію пошукових запитів, реєстраційні дані, геолокацію, а також інші метадані, які

можуть характеризувати рівень підготовки злочинця та обраний ним спосіб учинення кримінального правопорушення.

Під час безпосереднього вчинення корисливого злочину цифрові сліди виникають у процесі встановлення та підтримання контакту з потерпілим за допомогою телефонного зв'язку, електронної пошти, месенджерів, соціальних мереж або онлайн-платформ; надсилання фішингових посилань; використання підроблених платіжних форм; отримання відомостей про банківські рахунки, платіжні картки та засоби автентифікації; здійснення несанкціонованого доступу до облікових записів чи інформаційних систем. Самостійне значення мають сліди фінансових операцій, зокрема переказів між банківськими рахунками, електронними гаманцями та криптовалютними адресами, дроблення платежів, конвертації активів, використання рахунків підставних осіб і сервісів обміну цифрових валют. У разі вчинення злочину групою осіб джерелами інформації стають також цифрові комунікації між організаторами, виконавцями, технічними спеціалістами, фінансовими операторами та особами, залученими до одержання або переведення у готівку незаконно отриманих коштів.

На етапі приховування корисливого злочину відповідні сліди утворюються внаслідок видалення повідомлень і облікових записів, очищення історії переглядів, зміни налаштувань пристроїв, використання програм для знищення або шифрування інформації, переміщення коштів через ланцюги пов'язаних рахунків, криптовалютні міксери чи інші засоби ускладнення фінансового моніторингу. Водночас навіть дії, спрямовані на приховування злочинної активності, можуть залишати відомості у журналах подій, резервних копіях, хмарних сховищах, інформаційних системах банків, операторів електронних комунікацій і власників цифрових платформ. Тому цифровий слід у механізмі корисливого злочину слід розглядати не лише як технічний результат використання певного пристрою або сервісу, а й як відображення конкретного поведінкового рішення злочинця, пов'язаного з вибором потерпілого, способу взаємодії з ним, каналу заволодіння майном та механізму приховування отриманих активів.

Сукупність таких відомостей дозволяє встановлювати рівень технічної підготовки особи, її обізнаність із принципами функціонування платіжних систем, засобами анонімізації, криптовалютними сервісами та механізмами дистанційної взаємодії з потерпілими. Важливого значення набуває також аналіз стилю листування, змісту повідомлень, способів переконання і психологічного впливу, що може свідчити про наявність у злочинця спеціальних знань, попереднього досвіду вчинення аналогічних правопорушень або чітко визначеної ролі у структурі злочинної групи.

Цифрова аналітика дає можливість не лише встановити окремі характеристики невідомої особи, а й виявити повторювані моделі її поведінки. Зокрема, зіставлення відомостей про обраний час учинення злочинних дій, типи потерпілих, способи встановлення контакту, використовувані цифрові платформи,

напрями переміщення грошових коштів та характер подальшого приховування активів може свідчити про серійність відповідної злочинної діяльності. Повторюваність таких ознак дозволяє об'єднувати окремі кримінальні епізоди, формувати версії щодо причетності до них однієї особи або групи осіб, а також прогнозувати найбільш імовірні способи подальшої злочинної поведінки. У цьому аспекті цифрові дані фактично стають відображенням поведінкових рішень злочинця, а їх аналітичне опрацювання створює можливість реконструювати логіку його дій.

Разом із тим побудований на основі цифрової аналітики профіль злочинця не може розглядатися як самостійний доказ причетності конкретної особи до вчинення кримінального правопорушення. Його значення полягає насамперед у формуванні та конкретизації слідчих версій, звуженні кола осіб, які підлягають перевірці, визначенні найбільш перспективних напрямів пошуку цифрових і матеріальних слідів, а також плануванні слідчих (розшукових), негласних слідчих (розшукових) дій та оперативно-розшукових заходів. Ефективність такого профілювання залежить від повноти вихідної інформації, правильності її інтерпретації та обов'язкової перевірки сформованих припущень процесуальними засобами. Саме тому цифрова аналітика має використовуватися у поєднанні з традиційними криміналістичними методами, матеріалами експертних досліджень, показаннями учасників кримінального провадження та іншими фактичними даними.

Перелік використаних джерел:

1. Аркуша Л., Чернов О., Хижняк Є. Психологічні та поведінкові аспекти криміналістичного профайлінгу в системі розслідування кримінальних правопорушень. *Національні інтереси України.* 2026. № 4(21). С. 1019–1035. DOI: https://doi.org/10.52058/3041-1793-2026-4(21)-1019-1034.

2. Мурашко А.С. Профайлінг як складова пізнавальної діяльності у досудовому розслідуванні. *Науковий вісник Міжнародного гуманітарного університету.* Серія: Юриспруденція. 2023. № 66. С. 159–162. DOI: 10.32782/2307-1745.2023.66.33.

DOI https://doi.org/10.32837/11300.33439

Загородній Андрій
аспірант кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
м.Одеса, Україна
ORCID: https://orcid.org/0009–0004–3989–7203
E–mail: zahorodnii.ai@ukr.net

ВЗАЄМОДІЯ СУБ'ЄКТІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА ВИКОРИСТАННЯ АНАЛІТИЧНОЇ ПІДТРИМКИ ШТУЧНОГО ІНТЕЛЕКТУ НА СТАДІЇ ДОСУДОВОГО РОЗСЛІДУВАННЯ

У тезах досліджуються актуальні питання організації взаємодії слідчого, прокурора, оперативних підрозділів, криміналістів і судових експертів на різних стадіях кримінального провадження. На підставі положень Кримінально процесуального кодексу України та аналізу судово–слідчої практики розкриваються процесуальні й організаційні форми взаємодії під час огляду місця події, проведення слідчих (розшукових) дій, відбору зразків для експертних досліджень, проведення слідчого експерименту та негласних слідчих (розшукових) дій.

Особлива увага приділяється можливостям використання аналітичної підтримки штучного інтелекту на початковому, подальшому та завершальному етапах досудового розслідування з метою підвищення ефективності розкриття, документування та доказування кримінальних правопорушень.

Ключові слова: Кримінально процесуального кодексу України, досудове розслідування, взаємодія, слідчий, прокурор, криміналістика, судовий експерт, Негласні слідчі розшукові дії, штучний інтелект, алгоритмізація.

Zahorodnii Andrii
Postgraduate Student at the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine
ORCID: https://orcid.org/0009–0004–3989–7203
e–mail: zahorodnii.ai@ukr.net

INTERACTION OF PRE–TRIAL INVESTIGATION SUBJECTS AND THE USE OF ARTIFICIAL INTELLIGENCE ANALYTICAL SUPPORT AT THE STAGE OF PRE–TRIAL INVESTIGATION

The theses examine current issues related to the organization of interaction between the investigator, prosecutor, operational units, criminalists and forensic experts at different stages of pre–trial investigation. Based on the provisions of the Criminal

Procedure Code of Ukraine and the analysis of judicial and investigative practice, the paper reveals the procedural and organizational forms of interaction during crime scene examination, investigative search actions, collection of samples for expert examination, investigative experiments, appointment of forensic examinations and covert investigative search actions.

Particular attention is paid to the possibilities of using artificial intelligence analytical support at the initial, subsequent and final stages of pre–trial investigation. It is substantiated that digital tools may contribute to the systematization of criminal proceedings materials, identification of links between evidence, forecasting of investigative situations, optimization of procedural planning and improvement of forensic support for the investigation.

It is emphasized that the use of artificial intelligence in pre–trial investigation is auxiliary in nature and cannot replace the procedural independence of the investigator, prosecutorial supervision, expert examination or judicial assessment of evidence. The conclusion is drawn that the combination of proper intersubject interaction and modern information and analytical technologies can improve the quality of detection, documentation and proving of criminal offences, provided that legality, admissibility of evidence and human rights guarantees are observed.

Key words: Criminal Procedure Code of Ukraine, pre–trial investigation, interaction, investigator, prosecutor, criminalistics, forensic expert, covert investigative search actions, artificial intelligence, algorithmization.

Сучасний стан розвитку криміналістики, цифрових технологій та інформаційно–аналітичних систем обумовлює необхідність удосконалення організації досудового розслідування шляхом алгоритмізації діяльності слідчого, прокурора, працівників оперативних підрозділів, криміналістів та судових експертів. Особливого значення це набуває при розслідуванні тяжких та особливо тяжких кримінальних правопорушень, де ефективність початкових процесуальних дій безпосередньо впливає на кінцевий результат доказування.

Відповідно до ст. 2 Кримінально процесуального кодексу України завданнями кримінального провадження є забезпечення швидкого, повного та неупередженого розслідування, а також притягнення винної особи до відповідальності в міру її вини [3]. Реалізація цих завдань неможлива належної взаємодії між усіма суб'єктами кримінального провадження.

Судово–слідча практика свідчить, що найбільш результативними є кримінальні провадження, у яких забезпечується комплексна взаємодія слідчого, прокурора, оперативних працівників, криміналістів та експертів вже на початковій стадії досудового розслідування – з моменту отримання повідомлення про кримінальне правопорушення та внесення відомостей до Єдиний реєстр досудових розслідувань.

Відповідно до ст. 36 Кримінально процесуального кодексу України прокурор здійснює процесуальне керівництво досудовим розслідуванням,

координує діяльність правоохоронних органів та забезпечує законність процесуальних рішень [2; 3].

Ст. 40 Кримінально процесуального кодексу України визначає процесуальну самостійність слідчого, який організовує проведення слідчих (розшукових) дій та відповідає за повноту доказування [3].

Однією з ключових форм взаємодії є діяльність слідчо–оперативної групи під час огляду місця події. Практика свідчить, що саме перші години після вчинення кримінального правопорушення мають вирішальне значення для виявлення, фіксації та вилучення слідів. У таких випадках слідчий здійснює керівництво оглядом місця події відповідно до ст. 237 Кримінально процесуального кодексу України, криміналіст забезпечує використання техніко–криміналістичних засобів фіксації, спеціаліст надає консультаційну допомогу щодо механізму утворення слідів, а оперативні працівники здійснюють переслідування злочинців «по гарячих слідах», встановлення свідків, очевидців та перевірку оперативної інформації.

Особливого значення набуває взаємодія під час вилучення біологічних, трасологічних, балістичних та цифрових слідів. При відборі зразків для проведення судових експертиз слідчий забезпечує процесуальне оформлення відповідно до вимог Кримінально процесуального кодексу України, криміналіст визначає порядок пакування та збереження слідів, а експерт надає рекомендації щодо придатності об’єктів для подальших експертних досліджень. Така взаємодія дозволяє мінімізувати ризики втрати доказової інформації та уникнути визнання доказів недопустимими.

Важливою формою взаємодії є організація та проведення слідчого експерименту (відтворення обстановки та обставин події) відповідно до ст. 240 Кримінально процесуального кодексу України, особливо у випадках участі особи, яка перебуває під вартою. У таких ситуаціях слідчий забезпечує процесуальне оформлення дії, прокурор контролює законність її проведення, працівники оперативних та конвойних підрозділів відповідають за безпеку учасників та недопущення втечі, а криміналіст здійснює технічну фіксацію результатів із застосуванням фото–, відеозапису та цифрового моделювання.

Окремого значення набуває взаємодія при проведенні негласних слідчих (розшукових) дій відповідно до глави 21 Кримінально процесуального кодексу України [3].

На підставі ухвали слідчого судді фактично саме оперативні підрозділи здійснюють практичну реалізацію негласних слідчих (розшукових) дій, а прокурор забезпечує процесуальний контроль, у той час як слідчий організовує використання отриманих результатів у доказуванні [1].

Судово–слідча практика підтверджує, що порушення алгоритму взаємодії між суб’єктами, які забезпечують проведення негласних слідчих (розшукових) дій, часто призводить до втрати доказового значення отриманої інформації.

У сучасних умовах особливого значення набуває використання аналітичної підтримки штучного інтелекту на всіх стадіях досудового розслідування. На початковому етапі досудового розслідування технології штучного інтелекту можуть використовуватись слідчим для:

- автоматизованого аналізу повідомлень про кримінальні правопорушення;
- побудови первинних криміналістичних версій;
- аналітичного зіставлення слідів та даних із базами обліків;
- аналізу відеозаписів систем спостереження;
- прогнозування маршрутів пересування підозрюваних;
- автоматизованого формування процесуальних документів.

На подальшому етапі досудового розслідування застосування слідчим можливостей ШІ може забезпечувати:

- аналітичне узагальнення великих масивів доказової інформації;
- виявлення зв’язків між учасниками злочинної діяльності;
- аналіз телефонних з’єднань, геолокаційних даних та цифрових слідів;
- підтримку планування слідчих (розшукових) дій;
- моделювання механізму вчинення кримінального правопорушення.

На завершальному етапі досудового розслідування аналітичні системи слідчим можуть використовуватись для:

- перевірки повноти доказової бази;
- контролю процесуальних строків;
- систематизації матеріалів кримінального провадження;
- автоматизованого формування обвинувального акта;
- створення електронних схем доказування та логічних зв’язків між доказами.

Таким чином, впровадження сучасних цифрових на стадії досудового розслідування включаючи аналітичну підтримку штучного інтелекту, формують новий напрям розвитку криміналістики та кримінального процесу. Комплексна взаємодія слідчого, прокурора, працівників оперативних підрозділів, криміналістів та експертів є необхідною умовою ефективного розкриття кримінальних правопорушень, належного доказування та забезпечення об’єктивного правосуддя відповідно до вимог Кримінально процесуального кодексу України.

Перелік використаних джерел:

1. Гресь Ю.О., Колодіна А.С. Напрями та форми взаємодії при розслідуванні вбивств. *Юридичний науковий електронний журнал*. 2025. № 4. С.533-538. URL: http://lsej.org.ua/4_2025/130.pdf

2. Кісліцина І.О., Гресь Ю.О. Організація і тактика взаємодії прокурора з іншими учасниками досудового розслідування злочинів проти довкілля. *Правові новели.* 2025. № 27. С.208-217. URL: https://legalnovels.in.ua/journal/27_2025/27.pdf

3. Кримінальний процесуальний кодекс України // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651–17.

DOI https://doi.org/10.32837/11300.33440

Караман Микола
доктор філософії за спеціальністю 081 «Право»,
соціальний педагог Відокремленого підрозділу «Об'єднане вище
професійно–технічне училище сфери послуг
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–8445–7021
E–mail: karaman@onua.edu.ua

ОКРЕМІ ПИТАННЯ ОСОБЛИВОСТЕЙ ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОСУДДЯ ЩОДО ЗЛОЧИНІВ АГРЕСІЇ ТА ВОЄННИХ ЗЛОЧИНІВ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ

У тезах присвячено увагу аналізу сучасних викликів у сфері експертного забезпечення правосуддя. Проаналізовано доктринальні підходи до напрямків розвитку експертного правосуддя в умовах особливостей епохи цифрових технологій. Досліджено проблеми використання цифрових доказів задля забезпечення правосуддя. Розглянуто особливості проблем доказування з використанням цифрових технологій.

Ключові слова: експертне забезпечення правосуддя, злочини агресії, воєнні злочини, епоха цифрових технологій, цифрові докази.

Karaman Mykola
Doctor of Philosophy in specialty 081 «Law»
Social educator of the Separate subdivision «United Higher Vocational and Technical School of the Service Sector of the National University «Odesa Law Academy»,
Odesa, Ukraine

SPECIFIC ISSUES OF THE FEATURES OF EXPERT PROVISION OF JUSTICE IN RELATION TO CRIMES OF AGGRESSION AND WAR CRIMES IN THE ERA OF DIGITAL TECHNOLOGIES

Social educator of the Separate unit «Joint higher vocational and technical school of the service sector of the National university «Odesa law academy», Odesa, Ukraine

The abstracts focus on the analysis of modern challenges in the field of expert justice provision. Doctrinal approaches to the development of expert justice in the context of the specifics of the era of digital technologies are analyzed. The problems of using digital evidence to ensure justice are investigated. The specifics of the problems of evidence using digital technologies are considered.

Key words: expert justice, crimes of aggression, war crimes, the era of digital technologies, digital evidence.

В умовах збройної агресії російської федерації не викликає сумнівів актуальність дослідження забезпечення правосуддя щодо злочинів агресії та воєнних злочинів. В той же час, епоха цифрових технологій є передумовою виникнення нових викликів експертного забезпечення правосуддя, адже досить часто фізичного доступу до місця вчинення злочину не відбувається через бойові дії або окупацію, або ж багато злочинів вчиняються механізмами цифрової епохи.

За даними Офісу Генерального прокурора України, на початку 2024 року зареєстровано понад 120 тис. кримінальних проваджень щодо воєнних злочинів та злочинів агресії (це число взято з офіційного обліку) [1,с. 57].

Воєнні злочини та злочини агресії – це не лише рядок у правовому документі. Це ще й соціальна, політична та культурна історія – і це відчувається в реальному житті. Вони охоплюють багато різних дій: від умисних нападів на цивільне населення до руйнування культурної спадщини, від катувань до депортацій. У кожного злочину своя «специфіка», але всі вони ламають базові правила гуманності.

Під час війни в Україні такі злочини трапляються масово. Таке відбувається не з рідкісними випадками – а зі системними порушеннями, які повторюються. І тут додається ще одна складність: епоха цифровізації. Вона з одного боку полегшує збір і фіксацію доказової бази, а з іншого – піднімає питання, як саме досліджувати ці матеріали експертам (і як робити це якісно).

Як каже А.М. Бабенко, проблеми зі судовими експертизами у воєнних злочинах часто тягнуться за тим, як важко зібрати достовірні докази в зоні конфлікту [2, с. 36]. Але цифрова доба теж відкриває двері – і не порожні. Тепер можна документувати злочини по–новому, від супутникових знімків до розбору даних із соціальних мереж [3, с. 70].

Одна з головних труднощів – доказування. Дрібні нюанси тут вирішують усе. Традиційні методи – свідчення очевидців, експертизи, матеріальні докази – нерідко виходять недостатніми. У сучасних умовах цифрові докази стають дедалі важливішими: відеозаписи, записи з камер спостереження, дописи у соціальних мережах.

Україна не одна в цій проблемі. Є багато інших країн, які теж стикаються з воєнними злочинами. Міжнародні трибунали (ICTY –Міжнародний трибунал по колишній Югославії, ICTR – Міжнародний кримінальний трибунал з Руанди, МКС – Міжнародний кримінальний суд) уже напрацювали певні стандарти – і це дає хоч якусь опору. Такі орієнтири допомагають порівнювати підходи й вимоги, коли йдеться про розслідування та судовий розгляд.

ICTY визнавав навіть одиничні факти порушення міжнародного гуманітарного права достатніми для кваліфікації злочину. МКС активно використовує цифрові докази, зокрема матеріали OSINT. Українська практика поступово інтегрує ці стандарти, але водночас формує власну доктрину.

Буткевич В. Г. у своїй статті «Міжнародне кримінальне право та українська практика» наголошує, що українське законодавство має бути узгоджене з міжнародними стандартами, зокрема нормами Римського статуту МКС [4, с. 20]. В той же час, формальна гармонізація не гарантує ефективності. Україна має власний контекст – масові злочини на території держави, яка водночас прагне інтеграції до ЄС. Тому гармонізація повинна бути не лише формальною, а й практичною.

В умовах сучасної війни в Україні воєнні злочини стали предметом не лише кримінального переслідування, а й міжнародної політики та суспільної пам'яті. Як зазначає Александренко О., криміналістичне та судово–експертне забезпечення правоохоронної діяльності в умовах воєнного стану має бути системним і включати створення спеціалізованих слідчих груп [5, с. 49].

Однак сама ідея спеціалізованих груп потребує розширення. Воєнні злочини охоплюють не лише юридичні факти, а й психологічні травми, технологічні виклики та політичні наслідки. Тому слідчі групи повинні бути міждисциплінарними, включати юристів, експертів з цифрових технологій, психологів, соціологів і навіть істориків. Це дозволить уникнути вузького формалізму й забезпечити більш глибоке розслідування.

Важливо також враховувати, що кваліфікація воєнних злочинів не може ґрунтуватися лише на формальних ознаках складу злочину. Вона повинна враховувати контекст – політичний, соціальний, культурний. Лише тоді правосуддя буде не лише юридично правильним, а й морально переконливим.

Також, цифрова криміналістика вже стала окремим напрямком науки. Шевчук В. М. визначає її як ключовий інструмент доведення воєнних злочинів [3, с. 72]. Водночас Ткачук Т. Ю. та Оніщенко В. Г. акцентують на проблемі достовірності цифрових доказів [6, с. 91]. Це питання є критичним, адже відеозаписи, дані з камер спостереження чи дописи у соцмережах можуть бути змонтовані або сфальсифіковані. Саме тому необхідно створити національні стандарти перевірки цифрових доказів, які б гарантували їхню автентичність.

Перспективними є технології OSINT (Open Source Intelligence), що дозволяють залучати дані з відкритих джерел, та блокчейн, який може забезпечити неперервність ланцюга збереження доказів. Використання блокчейну здатне стати «золотим стандартом» для збереження цифрових доказів, адже воно не лише технічно унеможливлює їхню зміну, а й підвищує довіру суспільства до правосуддя [7].

Правосуддя у сфері воєнних злочинів має бути не лише формально правильним, а й морально переконливим. Якщо суспільство сумнівається у достовірності доказів, навіть юридично бездоганне рішення може втратити легітимність.

Тому судові процеси повинні бути максимально прозорими, а суспільство має мати доступ до інформації про злочини та їхнє розслідування. Лише тоді

правосуддя стане не лише юридичним, а й суспільним актом, що зміцнює довіру до держави та її інституцій.

Це особливо важливо в умовах війни, коли суспільство переживає травму і потребує не лише покарання винних, а й підтвердження того, що справедливість існує. Таким чином, довіра суспільства стає ключовим фактором успіху правосуддя. Українська система експертного забезпечення правосуддя стоїть перед історичним викликом. Воєнні злочини та злочини агресії – це не лише питання права, а й питання справедливості, пам'яті та майбутнього. Якщо національна система експертного забезпечення правосуддя зможе побороти виклики, які постають перед нею в умовах злочинів агресії та воєнних злочинів в епоху цифрових технологій це дозволить не лише якісно розслідувати злочини, а й підвищити довіру суспільства до правосуддя.

Перелік використаних джерел:

1. Бундз Р., Яровик Д. Воєнні злочини в кримінальному праві України. *Юридичні науки.* 2023. № 2. С. 55–63.
2. Бабенко А. М., Матвєєвський О. В., Саінчин С. О. Проблеми проведення судових експертиз під час розслідування воєнних злочинів. *PDU*. 2024. № 1. С. 33–41.
3. Шевчук В. М. Цифрова криміналістика: воєнні виклики та нові завдання. *Вісник НАПрН України.* 2023. № 4. С. 67–75.
4. Буткевич В. Г. Міжнародне кримінальне право: сучасні виклики. *Юридична Україна.* 2021. № 3. С. 15–23.
5. Александренко О. Криміналістичне та судово–експертне забезпечення правоохоронної діяльності в умовах воєнного стану. *Наукові праці НАВС.* 2023. № 2. С. 49–55.
6. Ткачук Т. Ю., Оніщенко В. Г. Проблеми достовірності цифрових доказів у кримінальному процесі. *Юридичні науки*. 2025. № 1. С. 91–98.
7. Степаненко Н. Використання технологій блокчейн у кримінальному процесі. *Вісник НУ «Львівська політехніка»*. 2025. № 3. С. 104–110.

DOI https://doi.org/10.32837/11300.33442

Мирошниченко Юрій
доктор юридичних наук,
суддя Мукачівського міськрайонного суду Закарпатської області,
м. Мукачево, Україна
ORCID: https://orcid.org/0000–0002–9114–1495
e–mail: zaruba264@gmail.com

ЦИФРОВА ВІЗУАЛІЗАЦІЯ ЯК ЗАСІБ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ СУДОВОГО ПРОВАДЖЕННЯ

Розкрито значення мультимедійних технологій для оптимізації судового пізнання у кримінальному провадженні. Запропоновано розмежування доказових та ілюстративних форм візуалізації, визначено їх процесуальні функції й перспективи нормативного врегулювання.

Ключові слова: судове провадження, візуалізація, судове пізнання, доказування, криміналістика.

Yurii Myroshnychenko
Doctor of Law,
Judge of the Mukachevo City District Court of Zakarpattia Region,
Mukachevo, Ukraine

DIGITAL VISUALIZATION AS A MEANS OF FORENSIC SUPPORT OF JUDICIAL PROCEEDINGS

The paper reveals the significance of multimedia technologies for optimizing judicial cognition in criminal proceedings. A distinction between evidentiary and illustrative forms of visualization is proposed, and their procedural functions and prospects for normative regulation are determined.

Key words: judicial proceedings, visualization, judicial cognition, proof, criminalistics.

У сучасних умовах цифровізації кримінального судочинства особливого значення набувають засоби візуалізації доказової інформації у судовому провадженні. Необхідність їх використання обумовлена не лише розвитком інформаційних технологій, але й об’єктивним ускладненням предмета судового пізнання у кримінальних провадженнях щодо злочинів із багатокомпонентною просторово–часовою, технологічною або ситуаційною структурою.

Можливість подання складної доказової інформації у формі, придатній для її повного та належного осягнення учасниками судового провадження, залишається проблематичною, оскільки індивідуальні суб’єктивні інтерпретації можуть перешкоджати правильному колективному розумінню досліджуваної

події [1]. Водночас результати досліджень у сфері когнітивного сприйняття свідчать про вищу ефективність засвоєння інформації при одночасному залученні декількох каналів сприйняття [2]. Саме тому використання мультимедійних засобів презентації доказової інформації здатне підвищити ефективність розуміння судом складних просторових, часових і технологічних характеристик кримінального правопорушення.

У контексті криміналістичного забезпечення судового провадження [3] цифрову візуалізацію доцільно розглядати як засіб оптимізації судового пізнання, спрямований на забезпечення належного сприйняття судом складних обставин кримінального правопорушення, просторових взаємозв'язків між об'єктами, послідовності дій учасників події, механізму утворення слідів, а також функціонування технологічних процесів і систем. У складних багатоепізодних або технологічно обумовлених кримінальних провадженнях виключно вербальна форма передачі інформації створює надмірне когнітивне навантаження на суд, ускладнюючи формування цілісного уявлення про механізм досліджуваної події.

Особливого значення такі засоби набувають у кримінальних провадженнях щодо: злочинів проти життя та здоров'я особи; порушень правил безпеки руху або експлуатації автомобільного, залізничного, водного чи повітряного транспорту; техногенних аварій та нещасних випадків на виробництві; воєнних злочинів та кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку.

Спільною ознакою таких проваджень є складність динаміки досліджуваної події, значна кількість просторових, часових і технологічних взаємозв'язків, які важко адекватно відтворити виключно вербальними засобами. У багатьох випадках суддя, не будучи спеціалістом у відповідній галузі знань, об'єктивно не має можливості сформувати повне уявлення про механізм події лише на підставі усного опису. Саме тому цифрова візуалізація виконує не декоративну, а когнітивну функцію, забезпечуючи сприйняття складних алгоритмів, процесів, просторових конфігурацій та послідовності розвитку події.

У зарубіжній правовій доктрині використання візуальних моделей, схем, анімацій та мультимедійних реконструкцій традиційно пов'язується з категорією «demonstrative evidence». Водночас сучасний розвиток американського доказового права свідчить про тенденцію до чіткого розмежування доказів та ілюстративних засобів пояснення доказової інформації. Зокрема, Federal Rule of Evidence 107 визначає illustrative aids як засоби, що використовуються не як докази, а для сприяння розумінню доказів або аргументації судом [4, 5].

Доказова цифрова візуалізація є формою відображення та представлення доказової інформації і може використовуватися як додаток до протоколу слідчої (розшукової) дії або висновку експерта. До неї можуть належати тривимірні моделі місця події, результати лазерного сканування, цифрові реконструкції, анімовані результати слідчого експерименту, фотограмметричні моделі,

ситуативне експертне моделювання тощо. У таких випадках візуалізація має похідний характер і підлягає оцінці у сукупності з іншими доказами.

Ілюстративна цифрова візуалізація не має самостійного доказового значення та використовується стороною обвинувачення або захисту як засіб презентації власної версії події кримінального правопорушення. Йдеться, зокрема, про використання прокурором під час вступної промови анімаційної або мультимедійної реконструкції механізму злочину, яка відображає сформовану на підставі наявних доказів модель події та супроводжується заявою про готовність підтвердити продемонстровані обставини відповідними доказами під час судового розгляду.

У цьому аспекті цифрова візуалізація виконує функцію криміналістичного моделювання версії сторони обвинувачення та сприяє попередній когнітивній організації сприйняття доказової інформації судом. Основною перевагою використання технологій під час судового розгляду є різноманітність методів презентації, які дозволяють зробити складну доказову інформацію більш доступною для сприйняття судом. Наприклад, тривимірні моделі місця події дозволяють сформувати уявлення про просторову структуру досліджуваного середовища, а цифрова візуалізація тілесних ушкоджень – більш наочно продемонструвати характер і механізм спричинення шкоди.

Впровадження в судовий розгляд сучасних технологій візуалізації поступово змінює саму модель судової комунікації. Використання інтерактивних дисплеїв, мультимедійних презентацій, кількох екранів для демонстрації документів, схем, графіків і відеоматеріалів дозволяє підвищити ефективність представлення доказової інформації [6]. У низці іноземних судових установ уже функціонують спеціалізовані системи цифрового подання доказів та мультимедійної демонстрації інформації у суді [7; 8]. Водночас чинний КПК України не містить спеціальних положень, які б прямо регламентували використання сторонами цифрових засобів візуалізації під час вступних промов, що зумовлює неоднорідність судової практики та залежність розв’язання цього питання від розсуду головуючого.

З огляду на це потребує нормативного врегулювання питання використання сторонами під час вступних промов засобів візуалізації та демонстрації інформації, що ілюструють обставини, які, на думку сторони, будуть підтверджені дослідженими у судовому розгляді доказами.

При цьому ризики сугестивного або надмірного емоційного впливу цифрової візуалізації на суд мінімізуються процесуальною природою змагального судочинства, можливістю сторін пропонувати альтернативні моделі події та обов’язком суду оцінювати не саму презентацію, а підтвердження продемонстрованої інформації належними та допустимими доказами.

Підсумовуючи, слід констатувати, що цифрова візуалізація поступово трансформується із допоміжного технічного засобу демонстрації інформації на самостійний елемент криміналістичного забезпечення судового провадження,

здатний оптимізувати процес судового пізнання у складних кримінальних провадженнях. Запропоноване розмежування доказової та ілюстративної цифрової візуалізації створює підґрунтя для визначення їх процесуального статусу, функціонального призначення та меж допустимого використання у судовому розгляді. Водночас порушена проблематика потребує подальшого комплексного дослідження, зокрема у частині співвідношення цифрової візуалізації з концептом «demonstrative evidence», критеріїв процесуальної допустимості цифрових реконструкцій, використання технологій штучного інтелекту під час моделювання події кримінального правопорушення, а також розроблення криміналістичних і процесуальних стандартів використання засобів візуалізації у судовому провадженні.

Перелік використаних джерел:

1. Sheppard K., Fieldhouse S. J., Cassella J. P. Experiences of evidence presentation in court: an insight into the practice of crime scene examiners in England, Wales and Australia. Egyptian Journal of Forensic Sciences. 2020. Vol. 10, № 1. DOI: 10.1186/s41935–020–00184–5.

2. How Using Tech in the Courtroom Can Impact Case Outcomes. Law Technology Today. 2020. URL: https://www.lawtechnologytoday.org/2020/11/how–using–tech–in–the–courtroom–can–impact–case–outcomes/

3. Мирошниченко Ю. М. Криміналістичне забезпечення судового провадження: концептуальні основи : дис. … д–ра юрид. наук : 12.00.09. Кропивницький, 2024. 493 с. URL: https://dnuvs.ukr.education/wp–ontent/uploads/2024/08/dysertacziya_myroshnychenko_yu_m_compressed.pdf

4. Rule 107. Illustrative Aids. Legal Information Institute. URL: https://www.law.cornell.edu/rules/fre/rule_107

5. Capra D. J., Richter L. L. Painting a Clearer Picture: Introducing New Federal Rule of Evidence 107 Regulating Illustrative Aids. Vanderbilt Law Review. 2024. Vol. 77, № 5. P. 1381–1434.

6. Kuchler D. D., O'Toole L. C. How Technological Advances in the Courtroom Are Changing the Way We Litigate. FDCC Quarterly. 2008. Vol. 58, № 2. P. 205–217. URL: https://2zqe7a.p3cdn1.secureserver.net/wp–content/uploads/2021/01/2008–technological–advances–in–the–courtroom.pdf

7. NYS Court of Claims Evidence Presentation System. New York State Court of Claims. URL: https://ww2.nycourts.gov/Courts/nyscourtofclaims/overview–technology.shtml.

8. Courtroom Technology: Evidence Presentation. United States Bankruptcy Court: District of Utah. URL: https://www.utb.uscourts.gov/courtroom–technology–evidence–presentation

DOI https://doi.org/10.32837/11300.33443

Недашківська Ольга
старший судовий експерт сектору товарознавчих досліджень відділу товарознавчих, економічних, будівельних, земельних досліджень та оціночної діяльності Житомирський науково–дослідний експертно–криміналістичний центр МВС України,
м. Житомир, Україна
ORCID: https://orcid.org/0000–0003–2568–0201,
e–mail: persik.emir@gmail.com

Гунько Олександр
Директор Житомирський науково–дослідний е кспертно–криміналістичний центр МВС України,
м. Житомир, Україна
ORCID: https://orcid.org/0009–0003–7119–720X,
e–mail: omgunko@ukr.net

ЦИФРОВІЗАЦІЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ: ТРАНСФОРМАЦІЯ ДОКАЗУВАННЯ, НОВІ ТЕХНОЛОГІЧНІ МОЖЛИВОСТІ ТА ВИКЛИКИ ПРАВОСУДДЯ

Розглянуто вплив цифровізації та штучного інтелекту на судово–експертну діяльність. Висвітлено трансформацію доказування, нові технологічні можливості аналізу цифрових доказів, специфіку правосуддя та перспективи розвитку в Україні.

Ключові слова: судова експертиза, цифровізація, цифрова криміналістика, штучний інтелект, цифрові докази.

Nedashkivska Olga,
senior forensic expert of the commodity research sector of the department of commodity, economic, construction, land research and appraisal activities Zhytomyr Scientific Research Expert and Forensic Center of the Ministry of Internal Affairs of Ukraine,
Zhytomyr, Ukraine

Gunko Olexandr
Director Zhytomyr Scientific Research Expert and Forensic Center of the Ministry of Internal Affairs of Ukraine,
Zhytomyr, Ukraine

DIGITIZATION AND ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ACTIVITY: TRANSFORMATION OF EVIDENCE, NEW TECHNOLOGICAL CAPABILITIES, AND CHALLENGES TO JUSTICE

The impact of digitalization and artificial intelligence on forensic expert activity is examined. The transformation of evidence, new technological capabilities for analyzing digital evidence, the specifics of justice, and development prospects in Ukraine are highlighted.

Key words: forensic examination, digitalization, digital forensics, artificial intelligence, digital evidence.

Стрімка цифровізація суспільства, розвиток штучного інтелекту та трансформація сучасної злочинності формують нові вимоги до системи правосуддя й судово–експертної діяльності [1]. У XXI столітті цифрові дані фактично стали одним із головних джерел доказової інформації, а тому ефективність розслідування кримінальних правопорушень дедалі більше залежить від технологічних можливостей експертного забезпечення. Особливо актуальним це питання є для України в умовах воєнного стану, зростання кіберзагроз та інтеграції до європейського правового простору.

Сучасна судово–експертна діяльність уже не обмежується традиційними криміналістичними методиками [2]. Значна частина доказів сьогодні існує виключно у цифровій формі: листування у месенджерах, дані мобільних операторів, геолокація, відео з камер спостереження, цифрові фінансові операції, інформація з соціальних мереж, хмарних сервісів та електронних реєстрів. Це вимагає формування принципово нової моделі експертного забезпечення правосуддя, у якій ключову роль відіграють цифрові технології, автоматизовані системи аналізу інформації та алгоритми штучного інтелекту.

Одним із найбільш динамічних напрямів є розвиток цифрової криміналістики [2]. Сучасні експерти працюють із великими масивами даних, здійснюють відновлення видаленої інформації, аналізують цифрові сліди та встановлюють часову послідовність дій користувачів. Комп’ютерно–технічні експертизи сьогодні охоплюють дослідження:

мобільних телефонів;
серверів;
електронних носіїв інформації;
криптовалютних транзакцій;
соціальних мереж;
систем відеоспостереження;
хмарних сховищ;
цифрових логів активності.

Особливу роль у сучасній експертній діяльності відіграє штучний інтелект. AI–системи здатні автоматично аналізувати великі масиви інформації, виявляти приховані закономірності та пришвидшувати процес дослідження доказів. Алгоритми машинного навчання вже активно застосовуються для:

розпізнавання облич;

аналізу поведінкових моделей;
автоматичного порівняння відбитків пальців;
дослідження балістичних слідів;
виявлення фальсифікованих фото та відео;
аналізу текстів і голосових повідомлень.

У сфері кібербезпеки штучний інтелект дозволяє виявляти ознаки кібератак, аналізувати шкідливе програмне забезпечення та прогнозувати потенційні цифрові загрози. Це набуває особливого значення в умовах гібридної війни, коли кібератаки стають елементом дестабілізації державної інфраструктури та системи управління.

В умовах воєнного конфлікту цифрові технології фактично стали одним із головних інструментів документування воєнних злочинів. Використання супутникових знімків, дронів, геолокаційного аналізу, систем OSINT та 3D–моделювання дозволяє фіксувати наслідки обстрілів, ідентифікувати військову техніку, встановлювати місце та час подій. Значна частина доказової бази формується саме на основі цифрової інформації, отриманої з відкритих джерел або електронних пристроїв.

Суттєво змінюється й сама організація експертної діяльності. Впровадження електронного документообігу, автоматизованих реєстрів експертних висновків та цифрових платформ взаємодії між правоохоронними органами й експертними установами дозволяє оптимізувати процеси призначення та проведення експертиз [3]. Формування єдиного цифрового середовища забезпечує швидкість обміну інформацією та підвищує контроль за збереженням доказів.

Перспективним напрямом є використання технологій Big Data та predictive analytics. Аналіз великих обсягів інформації дозволяє встановлювати приховані зв’язки між подіями, особами та фінансовими операціями. Такі технології активно використовуються під час розслідування організованої злочинності, фінансових махінацій, терористичної діяльності та кіберзлочинів.

На окрему увагу заслуговує використання блокчейн–технологій у сфері доказування. Блокчейн дозволяє фіксувати незмінність цифрової інформації, підтверджувати час створення файлів та забезпечувати контроль ланцюга збереження доказів. Це мінімізує ризики втрати або фальсифікації цифрових матеріалів та підвищує рівень довіри до результатів експертиз.

Разом із позитивними аспектами цифровізація породжує й нові ризики. Однією з найбільш серйозних проблем стає використання deepfake–технологій та генеративного штучного інтелекту для створення підроблених відео–, аудіо– та інших документів. Це суттєво ускладнює процес перевірки достовірності доказів та вимагає розробки нових методик цифрової верифікації.

Крім того, використання AI у сфері правосуддя породжує дискусії щодо етичних і правових меж автоматизації. Алгоритми можуть містити помилки, працювати з упередженнями або створювати ризики порушення прав людини.

Саме тому штучний інтелект повинен розглядатися як допоміжний інструмент експерта, а не повноцінна заміна професійного людського аналізу.

Серед актуальних проблем слід виокремити:

недостатнє технічне забезпечення окремих експертних установ;

дефіцит фахівців у сфері цифрової криміналістики;

відсутність єдиних стандартів дослідження цифрових доказів;

складність міжнародного обміну цифровою інформацією;

високі ризики кібервтручання у державні реєстри та бази даних.

Подальший розвиток системи експертного забезпечення правосуддя повинен ґрунтуватися на комплексній цифровій модернізації. Ключовими напрямами мають стати:

створення національної системи цифрової криміналістики;

інтеграція AI–технологій у процес аналізу доказів;

впровадження міжнародних стандартів кібербезпеки;

розвиток захищених цифрових платформ;

удосконалення підготовки експертів у сфері штучного інтелекту;

формування єдиної електронної системи експертних досліджень.

Особливе значення має гармонізація українського законодавства із європейськими стандартами у сфері електронних доказів та використання AI у правосудді. Інтеграція України до міжнародних цифрових платформ і професійних мереж сприятиме взаємному визнанню експертних висновків та підвищенню ефективності міжнародного співробітництва [4].

Отже, цифрові технології та штучний інтелект поступово стають фундаментальними елементами сучасної системи експертного забезпечення правосуддя. Їх впровадження суттєво підвищує швидкість, точність та ефективність дослідження доказів, водночас формуючи нові виклики для правової системи. У сучасних умовах саме поєднання інноваційних технологій, міжнародних стандартів та професійної експертної підготовки визначатиме подальший розвиток судово–експертної діяльності та ефективність функціонування правосуддя в Україні [5].

Водночас подальша цифрова трансформація експертної діяльності потребує комплексного вдосконалення нормативно–правового регулювання, забезпечення належного рівня кібербезпеки та створення ефективних механізмів перевірки достовірності електронних доказів. Важливим напрямом розвитку залишається інтеграція української системи судової експертизи до міжнародного професійного простору, розширення використання інтелектуальних аналітичних систем, а також формування сучасної матеріально–технічної бази, здатної забезпечити належне функціонування правосуддя в умовах стрімкого технологічного розвитку та глобальних безпекових викликів.

Перелік використаних джерел:

1. Про судову експертизу : Закон України від 25.01.1994 р. № 4038–XII. URL: https://zakon.rada.gov.ua/laws/show/4038–12#Text.

2. В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : колективна монографія / за заг. ред. В. Ю. Шепітька. НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 208 с.

3. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851–IV. URL: https://zakon.rada.gov.ua/laws/show/851–15#Text.

4. Ковальов К.М. Оптимізація законодавства у сфері судово–експертної діяльності. Проблеми реформування базового законодавства України з питань експертного забезпечення правосуддя : матеріали круглого столу, м. Харків, 6–7 лютого 2020 р. Харків, 2020. С. 21–24.

5. Недашківська О.А. Шляхи забезпечення інформаційної підтримки судових експертиз в умовах цифрової трансформації : аналіз і пропозиції. Актуальні питання криміналістики та судової експертизи в умовах воєнного стану : матеріали всеукр. наук.–практ. конф., м. Київ, 3 липня 2024 р. Київ, 2024. С. 284–286.

DOI https://doi.org/10.32837/11300.33444

Остапенко Артур
завідувач криміналістичної лабораторії,
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0009–0000–7148–1778
e–mail: ostapenko.12232@gmail.com

ТЕХНІКО–КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

У тезах розглянуто особливості техніко–криміналістичного забезпечення розслідування кримінальних правопорушень у сучасних умовах цифрової трансформації. Проаналізовано вплив цифрових технологій на процес виявлення, фіксації, вилучення та дослідження доказової інформації. Визначено значення автоматизованих систем, електронних баз даних, засобів цифрової фіксації та інтелектуальних алгоритмів у діяльності слідчих та експертних підрозділів. Обґрунтовано необхідність модернізації криміналістичного інструментарію відповідно до сучасних викликів злочинності. Підкреслено важливість поєднання класичних криміналістичних методик із новітніми цифровими технологіями для забезпечення ефективності доказування.

Ключові слова: криміналістика, техніко–криміналістичне забезпечення, цифрові технології, кримінальне провадження, доказова інформація, цифровізація, судова експертиза.

Ostapenko Artur
Head of the Criminalistics Laboratory,
National University «Odesa Law Academy»,
Odesa, Ukraine

TECHNICAL AND CRIMINALISTICS SUPPORT FOR THE INVESTIGATION OF CRIMINAL OFFENSES IN THE CONDITIONS OF DIGITAL TRANSFORMATION

The theses examine the peculiarities of technical and criminalistics support for the investigation of criminal offenses in the context of digital transformation. The influence of digital technologies on the process of detecting, recording, seizing and examining evidentiary information is analysed. The importance of automated systems, electronic databases, digital recording tools and intelligent algorithms in the activities of investigative and forensic units is determined. The necessity of modernizing forensic tools in accordance with modern criminal challenges is substantiated. The importance of

combining classical forensic methods with the latest digital technologies to ensure the effectiveness of evidence is emphasized.

Keywords: criminalistics, technical and forensic support, digital technologies, criminal proceedings, evidentiary information, digitalization, forensic examination.

Розвиток цифрових технологій суттєво вплинув на сучасну систему криміналістичного забезпечення правоохоронної діяльності [1, с. 37]. Сьогодні розслідування кримінальних правопорушень дедалі частіше пов'язане з необхідністю роботи з електронними носіями інформації, цифровими слідами, відеозаписами, даними мобільних пристроїв та мережевими комунікаціями. У таких умовах традиційні криміналістичні засоби поступово інтегруються з цифровими технологіями, що змінює підходи до організації досудового розслідування.

Техніко–криміналістичне забезпечення розслідування кримінальних правопорушень охоплює систему науково–технічних засобів, методів і технологій, спрямованих на ефективне виявлення, фіксацію, вилучення, дослідження та використання доказової інформації [2, с. 114]. У сучасних умовах така система включає не лише класичні криміналістичні засоби, а й цифрові інформаційні платформи, автоматизовані пошукові комплекси, програмні аналітичні системи та інструменти цифрової візуалізації.

Одним із найважливіших напрямів модернізації криміналістичної діяльності є застосування сучасних засобів цифрової фіксації під час проведення слідчих (розшукових) дій [3, с. 91]. Використання цифрової фото– та відеозйомки, панорамної зйомки, 3D–моделювання, лазерного сканування та аерофотозйомки дозволяє створити максимально точну модель місця події. Науковці зазначають, що такі технології сприяють не лише підвищенню якості фіксації доказів, а й забезпечують можливість повторного аналізу слідової картини вже після завершення огляду [4, с. 63].

Особливу роль у сучасній криміналістиці відіграють автоматизовані інформаційно–пошукові системи. Дактилоскопічні, балістичні, генетичні та трасологічні обліки дозволяють швидко здійснювати порівняльний аналіз великої кількості об'єктів та встановлювати взаємозв'язки між окремими кримінальними правопорушеннями [5, с. 205]. Використання таких систем значно скорочує часові витрати під час розслідування та підвищує ефективність розкриття злочинів.

У сучасних умовах особливого значення набуває дослідження цифрових слідів. Йдеться про інформацію, що зберігається на мобільних телефонах, комп'ютерах, серверах, хмарних сервісах та інших електронних носіях [6, с. 74]. Саме цифрові сліди часто стають ключовим джерелом доказової інформації у кримінальних провадженнях, пов'язаних із шахрайством, кіберзлочинністю, незаконним обігом наркотичних засобів, організованою злочинністю та корупційними правопорушеннями.

Науково–технічний прогрес також сприяв активному впровадженню елементів штучного інтелекту у криміналістичну практику [7, с. 118]. Інтелектуальні алгоритми використовуються для автоматичного розпізнавання облич, аналізу відеопотоку, обробки великих масивів даних та прогнозування кримінальних ризиків. Водночас використання таких технологій потребує належної процесуальної регламентації та перевірки достовірності результатів, оскільки автоматизовані системи не можуть повністю замінити професійну оцінку слідчого чи експерта.

Окремої уваги потребує питання професійної підготовки працівників криміналістичних підрозділів. Ефективне використання сучасних цифрових технологій вимагає від фахівців відповідного рівня технічної компетентності, навичок роботи з цифровими доказами та розуміння специфіки інформаційної безпеки [3, с. 94]. Саме тому модернізація техніко–криміналістичного забезпечення має супроводжуватися оновленням системи професійної підготовки та підвищення кваліфікації працівників правоохоронних органів.

Водночас цифровізація криміналістичної діяльності породжує низку процесуальних та етичних проблем. Серед них особливої уваги потребують питання допустимості цифрових доказів, захисту персональних даних, забезпечення цілісності електронної інформації та недопущення втручання в автоматизовані системи [1, с. 42]. У зв’язку з цим важливого значення набуває розроблення єдиних стандартів використання цифрових технологій у кримінальному провадженні.

Таким чином, техніко–криміналістичне забезпечення розслідування кримінальних правопорушень в умовах цифрової трансформації є одним із ключових напрямів розвитку сучасної криміналістики. Ефективність застосування цифрових технологій залежить від належного нормативного регулювання, технічного оснащення правоохоронних органів, наукового супроводу та професійної підготовки фахівців. Інтеграція класичних криміналістичних методик із сучасними цифровими інструментами створює передумови для підвищення ефективності доказування та вдосконалення механізму розслідування кримінальних правопорушень.

Перелік використаних джерел:

1. Варфоломеєва Т. В. Цифровізація криміналістичної діяльності в умовах сучасних викликів. Юридичний науковий електронний журнал. 2024. № 3. С. 36–43.
2. Гора І. В. Криміналістична техніка: сучасний стан та перспективи розвитку: монографія. Київ : Алерта, 2022. 276 с.
3. Матвієнко В. М. Використання цифрових технологій під час проведення слідчих (розшукових) дій. Криміналістичний вісник. 2023. № 2. С. 89–96.

4. Бахін В. П., Салтевський М. В. Технічні засоби фіксації доказової інформації у кримінальному провадженні. Право України. 2022. № 9. С. 58–66.

5. Сорока С. О. Автоматизовані інформаційно–пошукові системи у діяльності правоохоронних органів. Науковий вісник публічного та приватного права. 2024. № 1. С. 201–208.

6. Пясковський В. В. Цифрові сліди як джерело доказової інформації у кримінальному провадженні. Актуальні проблеми держави і права. 2023. № 96. С. 70–78.

7. Тертишник В. М. Штучний інтелект та перспективи його використання у криміналістиці. Вісник кримінального судочинства. 2025. № 1. С. 115–123.

DOI https://doi.org/10.32837/11300.33445

Платовський Сергій
судовий експерт лабораторії психологічних,
мистецтвознавчих та інших видів досліджень
Одеського науково–дослідного інституту судових експертиз
Міністерства юстиції України
м.Одеса, Україна
ORCID: http://orcid.org/0000–0002–3146–1390,
e–mail: rabotaondise@gmail.com

ДОСЛІДЖЕННЯ КОЛЕКЦІЙНИХ ТА ІСТОРИЧНИХ АВТОМОБІЛІВ В ПРАКТИЦІ ОХОРОНИ КУЛЬТУРНОЇ СПАДЩИНИ РЕСПУБЛІКИ ПОЛЬША

У тезах представлені підходи до оцінювання історичних і колекційних транспортних засобів у Республіці Польща як об’єктів культурної спадщини, з акцентом на критерії їх визнання пам’ятками, ступінь оригінальності та історичну цінність.

Ключові слова: історичні транспортні засоби, колекційні автомобілі, культурна спадщина, Республіка Польща, оцінка пам’яток, критерії автентичності, оригінальність, історична цінність.

Platovskiy Serhiy
Forensic expert of the laboratory of psychological,
art history and other types of research of the
Odesa Research Institute of
Forensic Expertise of the Ministry of Justice of Ukraine
Odesa, Ukraine

RESEARCH ON COLLECTIBLE AND HISTORICAL AUTOMOBILES IN THE PRACTICE OF CULTURAL HERITAGE PROTECTION IN THE REPUBLIC OF POLAND

The theses present approaches to the assessment of historical and collectible vehicles in the Republic of Poland as objects of cultural heritage, focusing on the criteria for their recognition as monuments, the degree of originality, and historical value.

Key words: historical vehicles, collectible cars, cultural heritage, Republic of Poland, monument assessment, authenticity criteria, originality, historical value.

Дослідження історичних та колекційних автомобілів у Республіці Польща в останні десятиліття стало важливим напрямом як наукових досліджень, так і практичної діяльності органів охорони культурної спадщини. Особлива увага цій проблематиці приділяється у контексті дослідження транспортних засобів як

об'єктів техніки, що мають історичну, наукову та культурну цінність. Польський досвід становить значний інтерес, оскільки у країні сформувалася достатньо розвинена система обліку та охорони історичних транспортних засобів, а також активно розвивається наукова дискусія щодо критеріїв їх оцінювання.

Однією з ключових проблем, на які звертають увагу польські дослідники, є відсутність чітких і універсальних критеріїв визнання автомобіля чи мотоцикла об'єктом культурної спадщини. У науковій літературі та адміністративній практиці одночасно використовуються різні поняття: «історичний транспортний засіб», «колекційний транспортний засіб», «унікальний транспортний засіб», «транспортний засіб–пам'ятка». Попри зовнішню схожість, ці категорії мають різне правове та культурне значення.

Вагомий внесок у дослідження цієї проблематики зробив польський історик права та дослідник охорони пам'яток Кароль Лопатецький. У своїй праці, присвяченій оцінюванню пам'яток на прикладі транспортних засобів, він наголошує, що головним критерієм історичної цінності автомобіля є не лише його вік, а здатність виступати «свідченням минулої епохи» або важливої історичної події [2]. Такий підхід суттєво розширює традиційне розуміння історичного автомобіля виключно як «старого транспортного засобу».

У польській практиці велике значення надається віковому критерію, однак він не розглядається як єдиний чи визначальний. Протягом останніх десятиліть мінімальний вік транспортних засобів, які можуть розглядатися як об'єкти культурної спадщини, поступово збільшувався. Якщо раніше орієнтиром часто виступав вік у 25 років, то сьогодні у практиці воєводських органів охорони пам'яток дедалі частіше використовуються межі 30–40 років, а в окремих випадках навіть 50 років. Подібна тенденція пов'язана як зі збільшенням середнього віку автомобілів, так і з необхідністю суворішого відбору об'єктів, які справді мають культурну цінність.

Важливою особливістю польського підходу є розуміння специфіки транспортних засобів як об'єктів масового промислового виробництва. Автомобілі XX століття випускалися великими серіями, що відрізняє їх від традиційних творів мистецтва або унікальних архітектурних об'єктів. У зв'язку з цим польські дослідники підкреслюють, що історична цінність визначається не лише моделлю транспортного засобу, а насамперед конкретним екземпляром, його історією, походженням і ступенем збереженості.

Особливе значення у польській системі оцінювання транспортних засобів має критерій автентичності. Органи охорони пам'яток приділяють значну увагу збереженню оригінальних конструктивних елементів автомобіля. В експертній практиці Польщі наразі використовується орієнтир у 75% збереження оригінальних деталей. Значна модернізація транспортного засобу або використання сучасних замінників може стати підставою для відмови у включенні об'єкта до воєводського обліку пам'яток [1].

Водночас польська практика враховує специфіку експлуатації транспортних засобів. Автомобілі та мотоцикли є технічними об'єктами, які неминуче піддаються ремонту, зносу та заміні окремих деталей. Тому оцінювання автентичності здійснюється комплексно, з урахуванням характеру проведених змін і ступеня збереження історичної матеріальної основи об'єкта.

Важливе місце у польських дослідженнях займає проблема визначення так званої «минулої епохи». На думку того ж К. Лопатецького, історичною межею для транспортних засобів можна вважати період 1989–1991 років, пов'язаний із розпадом соціалістичного блоку, глобалізацією виробництва та трансформацією світової автомобільної промисловості. Саме автомобілі, створені до цього періоду, найповніше відображають завершену індустріальну епоху, пов'язану з класичним автомобілебудуванням XX століття [2].

Подібний підхід має особливе значення для країн Центральної та Східної Європи, оскільки транспортні засоби соціалістичного періоду розглядаються не лише як технічні об'єкти, а і як елементи соціальної, промислової та повсякденної історії. У польській практиці історичну цінність можуть мати не лише рідкісні спортивні автомобілі чи довоєнні моделі, а й масові транспортні засоби, характерні для певного історичного періоду.

Суттєву увагу польські дослідники приділяють також індивідуальній історії конкретного автомобіля. Участь транспортного засобу в історичних подіях, його належність відомим особам, зв'язок із певними суспільними процесами або спортивними досягненнями можуть істотно підвищувати культурну цінність об'єкта. Саме тому у сучасній польській практиці великого значення набуває дослідження походження автомобіля, архівних матеріалів, реєстраційних документів та історії експлуатації.

Ще однією важливою тенденцією є зростання суспільного інтересу до історичних транспортних засобів. У Польщі спостерігається постійне збільшення кількості заяв про включення автомобілів і мотоциклів до воєводського обліку пам'яток. Це свідчить про поступове формування ставлення до історичних транспортних засобів як до повноцінної частини культурної спадщини [3].

Сучасні польські дослідження у цій сфері поєднують історичні, правові, технічні та експертні підходи. Завдяки цьому формується комплексна система оцінювання історичних і колекційних автомобілів, яка враховує не лише технічні характеристики об'єкта, а й його культурне, історичне та суспільне значення. Досвід Республіки Польща становить значний інтерес для подальшого розвитку досліджень та експертної практики у сфері охорони технічної спадщини в інших країнах Європи, зокрема й в Україні.

Перелік використаних джерел:

1. Cel i zakres ewidencji zabytków nieruchomych. URL: https://nid.pl/wp–content/uploads/2021/12/Cel–i–zakres–ewidencji–zabytkow–NIERUCHOMYCH.pdf.

2. Łopatecki K. Wartościowanie zabytków na przykładzie środków transportu. Z badań nad problematyką włączania pojazdódo wojewódzkiej ewidencji zabytków. URL: https://www.researchgate.net/publication/387502546_Wartosciowanie_zabytkow_na_przykladzie_srodkow_transportu_Z_badan_nad_problematyka_wlaczania_pojazdowdo_wojewodzkiej_ewidencji_zabytkow.

3. Pojazdy zabytkowe. URL: http://wkz.katowice.pl/uslugi/wojewodzka–ewidencja–zabytkow/pojazdy–zabytkowe.

DOI https://doi.org/10.32837/11300.33446

Савчук Олена
завідувач лабораторії почеркознавчих та технічних досліджень документів Львівського науково – дослідного інституту судових експертиз Міністерства юстиції України,
м. Львів, Україна
ORCID: https://orcid.org/0009–0006–3713–4741
e–mail:o.savchuk.lndise@gmail.com

ПОЧЕРКОЗНАВСТВО В ЦИФРОВУ ЕПОХУ: ВІД КЛАСИЧНИХ ОЗНАК ДО НОВИХ МОДЕЛЕЙ ІДЕНТИФІКАЦІЇ

В тезах досліджено зміну ознак почерку під впливом цифровізації та її вплив на достовірність експертного висновку. Визначено напрями формування підходів, що забезпечують стійку ідентифікацію підписів у цифровому середовищі.
Ключові слова: почеркознавство, ідентифікація, підпис.

Savchuk Olena
Head of the Handwriting and Document Technical Examination Laboratory of the Lviv Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine,
Lviv, Ukraine

FORENSIC HANDWRITING IN THE DIGITAL ERA: FROM CLASSICAL FEATURES TO NEW IDENTIFICATION MODELS

The study examines changes in handwriting features under digitalization and their impact on the reliability of expert conclusions. It outlines approaches that ensure stable signature identification in a digital environment.
Keywords: handwriting analysis, identification, signature

Трансформація ідентифікаційних ознак почерку в умовах загальної тенденції до цифровізації виступає неминучим технічним етапом розвитку криміналістики. Цей процес за своїм походженням охоплює нейрофізіологію, математичне моделювання та складні правові конструкції. В час, коли стилус витісняє традиційні ручки, а сенсорний екран – звичайний папір, почеркознавча експертиза стикається з проблемою застосування класичних ідентифікаційних ознак до підписів, виконаних за допомогою сучасних технологічних засобів. Водночас виникає необхідність створення такої доказової бази, яка відповідатиме стандартам цифрової епохи та успішно проходитиме судову перевірку.

Століттями традиційне письмо на папері формувало сталий динамічний стереотип, коли сила тертя пишучого засобу об папір забезпечувала природний

зворотний зв'язок для моторики. У цифровому середовищі взаємодія між стилусом та склом є мінімальною, що призводить до підсвідомого, рефлекторного прискорення рухів. Це в свою чергу спотворює мікроструктуру елементів: петлі звужуються, кути загострюються, нівелюється диференціація натиску. Тому зразки почерку чи підпису однієї і тієї ж особи, виконані на папері та на планшеті, можуть виглядати як виконані різними особами За відсутності експертних методик, адаптованих до такої ситуації, виникає доволі високий ризик помилкового негативного висновку, коли природні зміни моторики в цифрових умовах хибно трактуються як ознаки підробки. Як зазначає А.Чепелюк, «модифікація ознак почерку зумовлена специфікою взаємодії в системі «рука – стилус – екран», де зміна кінестетичного зворотного зв'язку (відсутність звичного опору паперу) веде до трансформації як просторових, так і динамічних характеристик підпису» [1, с. 114].

Інтеграція цифрового підпису в систему доказів стикається з низкою проблемних питань, що мають як технічний, так і суто методологічний характер.

Попри загальну тенденцію до цифровізації криміналістичних досліджень, у науковому середовищі зберігається обґрунтована позиція, згідно з якою цифрові масиви даних (зокрема, формати, які містять координати руху пера, тиску та часові мітки) не можуть розглядатися як самостійний об'єкт судово–почеркознавчої експертизи у класично прийнятому розумінні.

Передусім це пов'язано з відсутністю матеріальної фіксації рукописного підпису. Традиційна криміналістична доктрина виходить із того, що об'єктом почеркознавчого дослідження є рукопис, тобто, матеріально закріплений слід психофізіологічної діяльності особи на фізичному носії (папері). У випадку цифрового масиву даних безпосередній рукописний слід взагалі відсутній: експерту довелося б працювати не з штрихами, а з їх математичним відтворенням. Між рухом руки та отриманим файлом існує програмне середовище, яке обробляє сигнали шляхом оцифрування, фільтрування та реконструкції. Таким чином, об'єктом дослідження фактично стає не сам слід письма, а його програмно оброблена модель, що вже змінює природу первинної інформації. Аналізуючи стрімку інтеграцію ІТ–технологій у криміналістичну науку, слід розуміти, що цифровізація правосуддя загалом вимагає не просто механічного перенесення старих методик на цифрові носії, а насамперед фундаментального переосмислення поняття «матеріального сліду» [2, с. 45].

На відміну від паперу, який має відносно стабільні характеристики, цифрові пристрої суттєво відрізняються за роздільною здатністю сенсора, частотою дискретизації (зчитування) та чутливістю до натиску. Підпис, виконаний на бюджетному смартфоні, матиме значно нижчу ідентифікаційну інформативність, ніж такий самий підпис, виконаний на професійному графічному планшеті. Для експерта це потенційно означало б роботу із непорівнюваними даними: неможливо об'єктивно зіставити динамічні параметри, якщо вони були записані різними технічними засобами з різною допустимою похибкою.

Другою суттєвою проблемою є втрата автентичності через оцифровування даних. Будь–який цифровий запис є переривчастим і фіксується з певною частотою (наприклад, від 60 до 200 вимірювань за секунду). Якщо планшет фіксує 60 Гц, то підпис буде більш кутастим, якщо 200 Гц, то лінії зображення будуть плавнішими і точнішими. В будь–якому випадку між зафіксованими точками існує інформаційний розрив, який штучно заповнюється. У класичному рукописі навпаки, штрих є безперервним фізичним слідом руху руки, що містить мікроознаки (дрібні коливання, тремор, зміни ступеня натиску, рефлекторні штрихи, нематеріальні зв'язки). При цифровій передачі частина цих ознак може бути втрачена або спотворена, що знижує ідентифікаційну цінність об'єкта.

Критичним є питання відсутності єдиної національної та міжнародної бази референтних значень. У традиційному почеркознавстві експерт спирається на розроблені десятиліттями альбоми ознак та відносно зрозумілу з теорії і практики частотність їх появи. У цифровому ж середовищі ми не маємо достатніх статистичних даних про те, які зміни швидкості чи натиску є звичними і природніми для певної вікової групи в умовах письма на склі. Це породжує суб'єктивізм: один експерт може трактувати різку зміну швидкості як ознаку технічної підробки, а інший – як особливість ковзання стилуса по екрану графічного планшета.

Важливим аргументом є також проблема сприйняття об'єкта експертизи. Судово–почеркознавче дослідження традиційно має візуально–порівняльний характер і передбачає можливість безпосереднього огляду об'єкта. Однак набір числових координат в певному комп'ютерному форматі не є безпосередньо сприйнятним для людини без використання спеціального програмного забезпечення. Експерт фактично досліджує не сам підпис, а його візуалізоване відтворення, реконструкцію підпису в іншому просторі. У такому випадку виникає питання: що саме є об'єктом дослідження: файл, цифровий масив чи його графічне відображення, сформоване алгоритмом.

Окремо слід враховувати юридичну невідповідність процесуальним класифікаціям доказів. У більшості процесуальних систем докази поділяються на речові, письмові та електронні. Почеркознавча експертиза історично належить до експертизи з дослідження речових доказів, тобто, матеріальних об'єктів, які можна оглядати, зберігати та ідентифікувати без зміни їхньої суті. Натомість цифровий масив координат є формою електронної інформації, яка за своєю природою ближча до предмета комп'ютерно–технічної експертизи, ніж до класичного почеркознавства.

У традиційній почеркознавчій експертизі документ із рукописним текстом чи підписом є стійким, стабільним матеріальним носієм, зміни якого можна виявити шляхом мікроскопічного та фізико–хімічного аналізу. Натомість цифрові дані можуть бути змінені без залишення візуально доступних слідів, особливо за відсутності криптографічного захисту або належного протоколювання. Це ставить під сумнів автентичність масиву цифрових даних як об'єкта дослідження, оскільки

неможливо гарантовано підтвердити його походження без додаткових технічних засобів перевірки.

Не менш важливою є невідповідність таких даних чинним методикам почеркознавчого дослідження. Сучасні експертні методики орієнтовані на аналіз динамічних характеристик штрихів. У цифровому масиві ці параметри зводяться до певних числових значень (наприклад, рівня тиску пишучого пристрою за шкалою умовних одиниць). Відсутність фізичного носія штриха унеможливлює застосування класичних методів, що означає потребу в створенні та затвердженні принципово нових, ще не стандартизованих підходів.

У реаліях сьогодення цифровий масив координат поки що не може розглядатися як об'єкт почеркознавчого дослідження. Він виступає лише технічним середовищем фіксації інформації про рухову активність особи. Лише комплексне оновлення, починаючи від технічних стандартів і до формулювання коректних юридичних дефініцій та наукових методик, потенційно дозволить перетворити такий підпис в об'єкт почеркознавчого дослідження та забезпечити високу точність і актуальність висновків.

Перелік використаних джерел.

1.Чепелюк А. О. Особливості дослідження підписів, виконаних на цифрових пристроях (планшетах) за допомогою стилуса. *Криміналістичний вісник.* 2022. № 1 (37). С. 110–117.

2.Благута Р. І. Цифрова трансформація криміналістичної науки та судово–експертної діяльності: теоретичні та прикладні аспекти. *Вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2023. № 2. С. 41–49.

DOI https://doi.org/10.32837/11300.33447
Салтиков Олександр
завідувач Миколаївського відділення Одеського науково–дослідного інституту судових експертиз Міністерства юстиції України,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0002–6628–9743
e–mail:exsasha@ukr.net

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ: МОЖЛИВОСТІ ТА РИЗИКИ

У тезах проаналізовані можливості використання штучного інтелекту в судово–експертній діяльності та пов’язані з цим ризики. Наголошено на можливому виникненні помилок та необхідності перевірки результатів, отриманих за допомогою алгоритмів штучного інтелекту.
Ключові слова: судова експертиза, штучний інтелект, ризики, безпека.

Saltykov Oleksandr
Head of the Mykolaiv Branch of the Odesa Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine
Odesa, Ukraine

THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ACTIVITY: OPPORTUNITIES AND RISKS

The theses analyze the possibilities of using artificial intelligence in forensic expert activity and the risks associated with its implementation. Particular attention is paid to the potential occurrence of errors and the necessity of verifying results obtained through artificial intelligence algorithms.
Keywords: forensic examination, artificial intelligence, risks, security.

Сучасний етап розвитку суспільства характеризується безпрецедентним науково–технічним прогресом, що характеризується швидким розвитком технологій та втіленням нових розробок у життя людини, перетворенням науки на головну виробничу силу та глобальними змінами у всіх сферах життя. Функціональний потенціал штучного інтелекту (ШІ) охоплює здатність до міркування, моделювання мислення, вирішення комплексних завдань та ухвалення рішень.

Маючи значний технологічний потенціал, наразі технології ШІ стрімко розвиваються та інтегруються у більшість сфер людської життєдіяльності – від фінансового сектору та логістики до сфери охорони здоров’я та публічного управління. Одним з прикладів такої інтеграції є автономний транспорт, здатний

самостійно аналізувати дорожню обстановку й оперативно приймати рішення, реагуючи на її зміни.

Одним з типів ШІ, який набуває дедалі більшого значення, дозволяючи машинам аналізувати візуальні дані, такі як зображення та відео, є «комп'ютерний зір». Ця технологія використовується в таких додатках, як безпілотні автомобілі та системи розпізнавання обличь. Комп'ютерний зір включає кілька етапів, зокрема: отримання зображень, обробку зображень, виокремлення ознак, розпізнавання об'єктів [1].

Під час втілення новітніх технологій у сучасній судово–експертній діяльності «цифрову трансформацію» слід розуміти як комплексну роботу над побудовою екосистеми цифрових рішень у різних сферах – освіти, науки, включно зі створенням безпечного електронного освітнього середовища, забезпеченням необхідної цифрової інфраструктури закладів та установ освіти і науки, підвищення рівня цифрової компетентності, цифровою трансформацією процесів та послуг, а також автоматизацією збору і аналізу даних [2].

У межах реалізації цього підходу важливим практичним кроком став запуск Міністерством юстиції України у 2025 році першого сервісу на базі штучного інтелекту для замовників судових експертиз і експертних досліджень.

За інформацією пресслужби Мін'юсту: «Новий AI–помічник покликаний спростити підготовку документів і підвищити якість звернень до експертів. Сервіс допомагає сформувати заяву або постанову про призначення експертизи, підказує оптимальний вид дослідження, дає змогу визначити об'єкти експертизи та коректно сформулювати запитання для експерта. Скористатися інструментом можуть фізичні особи, адвокати та слідчі, які замовляють судові експертизи або експертні дослідження. Очікується, що сервіс дозволить уникнути типових помилок уже на етапі підготовки документів. Пілотний проєкт реалізовано на базі Науково–дослідного центру незалежних судових експертиз Міністерства юстиції України» [3].

Проте, навіть за наявності сучасних можливостей використання новітніх технологій, важливо не нехтувати обов'язками, які покладені на експерта при виконанні судових експертиз та експертних досліджень, а саме: експерт зобов'язаний особисто провести повне дослідження, дати обґрунтований та об'єктивний письмовий висновок на поставлені питання, а в разі необхідності – роз'яснити його.

Враховуючи викладене, можна припустити, що частину рутинної роботи експерта цілком доцільно перекласти на штучний інтелект як на своєрідного співвиконавця. Наприклад, це може стосуватися виконання завдань щодо відбору нормативно–правових актів і літератури, аналізу та порівняння характеристик даних, отриманих під час огляду об'єкта чи вивчення документів, а також проведення необхідних для висновку обрахунків (зокрема, щодо обсягів чи вартості). Проте детальний аналіз отриманих результатів та остаточні висновки повинні бути виключно у компетенції експерта.

Штучний інтелект не може цілком замінити людину у професійному світі, але може стати важливим допоміжним інструментом, який при мудрому використанні може значно посилити якість виконуваних робіт. Така допоміжна роль зумовлена тим, що замість сліпого виконання жорстких інструкцій, ШІ використовує математичні алгоритми та нейронні мережі для аналізу й пошуку закономірностей у величезних обсягах інформації.

Крім того, при використанні технологій штучного інтелекту доцільно враховувати супутні ризики, зокрема специфічні збої у генерації даних, відомі як «галюцинації» системи. Вчені доводять, що це не просто помилки тренування, а математично неминучий ефект роботи моделей. Вказане зумовлено тим, що ШІ формує відповіді шляхом послідовного прогнозування слів, що, своєю чергою, призводить до накопичення похибок у реченнях. Дослідники наголошують, що навіть за умови використання бездоганних тренувальних масивів, рівень помилок під час побудови тексту залишається високим, і він прямо залежить від частоти згадування конкретного факту в базі даних. Як наслідок, помилки в алгоритмах, недостатнє тестування та ігнорування етичних аспектів розробки здатні призводити до значних соціально–правових наслідків. Зазначені чинники підкреслюють необхідність відповідального підходу до створення та використання систем ШІ, де безпека, надійність і врахування можливих ризиків є головним пріоритетом [4].

Підсумовуючи результати проведеного дослідження, слід наголосити, що замовникам та виконавцям судових експертиз та експертних досліджень, у разі залучення до їх проведення алгоритмів штучного інтелекту, необхідно ретельно перевіряти отримані результати, зокрема проміжні розрахунково–аналітичні дані та наведені нормативно–джерельні посилання.

Перелік використаних джерел:

1. Штучний інтелект (ШІ) – що це таке, як працює і навіщо потрібен [Електронний ресурс]. URL: https://termin.in.ua/shtuchnyy–intelekt/

2. Цифрова трансформація освіти і науки [Електронний ресурс]. URL: https://mon.gov.ua/tag/tsifrova–transformatsiya–osviti–i–nauki?&tag=tsifrova–transformatsiya–osviti–i–nauki

3. Штучний інтелект у судовій сфері: Мін’юст впровадив AI–помічника для експертиз [Електронний ресурс]. URL: https://delo.ua/news/stucnii–intelekt–u–sudovii–sferi–minyust–vprovadiv–ai–pomicnika–dlya–ekspertiz–457285/

4. Користувачам не сподобається. OpenAI пояснила, чому ШІ помиляється, і як це виправити [Електронний ресурс]. URL: https://techno.nv.ua/ukr/it–industry/galyucinaciji–v–shi–chomu–pomilki–neminuchi–navit–za–idealnih–danih–50545642.html

DOI https://doi.org/10.32837/11300.33462

Сидорчук Інна
викладач Академічного фахового коледжу ОНЮА,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0005–6894–1872
e–mail: inna21511@gmail.com

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ СУДОВОЇ ЕКСПЕРТИЗИ

У тезах досліджено роль цифрових технологій та штучного інтелекту у підвищенні ефективності судової експертизи в умовах цифровізації сучасного суспільства. Проаналізовано основні напрями впровадження цифрових інструментів у систему експертного забезпечення правосуддя, зокрема автоматизацію аналізу даних, використання алгоритмів машинного навчання, нейронних мереж та технологій обробки цифрової інформації.

Ключові слова: цифрові технології, штучний інтелект, судова експертиза, правосуддя, машинне навчання, нейронні мережі, цифровізація.

Sydorchuk Inna
Teacher, Academic Professional College ONUA,
Odesa, Ukraine

THE ROLE OF DIGITAL TECHNOLOGIES IN IMPROVING THE EFFICIENCY OF FORENSIC EXAMINATION

The theses examine the role of digital technologies and artificial intelligence in improving the efficiency of forensic examination in the context of the digitalization of modern society. The main directions of implementing digital tools into the system of expert support for justice are analyzed, including the automation of data analysis, the use of machine learning algorithms, neural networks, and digital information processing technologies.

Keywords: digital technologies, artificial intelligence, forensic examination, justice, machine learning, neural networks, digitalization.

У сучасних умовах розвитку суспільства цифрові технології все активніше впроваджуються у різні сфери діяльності людини, зокрема й у систему правосуддя. Особливого значення вони набувають у сфері судової експертизи, адже сприяють підвищенню швидкості, точності та об’єктивності проведення експертних досліджень. Використання сучасних цифрових інструментів дозволяє значно спростити процес обробки інформації та підвищити ефективність роботи судових експертів.

Одним із головних напрямів цифровізації судової експертизи є автоматизація аналізу даних. Сучасні комп'ютерні програми здатні швидко обробляти великі обсяги інформації, порівнювати дані та виявляти важливі закономірності. Наприклад, у криміналістиці активно використовуються цифрові системи розпізнавання відбитків пальців, аналізу почерку, голосу або відеоматеріалів. Це допомагає експертам швидше отримувати результати та зменшує ймовірність людської помилки.

Як вказують вітчизняні науковці І. Пугач та В. Харченко «запровадження алгоритмів машинного навчання, зокрема рекурентних і глибинних нейронних мереж, дозволяє аналізувати великі обсяги даних та виявляти приховані взаємозв'язки між різними чинниками. Завдяки цьому стає можливим більш точне встановлення причинно–наслідкових зв'язків, а також прогнозування подальшого розвитку подій» [1, с. 267].

Британська ІТ–компанія NEC Software Solutions UK, яка спеціалізується на розробці програмного забезпечення та цифрових рішень для державного сектору, правоохоронних органів, медицини, місцевого самоврядування та систем громадської безпеки зазначає: «з переходом до епохи глибокого навчання експерти отримали змогу аналізувати відеозаписи та фотозображення з високою точністю, а обробка природної мови (NLP) – розбирати великі масиви текстових даних, наприклад електронні листи чи чати. Була створена низка міжнародних проєктів, що демонстрували здатність ШІ прогнозувати наслідки кримінальних подій, наприклад, система Connect у Великобританії, яка інтегрувала оперативні та аналітичні дані для формування цілісної картини злочинності» [4].

Важливу роль відіграє також штучний інтелект, який може застосовуватися для аналізу електронних доказів, пошуку необхідної інформації та прогнозування можливих результатів дослідження. Завдяки цьому значно скорочується час проведення експертизи, а сам процес стає більш точним та ефективним. Крім того, цифрові технології забезпечують можливість дистанційної взаємодії між експертами, судами та правоохоронними органами, що особливо актуально в умовах воєнного стану та розвитку електронного судочинства.

Ю Чечіль досить ґрунтовно зауважує, що сучасні алгоритми штучного інтелекту все активніше впроваджуються у сферу судової експертизи. Зокрема, у цифровій експертизі використовуються моделі машинного навчання для автоматичного виявлення ознак фальсифікації цифрових зображень, зокрема deepfake–контенту, а також для визначення каналів витоку конфіденційної інформації за допомогою аналізу метаданих. У документознавчих дослідженнях ШІ застосовується для класифікації документів, виявлення підроблених підписів та аналізу стилістичних особливостей тексту. У фонографічній експертизі технології штучного інтелекту допомагають автоматично розпізнавати голос, ідентифікувати осіб за мовленням та виявляти монтаж аудіозаписів. Крім того, у психологічних експертизах ШІ використовується для прогнозування поведінкових моделей на

основі аналізу різних даних, зокрема інформації із соціальних мереж, що дозволяє оцінювати ризики девіантної поведінки окремих осіб або груп [3, с. 298].

Саме тому сьогодні особлива увага приділяється формуванню принципів відповідального та безпечного використання штучного інтелекту у правовій сфері. Зокрема, як зазначено у розроблених Міністерством цифрової трансформації України Рекомендаціях з відповідального використання штучного інтелекту для правників: «ШІ стане інструментом посилення професійної експертизи, а не загрозою для неї» [2].

Отже, використання штучного інтелекту у сфері судової експертизи значно підвищує швидкість, точність та ефективність проведення експертних досліджень. Сучасні цифрові технології дозволяють автоматизувати складні процеси аналізу інформації, виявляти приховані ознаки підробки та більш об'єктивно оцінювати отримані дані. Водночас активне впровадження ШІ потребує належного правового регулювання, забезпечення кібербезпеки та контролю за достовірністю результатів, оскільки остаточне рішення у сфері правосуддя має залишатися за людиною.

Разом із перевагами використання цифрових технологій існують і певні ризики. Серед них можна виділити загрозу витоку конфіденційної інформації, кібератаки, технічні помилки програмного забезпечення та недостатнє правове регулювання використання штучного інтелекту у сфері правосуддя. Тому важливо забезпечити належний рівень кібербезпеки та вдосконалити законодавчу базу щодо застосування цифрових технологій у судово–експертній діяльності.

Перелік використаних джерел:

1. Пугач І., Харченко В. Сучасні цифрові технології в судово–експертній діяльності: виклики та перспективи розвитку гірничотехнічної експертизи : матеріали Міжнародної науково–практичної конференції «Діджиталізація судово–експертної науки в умовах воєнного стану». (Харків, 08.11.2024). Харків, 2024. С. 264–267.

2. Рекомендації з відповідального використання штучного інтелекту для правників. Міністерством цифрової трансформації України. 2025. URL: https://thedigital.gov.ua/news/yak–bezpechno–pratsyuvati–z–shi–rekomendatsii–dlya–pravnikiv.

3. Чечіль Ю. Інтеграція цифрових технологій у судово–експертну діяльність. Електронне наукове видання «Аналітично–порівняльне правознавство». 2025. № 5. С. 296–303.

4. NEC Software Solutions UK secures another eight years providing tech for the core policing platform «Athena». NEC. 08.10.2021 URL: https://www.nec.com/en/press/202110/global_20211008_05.html?utm_source=chatgpt.com.

DOI https://doi.org/10.32837/11300.33515
Смирнов Максим
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу Національного університету
«Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–4563–5902
e–mail: smirnov_maksim@ukr.net

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У РОЗСЛІДУВАННІ ЗЛОЧИНІВ В ДАРКНЕТ (DARKNET)

У роботі розглянуто особливості міжнародного співробітництва у розслідуванні злочинів, що вчиняються з використанням Даркнету. Акцентовано увагу на тому, що стрімка цифровізація злочинності, використання технологій анонімізації, зашифрованих каналів зв'язку, прихованих доменів та конфіденційних криптовалют істотно ускладнюють процес виявлення, документування й доказування протиправної діяльності. Визначено основні технічні та процесуальні проблеми розслідування злочинів у Даркнеті, серед яких складність деанонімізації користувачів, транскордонний характер злочинної діяльності, проблеми юрисдикції, швидкоплинність цифрових доказів та відмінності національних законодавств щодо їх збирання і використання. Обґрунтовано, що ефективне розслідування таких злочинів неможливе виключно національними засобами та потребує оперативної міжнародної взаємодії, зокрема через канали Інтерполу, Європолу, спільні слідчі групи, механізми міжнародної правової допомоги та обмін цифровою інформацією в режимі реального часу. Зроблено висновок, що протидія злочинності в Даркнеті вимагає комплексного підходу, який поєднує цифрову криміналістику, аналіз криптовалютних транзакцій, OSINT–інструменти, спеціальні процесуальні механізми та удосконалені форми міжнародного співробітництва.

Ключові слова: Даркнет, цифрова криміналістика, кіберзлочинність, міжнародне співробітництво, цифрові докази, анонімізація, Tor, I2P, криптовалюти, Інтерпол, Європол, транснаціональна злочинність

Smirnov Maksym
Candidate of Legal Sciences, Associate Professor,
Associate Professor of the Department of Criminal Procedure
National University «Odesa Law Academy»
Odesa, Ukraine

INTERNATIONAL COOPERATION IN THE INVESTIGATION OF CRIMES IN THE DARKNET

The paper examines the specific features of international cooperation in the investigation of crimes committed through the Darknet. Particular attention is paid to the fact that the rapid digitalization of crime, the use of anonymization technologies, encrypted communication channels, hidden domains and privacy–oriented cryptocurrencies significantly complicate the detection, documentation and proof of illegal activity. The main technical and procedural problems of investigating Darknet crimes are identified, including the difficulty of user deanonymization, the cross–border nature of criminal activity, jurisdictional issues, the volatility of digital evidence and differences in national legislation concerning its collection and use. It is substantiated that the effective investigation of such crimes is impossible by national means alone and requires prompt international interaction, in particular through Interpol and Europol channels, joint investigation teams, mutual legal assistance mechanisms and real–time exchange of digital information. It is concluded that countering crime in the Darknet requires a comprehensive approach combining digital criminalistics, cryptocurrency transaction analysis, OSINT tools, special procedural mechanisms and improved forms of international cooperation.

Keywords: Darknet, digital criminalistics, cybercrime, international cooperation, digital evidence, anonymization, Tor, I2P, cryptocurrencies, Interpol, Europol, transnational crime.

Сучасна криміналістика та розслідування вийшли далеко за межі традиційної дактилоскопії. Розслідування сьогодні – це високотехнологічна сфера, цифрова криміналістика, розвідка за відкритими даними, аналіз цифрових слідів, відстеження «брудних» криптогаманців тощо.

Стрімка цифровізація злочинності призвела до розширення тіньового сегмента Інтернету, що створило нові виклики для органів досудового розслідування. Анонімність Даркнету та використання зашифрованих каналів зв’язку значно ускладнюють процес документування протиправної діяльності та збирання доказів, необхідних для притягнення злочинців до відповідальності.

Даркнет являє собою приховану, анонімну та неконтрольовану частину Інтернету, яка не індексується звичайними пошуковими системами такими, як наприклад, Google і недоступна через стандартні браузери (Chrome, Opera, Safari тощо). Основний принцип роботи Даркнету, як багато хто вважає, це повна анонімність користувачів та власників сайтів. Він працює децентралізовано, доступ до нього здійснюється через спеціальні браузери, які маршрутизують зашифровані повідомлення через декілька серверів, щоб приховати місце знаходження користувача. Користувачі Даркнету можуть зберігати практично повну анонімність, яка досягається завдяки спеціальним технологіям передачі даних, зокрема:

1) спеціалізоване програмне забезпечення. Для входу в Даркнет потрібне спеціальне програмне забезпечення, найпопулярнішим з яких є Tor (The Onion Router) Browser або мережа I2P (Invisible Internet Project);

2) «цибулева» та «часникова» маршрутизація. Дані проходять через ланцюжок випадкових проміжних серверів (вузлів) у всьому світі. На кожному етапі інформація шифрується «шарами», тому жоден вузол не бачить одночасно джерело і кінцевий пункт призначення;

3) приховані домени. Сайти в Даркнеті зазвичай мають доменне закінчення .onion (у мережі Tor). Ці адреси складаються з випадкових наборів символів, що робить їх важкими для відстеження;

4) відсутність централізації. Мережа не має єдиного центру управління, що робить її неможливою для цензурування, керування або відключення державними органами;

5) невідстежувані криптовалюти. Монети конфіденційності або Privacy Coins використовують спеціальні криптографічні технології для приховування деталей транзакцій, таких як адреси відправника, отримувача та сума переказу.

Використання технологій Tor, I2P, «цибулевої» та «часникової» маршрутизації та невідстежуваних криптовалют (Monero, Zcash, Dash) створило сприятливе середовище для торгівлі наркотиками, зброєю, персональними даними, дитячою порнографією, надання послуг хакерів тощо. Оскільки сервери, адміністратори та покупці зазвичай перебувають у різних юрисдикціях, розслідування таких злочинів національними силами є фактично неможливим без ефективного міжнародного співробітництва.

Особливість злочинів у Даркнеті обумовлена транснаціональним характером мережі, використанням технологій анонімізації та складністю збирання доказів для їх використання у кримінальному провадженні. Можна виділити основні технічні та юридичні (процесуальні) особливості таких злочинів, зокрема:

1) складність ідентифікації (деанонімізація). «Цибулева» та «часникова» маршрутизація, використання Tor та I2P приховує IP–адресу користувача, що робить традиційні методи відстеження (наприклад, запити до провайдерів) неефективними. Крім цього, більшість транзакцій у Даркнеті здійснюється в анонімних криптовалютах, що ускладнює відстеження фінансових транзакцій;

2) специфічні види злочинів. Даркнет є основним майданчиком для незаконних ринків (торгівля наркотиками, зброєю, фальшивими документами тощо), cybercrime–as–a–Service (продаж шкідливого програмного забезпечення, послуг DDoS–атак та викрадених даних), розповсюдження забороненого контенту (дитячої порнографії);

3) екстериторіальність та питання юрисдикції. Це одна з найбільших перешкод для проведення швидкого розслідування злочинів в кіберпросторі. Вона перетворює розслідування в надскладний та надзвичайно тривалий процес. Проблема полягає в тому, що злочинці, сервери з незаконним контентом та потерпілі зазвичай перебувають у різних країнах. Це створює проблему «втрати місця розташування», коли правоохоронці не можуть встановити фізичне місцезнаходження сервера або підозрюваного через проксі–сервери та VPN.

Якщо, наприклад, злочинець в Україні використовує сервер у Панамі для атаки на банк у США, то виникає юридично складна ситуація, де дії є злочином за законами США, докази зберігаються під юрисдикцією Панами, а підозрюваний перебуває на території України;

4) складний процес збирання доказів та розслідування в цілому. Традиційні механізми міжнародної правової допомоги при розслідуванні таких злочинів не працюють, тому що занадто повільні для цифрового середовища, де дані можуть бути видалені за секунди. Крім того, відмінність національних законодавств щодо цифрових доказів та статусу криптовалют ускладнює їх визнання та використання в судах.

Оскільки сервери та суб'єкти правопорушень часто перебувають у різних юрисдикціях, ключовим фактором успішного розслідування стає оперативна взаємодія через канали Інтерполу та Європолу для фіксації цифрових слідів у режимі реального часу. Тому розслідування таких злочинів вимагає не лише оновлення технічного інструментарію кіберполіції, а й розробки нових, більш ефективних форм міжнародного співробітництва.

Для оперативного розслідування злочинів у цифровому середовищі та Даркнеті необхідний комплексний підхід, що поєднує спеціальні технічні інструменти, процесуальні дії та міжнародну взаємодію. Міжнародне співробітництво у розслідуванні злочинів у Даркнеті є критично важливим, оскільки анонімність та транскордонність цієї мережі не дозволяють одній країні самостійно проводити розслідування та збирати докази.

DOI https://doi.org/10.32837/11300.33516

Туляков Вячеслав
доктор юридичних наук,
професор, член–кореспондент НАПрН України,
професор кафедри кримінального права,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–7513–7714,
e–mail: tuliakov@onua.edu.ua

ЄВРОПЕЙСЬКЕ ЗАКОНОДАВСТВО З ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ: НОВІ ВИКЛИКИ ДЛЯ УКРАЇНИ

Стаття аналізує нові AML–стандарти ЄС та виклики для України в контексті євроінтеграції, конфіскаційної парадигми та цивільно–правової відповідальності за корупційні правопорушення.
Ключові слова: AML, ВАКС, конфіскація, відшкодування, євроінтеграція.

Tuliakov Viacheslav
Doctor of Legal Science, Professor,
Corresponding Member of the National Academy of Legal Sciences of Ukraine,
professor of the Criminal Law Department,
National University «Odesa Law Academy»,
Odesa, Ukraine

EU ANTI–MONEY LAUNDERING LEGISLATION: NEW CHALLENGES FOR UKRAINE

The paper analyses the new EU AML standards and challenges for Ukraine in the context of European integration, the confiscation paradigm, and civil liability for corruption offenses.
Keywords: AML, HACC, confiscation, compensation, European integration

Реформування правової архітектури протидії відмиванню доходів (AML/CFT) стало одним із ключових системних завдань на шляху України до повноправного членства в Європейському Союзі. Ухвалення нового пакету EU AML/CFT (AML6, AMLR, AMLD6) зумовило принципово новий рівень вимог до держав кандидатів на вступ: єдині правила ідентифікації бенефіціарних власників, обов'язкова реєстрація рахунків і трастів, посилені санкції за порушення режиму compliance, запровадження централізованого наглядового органу AMLA. Умовою доступу до єдиного європейського платіжного простору прямо названо приведення національного законодавства у відповідність до acquis у сфері AML/CFT [1; 4].

Водночас наукова дискусія щодо ефективності санкцій за корупційні правопорушення, зокрема у частині вибору між конфіскацією та компенсацією, набула нового виміру в контексті практики Європейського суду з прав людини (ЄСПЛ) та українського досвіду Вищого антикорупційного суду (ВАКС) [2; 3]. Метою цих тез є аналіз нових AML–стандартів ЄС крізь призму виявлених структурних асиметрій українського AML–середовища, а також оцінка правової парадигми відповідальності за корупційні правопорушення, що формується під впливом євроінтеграційних зобов'язань.

Новий регуляторний AML–пакет ЄС формує принципово іншу архітектуру фінансового моніторингу: замість директивної моделі (AMLD) впроваджується пряма дія регламенту (AMLR), що виключає можливість фрагментарної імплементації. Ключові новели охоплюють: уніфіковані процедури належної перевірки клієнтів (CDD/EDD); обов'язкову реєстрацію трастів та інших договірних утворень; посилену прозорість бенефіціарної власності через з'єднані UBO–реєстри; жорсткі вимоги до відповідальності фінансових установ і нефінансових суб'єктів обов'язкового моніторингу; новий наглядовий орган – Агентство з протидії відмиванню коштів (AMLA) зі штаб–квартирою у Франкфурті [1; 4].

Для України, яка перебуває на шляху до членства в ЄС, ці вимоги мають характер юридичних передумов, а не лише рекомендацій. Аналіз поточного стану свідчить про наявність системних прогалин: відсутність загального декларування доходів і майна, широта винятків статті 165 ПКУ (чайові, виграші, соціальні трансферти, «ФОП–оболонки»), застережна позиція щодо Варшавської конвенції, епізодичні амністії капіталу без реконструкції походження активів [1]. Усе це формує середовище «архіпелагу асиметрій», де різні категорії доходів по–різному включаються або виключаються з податкового, AML– та конфіскаційного контурів.

Особливе значення має практика ЄСПЛ щодо репаративної конфіскації. У справі «Флоріо та Бассіньяна проти Італії» ЄСПЛ сформулював концепцію «репаративної конфіскації» (reparative confiscation) як інструменту, що поєднує елементи відновлення справедливості та превенції без надмірного втручання у право власності [3]. Цей підхід може слугувати орієнтиром для України в контексті реформування ВАКС та вдосконалення інституту спеціальної конфіскації.

Харитонов Є. О., Харитонова О. І. та Білошкурський М. М. переконливо доводять, що традиційна конфіскація майна (ст. 59 КК України) та спеціальна конфіскація (ст. 96–2 КК України) мають суттєві правові вади: вони можуть суперечити Конституції України та порушувати право на мирне володіння майном, гарантоване ст. 1 Протоколу № 1 ЄКПЛ [2]. Статистика ВАКС підтверджує зростаючу тенденцію застосування конфіскації: від 9 осіб у 2021 р. до 46 у 2024 р., що свідчить про інтенсифікацію використання юридично складного інструменту. Натомість практика ВАКС 2023–2025 рр. засвідчила появу

de facto компенсаційного механізму через угоди про визнання вини: суди зобов'язують засуджених перераховувати кошти на рахунки Збройних сил України («Армія дронів», фонд United24). Загальна сума таких виплат у 2023 р. склала 77 498,0 тис. грн, у 2024 р. 16 121,1 тис. грн [2]. Однак ця практика залишається непослідовною та потребує законодавчого унормування.

Ключовим законодавчим кроком у цьому напрямі є законопроєкт № 11340 «Про внесення змін до КК та КПК України щодо підвищення ефективності угод про визнання вини». Попри прийняття його в першому читанні, він піддається справедливій критиці: відсутність вимоги повної співпраці зі слідством (включно зі свідченнями проти спільників), обмеження конфіскації лише доведеними активами, невідповідність розмірів штрафів тяжкості злочинів [2]. Автори обґрунтовують необхідність перегляду законопроєкту з урахуванням принципу людиноцентризму та відновлювальної функції санкцій.

Операційний висновок щодо векторів AML–реформи в Україні передбачає побудову координованої архітектури, де дані UBO–реєстрів, реєстрів рахунків і трастів з'єднуються з банківськими транзакційними даними в консолідованому профілі бенефіціарного власника [1]. Аналіз підозрілих операцій на рівні окремого банку (POP–аналіз) має стати частиною єдиного ризик–орієнтованого підходу, доступного Держфінмоніторингу в інтегрованому форматі.

Новий AML–пакет ЄС вимагає від України вирішення щонайменше чотирьох структурних проблем. По–перше, подолання «перекосу у бік слабких»: за відсутності належних гарантій суворі AML–інструменти передусім вражатимуть малий і середній бізнес, НПО та фізичних осіб, тоді як великі транснаціональні схеми адаптуватимуться до нових вимог. По–друге, усунення юрисдикційної асиметрії між податковим, AML–, санкційним і кримінальним режимами, яка дозволяє одному суб'єкту залишатися формально «чистим» у фіскальному сенсі, але токсичним у банківському та санкційному. По–третє, запровадження дієвої кримінальної відповідальності за незаконне збагачення відповідно до стандартів Варшавської конвенції. По–четверте, вирішення конфлікту між режимом GDPR та вимогами прозорості реєстрів бенефіціарних власників.

Концепція «репаративної конфіскації», що випливає з практики ЄСПЛ у справі «Флоріо та Бассіньяна проти Італії», пропонує синтетичну модель, яка поєднує превентивну, відновлювальну та пунітивну функції без порушення права власності [3]. На відміну від класичної конфіскації як кримінального покарання, репаративна конфіскація орієнтована на відновлення суспільного блага, яке постраждало внаслідок злочину, та на усунення неправомірної майнової вигоди.

Для України впровадження репаративної конфіскації як альтернативи або доповнення до наявної моделі спеціальної конфіскації означає: (1) законодавче визначення кола осіб, яким відшкодовується шкода (держава, потерпілі, суспільство); (2) встановлення чітких критеріїв пропорційності між розміром вилучення та доведеною шкодою; (3) інтеграцію з механізмом угод про визнання

вини таким чином, щоб компенсація стала обов'язковою умовою, а не опцією; (4) відповідність стандартам ЄКПЛ щодо «справедливого балансу» між публічним інтересом і захистом прав особи [2; 3].

Таким чином, нові AML–стандарти ЄС ставлять перед Україною не лише технічні, а й концептуальні виклики. Країна стоїть на порозі переходу до якісно іншої правової парадигми, де: по–перше, активи без документованої історії походження стають об'єктом підвищеної підозри; по–друге, право власності набуває умовного характеру щодо фінансової прозорості; по–третє, антикорупційні санкції мають виконувати відновлювальну, а не лише пунітивну функцію [1; 2; 3].

Вирішення цих завдань потребує: завершення криміналізації самовідмивання коштів; реформування інституту спеціальної конфіскації у напрямі репаративної моделі; доопрацювання законопроєкту № 11340 із запровадженням обов'язкових умов повної співпраці зі слідством та повного повернення незаконно набутих активів; побудови інтегрованої AML–архітектури, сумісної з вимогами AMLR та директив ЄС. Лише у такий спосіб Україна зможе не лише формально відповідати acquis ЄС, але й сформувати дієву систему фінансової безпеки, стійку до зловживань та спроможну захистити права всіх учасників фінансової екосистеми.

Перелік використаних джерел:

1. Туляков В. О. Пунітивна компенсація: український захист нацбезпеки в контексті розвитку. Правове забезпечення основ національної безпеки України в умовах війни: проблеми теорії та правозастосування : матеріали кругл. ст. (м. Харків, 17 жовт. 2025 р.) / НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2025. С. 39–43. URL: https://hdl.handle.net/11300/31467

2. Kharytonov E. O., Kharytonova O. I., Biloshkurskyi M. M. Civil Liability for Corruption Offenses: Confiscation or Compensation? Revista Jurídica Portucalense. 2026. № 39. DOI: https://doi.org/10.34625/issn.2183–2705(39.2)2026.ic–3

3. Tuliakov V. O. Reparative Confiscation in the ECtHR Case Law: Pragmatic Lessons from Florio and Bassignana v. Italy for the Ukrainian Legal System. –SSRN Preprint. February 05, 2026. 8 p. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6181360

4. AMLR vs AMLD6: Navigating the New Anti–Money Laundering Regulation Era Signicat Blog. 2026. URL: https://www.signicat.com/blog/amlr–vs–amld6–navigating–the–new–anti–money–laundering–regulation–erasignicat

DOI https://doi.org/10.32837/11300.33517

Усенко Олена
кандидат юридичних наук, доцент,
судовий експерт, завідувач Чернігівського відділення Київського науково–дослідного інституту судових експертиз Міністерства юстиції України,
м.Чернігів, Україна
ORCID https://orcid.org/0000–0003–0534–5422
e–mail:chernihiv@kndise.gov.ua

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ ЗАРУБІЖНИХ КРАЇН

У тезах здійснено комплексний аналіз сучасних підходів до використання технологій штучного інтелекту у судово–експертній діяльності зарубіжних країн. Досліджено особливості застосування алгоритмів машинного навчання, систем комп'ютерного зору та автоматизованого аналізу даних під час проведення криміналістичних, цифрових, судово–медичних, економічних і почеркознавчих експертиз.

Ключові слова: штучний інтелект, судова експертиза, судово–експертна діяльність, криміналістика, цифрова криміналістика, машинне навчання, цифрові докази, автоматизація експертних досліджень.

Usenko Olena
Ph.D. in Law, Associate Professor,
Forensic Expert, Head of the Chernihiv Branch of the Kyiv Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine,
Chernihiv, Ukraine

APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN FORENSIC EXPERT ACTIVITY OF FOREIGN COUNTRIES

The abstract provides a comprehensive analysis of modern approaches to the use of artificial intelligence technologies in forensic expert activity in foreign countries. The study examines the application of machine learning algorithms, computer vision systems and automated data analysis in criminalistic, digital, forensic medical, economic and handwriting examinations

Keywords: artificial intelligence, forensic examination, forensic expert activity, criminalistics, digital forensics, machine learning, digital evidence, automation of forensic research.

Стрімкий розвиток інформаційних технологій упродовж останніх десятиліть суттєво вплинув на трансформацію підходів до здійснення судово–експертної діяльності. Зростання обсягів цифрової інформації, ускладнення

способів учинення правопорушень та необхідність оперативного дослідження значних масивів даних обумовили активне впровадження технологій штучного інтелекту у практику експертних установ багатьох держав світу [1, с. 349]. У сучасних умовах використання систем штучного інтелекту розглядається як один із перспективних напрямів удосконалення механізму дослідження доказової інформації та підвищення ефективності експертної діяльності [2].

У міжнародній практиці штучний інтелект переважно застосовується як допоміжний інструмент автоматизації окремих процедур аналізу, систематизації та інтерпретації інформації. Водночас, у більшості держав домінує підхід, відповідно до якого остаточне формування експертного висновку залишається виключною компетенцією судового експерта [3, с. 410]. Такий підхід зумовлений необхідністю забезпечення належного рівня достовірності результатів дослідження, а також дотримання принципів законності та процесуальної допустимості доказів.

Одним із найбільш поширених напрямів використання штучного інтелекту є цифрова криміналістика. У Сполучених Штатах Америки алгоритми машинного навчання активно застосовуються у діяльності Federal Bureau of Investigation та інших криміналістичних лабораторій. Системи автоматизованого аналізу дозволяють здійснювати обробку значних масивів цифрової інформації, відновлення видалених файлів, встановлення взаємозв’язків між користувачами електронних пристроїв, а також виявлення прихованих цифрових слідів [4, с.1001]. Крім того, технології штучного інтелекту використовуються під час проведення біометричних досліджень, зокрема для розпізнавання облич, порівняння відбитків пальців та аналізу голосових характеристик.

У Великобританії значного розвитку набули системи автоматизованого аналізу відеоматеріалів та технології комп’ютерного зору. У діяльності Forensic Science Regulator та криміналістичних підрозділів поліції використовуються програмні комплекси, здатні здійснювати ідентифікацію осіб, транспортних засобів та окремих поведінкових характеристик на основі матеріалів відеоспостереження. Використання подібних технологій суттєво підвищує ефективність аналізу цифрових доказів та сприяє скороченню строків проведення криміналістичних досліджень. Окремого поширення набули алгоритми нейромережевого аналізу у сфері почеркознавчих експертиз, де системи штучного інтелекту використовуються для встановлення індивідуальних особливостей письма та порівняльного дослідження графічних ознак [5, с. 763].

У державах Європейського Союзу розвиток технологій штучного інтелекту у сфері криміналістики здійснюється в межах концепції «AI–assisted forensics», яка передбачає інтеграцію автоматизованих систем у процес дослідження доказової інформації. Важливу роль у координації міжнародного співробітництва у цій сфері відіграють Europol та European Network of Forensic Science Institutes. Основними напрямами використання штучного інтелекту є автоматизований аналіз цифрових доказів, виявлення ознак фальсифікації документів,

прогнозування кримінальних ризиків та дослідження фінансових операцій із метою встановлення ознак економічних правопорушень.

У Німеччині та Нідерландах широкого застосування набули технології тривимірного моделювання місця події. Використання лазерного сканування, фотограмметрії та автоматизованого цифрового аналізу дозволяє створювати високоточні 3D–моделі дорожньо–транспортних пригод, пожеж, вибухів та інших подій. Такі системи забезпечують можливість детального просторового аналізу механізму події та сприяють підвищенню об'єктивності експертних досліджень.

У Франції та Італії технології штучного інтелекту активно використовуються під час технічного дослідження документів. Автоматизовані системи дозволяють аналізувати структуру електронних файлів, встановлювати факти редагування документів, виявляти ознаки цифрового монтажу та досліджувати метадані електронної інформації. Застосування таких технологій суттєво розширює можливості сучасної технічної експертизи документів та сприяє підвищенню ефективності виявлення ознак фальсифікації.

Особливий інтерес становить практика Китайської Народної Республіки, де технології штучного інтелекту інтегровані у систему правосуддя та криміналістичної діяльності на державному рівні. У діяльності китайських експертних установ широко використовуються системи розпізнавання облич, аналізу голосу та автоматизованого дослідження поведінкових характеристик особи. Крім того, алгоритми штучного інтелекту застосовуються для аналізу значних масивів відеоданих та цифрової інформації, що дозволяє суттєво прискорити процес дослідження доказів.

У Канаді та Австралії активного розвитку набуло використання технологій штучного інтелекту у сфері судово–медичних експертиз. Алгоритми машинного навчання застосовуються під час аналізу рентгенологічних досліджень, встановлення характеру тілесних ушкоджень, оцінки токсикологічних показників та визначення орієнтовного часу настання смерті. Застосування автоматизованих систем у цій сфері сприяє підвищенню точності діагностичних досліджень та оптимізації діяльності судово–медичних експертів.

Важливим напрямом використання технологій штучного інтелекту є також проведення економічних та фінансових експертиз. Алгоритми автоматизованого аналізу застосовуються для дослідження бухгалтерської документації, моніторингу фінансових операцій, виявлення підозрілих транзакцій та встановлення ознак шахрайських схем. Подібні технології активно впроваджуються міжнародними аудиторськими компаніями, у межах проведення forensic investigations та корпоративних розслідувань.

Поряд із позитивними аспектами використання технологій штучного інтелекту виникають і суттєві правові та етичні проблеми. Насамперед це стосується недостатньої прозорості окремих алгоритмів, складності перевірки достовірності результатів автоматизованого аналізу, ризику виникнення алгоритмічної упередженості та можливості помилкової інтерпретації отриманих

даних. Окрему проблему становить питання процесуальної допустимості результатів, отриманих за допомогою систем штучного інтелекту, а також визначення меж відповідальності експерта у разі використання автоматизованих технологій.

На міжнародному рівні питання використання штучного інтелекту у сфері правосуддя регулюються рекомендаціями Council of Europe, UNESCO та нормативними актами Європейського Союзу, зокрема EU Artificial Intelligence Act. Вказані документи визначають необхідність забезпечення прозорості алгоритмів, захисту прав людини та дотримання принципу контролю людини за функціонуванням систем штучного інтелекту у сфері правосуддя.

Отже, міжнародний досвід свідчить про поступове формування нових підходів до організації судово–експертної діяльності із використанням технологій штучного інтелекту. Впровадження автоматизованих систем сприяє оптимізації процесу дослідження доказової інформації, підвищенню оперативності проведення експертиз та розширенню аналітичних можливостей експертних установ. Водночас подальший розвиток таких технологій потребує комплексного нормативно–правового регулювання, вироблення єдиних стандартів використання штучного інтелекту та забезпечення належного процесуального контролю за результатами автоматизованого аналізу.

Перелік використаних джерел:

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Hoboken : Pearson, 2021. 1136 p.
2. McCarthy J. What Is Artificial Intelligence? Stanford University, 2007. URL: www–formal.stanford.edu
3. Casey E. Digital Evidence and Computer Crime. 4th ed. London : Academic Press, 2020. 804 p.
4. Quick D., Choo K.–K. Digital Forensics in the Age of Artificial Intelligence // Digital Investigation. 2022. Vol. 41. 1337 p.
5. Found B. Deciphering the Human Condition: Handwriting Examination and Artificial Intelligence // Forensic Science International. 2021. Vol. 320. 1701 p.

DOI https://doi.org/10.32837/11300.33518

Чорноус Юлія
доктор юридичних наук, професор, професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ,
м. Київ, Україна
ORCID: https://orcid.org/0000–0001–9710–4858;
e–mail:chornous@ukr.net

АКТУАЛЬНІ ПИТАННЯ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Наголошено, що ефективність досягнення завдань кримінального провадження щодо воєнних злочинів, вчинених російською федерацією проти України – безпосередньо залежить від криміналістичного забезпечення процесу розслідування та судового розгляду.

Ключові слова: криміналістичне забезпечення; розслідування; воєнні злочини.

Chornous Yuliia
Doctor of Law, Professor, Professor of the Department of Criminalistics and Forensic Medicine of the National Academy of Internal Affairs,
Kyiv, Ukraine

CURRENT ISSUES OF FORENSIC SUPPORT FOR THE INVESTIGATION OF WAR CRIMES

It is emphasized that the effectiveness of achieving the objectives of criminal proceedings regarding war crimes committed by the Russian Federation against Ukraine directly depends on the forensic support of the investigation and trial process.

Keywords: forensic support; investigation; war crimes.

Розслідування воєнних злочинів як результату збройної агресії російської федерації проти України є пріоритетним напрямом правоохоронних органів нашої держави, з метою досягнення завдань кримінального провадження (ст. 2 КПК України) [1]. Воєнні злочини, передбачені ст. 438 Кримінального кодексу України, за своєю природою є міжнародними, що зобов'язує до залучення міжнародних механізмів відповідальності на порушення норм міжнародного гуманітарного права. Правова природа воєнних злочинів в Україні виходить за межі внутрішньодержавного регулювання. Вона має транснаціональний характер, що проявляється у взаємодії національних та міжнародних правових механізмів, а також у можливості притягнення винних осіб до відповідальності як у межах національної юрисдикції, так і в міжнародних судових інституціях.

Як відзначають Г. К. Тетерятник, Ю. М. Одажиу, воєнні злочини відносяться до категорії кримінальних правопорушень, які мають значну специфіку та складність розслідування. Це потребує системного наукового аналізу матеріально–правових, процесуальних, криміналістичних, організаційних, методичних аспектів здійснення кримінального провадження цієї категорії проваджень. Перспективними напрямками дослідження вбачаються розслідування, сучасні досягнення криміналістики, взаємодія органів та підрозділів під час розслідування окремих категорій воєнних злочинів та ін. [2, с. 688].

Ефективність досягнення завдань кримінального провадження щодо воєнних злочинів, вчинених російською федерацією проти України, її населення – безпосередньо залужить від належного криміналістичного забезпечення процесу розслідування та судового розгляду кримінальних проваджень.

Поняття «криміналістичне забезпечення» з теоретичного аспекту може бути охарактеризоване як окреме вчення науки криміналістики, а із практичного аспекту слід вести мову про застосування криміналістичних засобів, методів і прийомів діяльності у кримінальному провадженні, що реалізуються стороною обвинувачення, стороною захисту та судом як органом правосуддя. Власне криміналістичне забезпечення представлене такою структурою. Теоретичною основою є загальна теорія криміналістики, й три структурні елементи як от: криміналістична техніка (техніко–криміналістичне забезпечення), криміналістична тактика (тактико–криміналістичне забезпечення), криміналістична методика (методико–криміналістичне забезпечення). Особливою є сфера реалізації криміналістичного забезпечення – відповідно до проблематики, яка є безпосереднім предметом наукового дослідження вчених і практиків [3, с. 81–82].

Діяльність із розслідування воєнних злочинів за сучасних умов, у контексті сучасних суспільно–правових реалій, потребує використання всього арсеналу засобів, методів, прийомів правоохоронної діяльності, які відповідають міжнародним та європейським стандартам, враховують кращий іноземний досвід. Підвищення ефективності діяльності із розслідування залежить від систематичного удосконалення її нормативно–правового регулювання, ефективної організації, належного криміналістичного забезпечення, відповідності сучасним потребам практики.

Із початком повномасштабного вторгнення російської федерації на територію нашої держави та введенням воєнного стану значних змін зазнало кримінальне процесуальне законодавство, як в частині регламентації розслідування воєнних злочинів так й інших кримінальних правопорушень, розслідування котрих здійснюється за особливого правового режиму.

Так, новелою стало введення нового розділу КПК України, який присвячений урегулюванню процесуальних та організаційних аспектів взаємодії з Міжнародним кримінальним судом, на основі Закону України «Про внесення змін

до Кримінального процесуального кодексу України та інших законодавчих актів України щодо співробітництва з Міжнародним кримінальним судом» № 2236–IX від 03 травня 2022 року [4].

Також, відповідно до Закону України № 2201–IX від 01.05.2022 року «Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану» [5] законодавцем регламентовано процесуальний порядок досудового розслідування в умовах воєнного стану. Зокрема, зміни внесені до КПК України у зв'язку із його прийняттям, стосуються особливого змісту та форми кримінального провадження в умовах воєнного стану. Вказані зміни нормативно–правового регулювання впливають й на особливості реалізації криміналістичного забезпечення кримінального провадження.

Враховуючи події в Україні, систематичні обстріли як наслідок збройної агресії російської федерації, порядок збереження та відновлення матеріалів досудового розслідування, речових доказів, висновків експерта та інших процесуальних документів під час розслідування кримінальних правопорушень – набуває неабиякої важливості. Необхідним є збереження якомога широкого кола криміналістично значимої, у тому числі доказової, інформації до розгляду відповідних справ у національних судових інстанціях і безпосередньо – Міжнародним кримінальним судом.

В умовах активного розвитку інформаційних технологій Україна поступово переходить до впровадження електронного судочинства, активно поширюється електронний документообіг. З цією метою, задля забезпечення збереження матеріалів досудового розслідування, зокрема висновку експерта, запобігання їх втрати чи знищення внаслідок ведення активних бойових дій на території нашої держави, окупації та деокупації територій, слід передбачити можливість його викладу та зберігання в електронній формі [6, с. 58].

Нові завдання у зв'язку протидією повномасштабній агресії російській федерації постали і щодо техніко–криміналістичного забезпечення правоохоронних органів України.

Техніко–криміналістичне забезпечення проведення процесуальних дій повинно відповідати передовому досвіду іноземних держав. Наприклад, технології 3D сканування проведення процесуальних дій ввійшли до повсякденної практики правоохоронних органів провідних світових та європейських держав, а нині – застосовуються правоохоронцями України. Також важливим напрямом є застосування мобільних ДНК–лабораторій, які активно застосовуються на практиці. Підвищенню ефективності розшуку безвісно зниклих осіб, жертв обстрілів та інших категорій постраждалих категорій осіб сприяє створення уніфікованої бази ДНК–даних, з доступом до неї співробітників Національної поліції України, експертів Експертної служби МВС України.

Сучасною є технологія відеоконференції під час проведення процесуальних дій. Вона має широку сферу використання, адже процесуальні дії у режимі

відеоконференції проводяться як під час досудового розслідування, так і судового розгляду; як під час здійснення кримінального провадження як у межах держави, так і в порядку міжнародного співробітництва. Власне криміналістичне забезпечення проведення процесуальних дій у режимі відеоконференції потребує формування єдиних, уніфікованих на міжнародному рівні підходів, що стосуються правової основи, технології, організації й тактики проведення.

Сучасні бази даних державних та правоохоронних органів, міжнародних організацій, надають можливість інформаційно–довідкового супроводження розслідування та судового розгляду, забезпечують розшук безвісно зниклих осіб та підозрюваних у вчиненні злочинів [7, с. 221–223].

Отже, нині нові завдання постали перед криміналістикою, яка використовуючи останні досягнення природничих, технічних та суспільних наук, трансформує їх у практику, а нині здійснює комплексне і системне криміналістичне забезпечення розслідування та судового розгляду справ про воєнні злочини, вчинені в Україні.

Перелік використаних джерел:

1. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651–VI. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text.
2. Тетерятник Г. К., Одажиу Ю. М. Розслідування воєнних злочинів: окремі теоретико–прикладні питання. Юридичний науковий електронний журнал № 6/2023. С. 686–688. DOI https://doi.org/10.32782/2524–0374/2023–6/161
3. Чорноус Ю., Чечотка І. Сучасний стан і напрями розвитку криміналістичного забезпечення кримінального провадження. Наука і правоохорона. 2026. Вип. 1 (71). С.80–88. DOI: 10.33270/05267101.8
4. Про внесення змін до Кримінального процесуального кодексу України та інших законодавчих актів України щодо співробітництва з Міжнародним кримінальним судом. Закон України № 2236–IX від 03 травня 2022 року https://zakon.rada.gov.ua/laws/show/2236–20#Text
5. Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану. Закон України № 2201–IX від 01.05.2022 року. URL: https://zakon.rada.gov.ua/laws/show/2201–20#Text
6. Chornous, Yu., & Leliuk, T. (2023). Organization of forensic examinations in criminal proceedings as a condition for the effectiveness of the investigation of criminal offences. Law Journal of the National Academy of Internal Affairs, 13(2), 50–62. https://doi.org/10.56215/naia–chasopis/2.2023.50
7. Чорноус Ю.М. Криміналістичне забезпечення діяльності Міжнародного кримінального суду. Актуальні аспекти криміналістичного та психологічного забезпечення правоохоронної діяльності. Матеріали Всеукраїнської науково–практичної конференції (м. Одеса, 06 жовтня 2023 р.). – Одеса : ОДУВС, 2023. С. 219–225.

DOI https://doi.org/10.32837/11300.33519

Шевчук Віктор
доктор юридичних наук, професор,
завідувач кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого,
провідний науковий співробітник НДІ вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України,
заслужений юрист України,
м. Харків, Україна
ORCID: http://orcid.org / 0000–0001–8058–3071
e–mail: Shevchuk_viktor@ukr.net

КРИМІНАЛІСТИКА МАЙБУТНЬОГО В ЕПОХУ ЦИФРОВІЗАЦІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ: ГЛОБАЛЬНІ ВИКЛИКИ Й ПЕРСПЕКТИВИ РОЗВИТКУ

Анотація: Розглянуто та досліджено актуальні проблеми розвитку криміналістики майбутнього в епоху цифровізації та ШІ в контексті глобальних викликів, безпекових ризиків і воєнних загроз. Висвітлено можливості комплексного використання інноваційних криміналістичних засобів, цифрових технологій та інструментів штучного інтелекту у діяльності з виявлення, розслідування та запобігання кримінальним правопорушенням. Зазначено, що розроблення та впровадження інноваційних криміналістичних технологій мають здійснюватися з урахуванням сучасних тенденцій розвитку криміналістичної науки, потреб цифрової трансформації суспільства та особливостей функціонування правоохоронної системи в умовах воєнного стану та повоєнного відновлення. Визначено основні напрями застосування технологій ШІ у криміналістичній діяльності та протидії сучасним формам злочинності. Обґрунтовано, що подальший розвиток криміналістики відбуватиметься під впливом цифрової трансформації суспільства, автоматизації процесів обробки інформації та стрімкого поширення систем ШІ. Наголошено, що ефективне реагування на новітні загрози потребує модернізації криміналістичних методів і засобів, удосконалення нормативно–правового регулювання використання цифрових технологій та формування нової наукової парадигми криміналістики, здатної забезпечити ефективне розслідування злочинів у цифровому середовищі та належний захист прав людини та громадянина в сучасних умовах технологічних змін та воєнних загроз.

Ключові слова: цифрові технології; протидія злочинності, штучний інтелект; судова експертиза; воєнний стан; кіберзлочини; цифрові сліди; криміналістичні інновації.

Viktor Shevchuk
Doctor of Law, Professor,
Head of the Department of Criminalistics,
Yaroslav Mudryi National Law University,
Leading Researcher at the Academician V. V. Stashis Research Institute for the Study of Crime Problems of the National Academy of Legal Sciences of Ukraine,
Honored Lawyer of Ukraine,
Kharkiv, Ukraine

FUTURE CRIMINALISTICS IN THE ERA OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE: GLOBAL CHALLENGES AND DEVELOPMENT PROSPECTS

The paper examines and explores current issues in the development of future criminalistics in the era of digitalization and artificial intelligence within the context of global challenges, security risks, and wartime threats. The possibilities of the integrated use of innovative criminalistic tools, digital technologies, and artificial intelligence applications in the detection, investigation, and prevention of criminal offenses are highlighted. It is emphasized that the development and implementation of innovative criminalistic technologies should be carried out with due regard to contemporary trends in criminalistic science, the needs of society's digital transformation, and the specific features of law enforcement activities under martial law and post–war recovery conditions. The main directions for the application of artificial intelligence technologies in criminalistic activities and in combating contemporary forms of crime are identified. It is substantiated that the further development of criminalistics will be driven by the digital transformation of society, the automation of information–processing processes, and the rapid advancement of artificial intelligence systems. It is stressed that effective responses to emerging threats require the modernization of criminalistic methods and tools, the improvement of the legal framework governing the use of digital technologies, and the formation of a new scientific paradigm of criminalistics capable of ensuring effective crime investigation in the digital environment and the proper protection of human and civil rights under conditions of technological change and wartime challenges.

Key words: digital technologies; digital technologies; combating crime; artificial intelligence; forensic examinations; martial law; cybercrime; digital evidence; criminalistic innovations.

Стрімкий розвиток цифрових технологій, глобальна цифровізація суспільства та впровадження систем штучного інтелекту зумовлюють докорінні зміни у сфері протидії злочинності та криміналістичного забезпечення правоохоронної діяльності. Цифровізація суспільних відносин спричинила появу нових джерел криміналістично значущої інформації. Поряд із традиційними речовими доказами дедалі більшого значення набувають цифрові сліди, що

містяться у мобільних пристроях, комп'ютерних системах, хмарних сервісах, соцмережах, блокчейн–мережах, а також у пристроях Інтернету речей. У зв'язку з цим сучасна криміналістика поступово трансформується з науки, орієнтованої переважно на дослідження матеріальних слідів злочину, у міждисциплінарну галузь знань, що активно використовує цифрові технології, інструменти аналізу даних та інтелектуальні інформаційні системи [1, с.1–19].

Особливе значення для майбутнього криміналістики має впровадження технологій штучного інтелекту. Системи штучного інтелекту здатні здійснювати автоматизований аналіз великих масивів даних, виявляти приховані закономірності, прогнозувати можливі зв'язки між подіями та особами, здійснювати розпізнавання облич, голосу, текстів, відеозображень і цифрових об'єктів. Використання таких технологій сприяє підвищенню ефективності розслідування кримінальних правопорушень, скороченню часу на опрацювання доказової інформації та вдосконаленню криміналістичної аналітики. У цьому контексті цифрова криміналістика поступово стає одним із провідних напрямів розвитку криміналістичної науки та практики [1, с. 32].

В реаліях російської військової агресії інструменти ШІ істотно сприяють виявленню, розкриттю та розслідуванню воєнних злочинів, злочинів проти людяності та геноциду. Практика показує, що за допомогою технологій штучного інтелекту можна ідентифікувати російських військових за соціальними мережами й записами камер відеоспостереження. Достатньо активно застосовуються технології розпізнавання обличчя Clearview AI для боротьби з дезінформацією, розпізнавання й ідентифікації загиблих і воєнних злочинців [3] . Використання технологій ШІ допомогає руйнувати міфи про нібито невмирущих солдатів так званої «спецоперації», розпізнаючи обличчя трупів російських військових окупантів, відшукуючи їх у соціальних мережах і за допомогою автодозвонів повідомляючи родичів про їхню смерть [4].

Сьогодні в реаліях воєнних та глобальних загроз усі практики у сфері міжнародного кримінального правосуддя повинні покращувати своє технічне розуміння новітніх технологій ШІ і повинні культивувати глибше сучасне розуміння застосування того, як соціальні мережі, геолокації, розмови мобільного зв'язку, коп'ютерна інформація та інші цифрові сліди й комунікації використовуються в зонах проведення воєнних дій [5, с. 335] . Зважаючи на воєнну агресію російськими військами на територію України та вчинення ними масових вбивств, гвалтувань, мародерства, сьогодні гостро постає проблема збирання доказів воєнних злочинів. Це потребує активізації та поширення застосування технологій штучного інтелекту при виявлені, документуванні та розслідуванні воєнних злочинів, злочинів проти людяності та геноциду.

Застосування штучного інтелекту в розслідуванні воєнних злочинів в Україні може бути корисним в багатьох аспектах. Основними напрямками, в яких він може бути використаний, є такі: 1) аналіз супутникових знімків. Штучний інтелект може допомогти аналізувати великі обсяги супутникових знімків для

виявлення змін у ландшафті, зокрема будівель, доріг, об'єктів інфраструктури, які можуть бути пов'язані з воєнними злочинами, а також допомогти в ідентифікації місць, де можуть бути поховані тіла жертв воєнних злочинів; 2) аналіз відео– та фотоматеріалів. Штучний інтелект може бути використано для аналізу великого обсягу відео– та фотоматеріалів, які були зняті на місцях вчинення воєнних злочинів, що, у свою чергу, може допомогти в ідентифікації підозрюваних та свідків, а також встановити, чи були зображені на них об'єкти, які можуть містити криміналістично–значущу інформацію для розслідування таких злочинів [6] ; 3) обробка аудіоматеріалів. За записами телефонних розмов та під час обробки аудіоматеріалів щодо розслідування воєнних злочинів штучний інтелект може допомогти в ідентифікації голосів, які містяться на таких носіях, а також визначити місця, де були здійснені ці розмови; 4) аналіз соціальних мереж [7, с. 56–61]. Аналізуючи соціальні мережі, штучний інтелект може допомогти виявити зв'язки між підозрюваними, які можуть бути пов'язані з воєнними злочинами, та ідентифікувати осіб, які можуть бути свідками воєнних злочинів або мати інформацію про них [8]; 5) аналіз даних з медичних закладів. Штучний інтелект може допомогти в ідентифікації тіл жертв воєнних злочинів, встановленні причини смерті, ідентифікації військовополонених, військових злочинців та їх пошук за даними про хворобу та відомостями про їх ідентифікаційні ознаки, які допомагають встановленню конкретної особи [9]; 6) розпізнавання облич. Штучний інтелект може бути використаний для розпізнавання облич на фото та відео з місць вчинення воєнних злочинів. Це може допомогти в ідентифікації підозрюваних, причетних до вчиненя таких злочинів, та встановленню свідків, які можуть повідомити важливу інформацію про розслідувану подію воєнного злочину; 7) аналіз текстової інформації. Аналіз штучним інтелектом текстової інформації (наприклад, повідомлень у соціальних мережах та інших джерелах), пов'язаної з воєнними злочинами, сприятиме ідентифікації підозрюваних і свідків та з'ясуванню криміналістично значущої інформації про воєнні злочини, які розслідуються [10, с. 37]. Отже, застосування штучного інтелекту може бути корисним для ефективного розслідування воєнних злочинів, злочинів проти людяності та геноциду й допомогти встановити винних і притягти їх до відповідальності за вчиненні злочини.

Водночас розвиток цифрових технологій породжує низку нових викликів. Одним із найбільш небезпечних явищ стає використання генеративного штучного інтелекту для створення підробленого цифрового контенту (deepfake), який може імітувати зовнішність, голос або поведінку конкретної особи. Такі технології створюють серйозні ризики для процесу доказування, оскільки ставлять під сумнів достовірність цифрових доказів та ускладнюють встановлення об'єктивної істини у кримінальному провадженні.

Суттєвим викликом для криміналістики залишається і зростання масштабів кіберзлочинності. Використання штучного інтелекту злочинними угрупованнями для автоматизації кібератак, соціальної інженерії, поширення дезінформації та

приховування злочинної діяльності вимагає розроблення нових криміналістичних методик і засобів протидії. Особливої актуальності набуває криміналістичне забезпечення розслідування злочинів, вчинених у кіберпросторі, а також використання OSINT–технологій, інструментів цифрової аналітики та систем автоматизованого моніторингу інформаційного середовища.

Важливо зауважити, що нові та досить складні виклики формуютьсятакож в умовах збройних конфліктів, війн та гібридних загроз. Документування воєнних злочинів, злочинів проти людяності та порушень міжнародного гуманітарного права дедалі більше спирається на цифрові докази, супутникові знімки, матеріали соціальних мереж, геопросторові дані та результати відкритої розвідки (OSINT).

Перспективи розвитку криміналістики пов’язані з подальшою інтеграцією штучного інтелекту, технологій великих даних (Big Data), машинного навчання, цифрової криміналістики, квантових обчислень та інтелектуальних систем підтримки прийняття рішень. У майбутньому можливе створення комплексних криміналістичних платформ, здатних автоматично аналізувати цифрові докази, формувати версії розслідування та прогнозувати напрями пошуку доказової інформації.

Отже, криміналістика майбутнього розвиватиметься під впливом цифрової трансформації суспільства та стрімкого поширення технологій штучного інтелекту. Ефективне реагування на нові загрози потребує модернізації криміналістичних методів, удосконалення нормативно–правового регулювання використання цифрових технологій та формування нової наукової парадигми, здатної забезпечити ефективне розслідування злочинів у цифровому середовищі та захист прав людини в умовах технологічних змін.

Перелік використаних джерел:

1. Shevchuk V., Morozova T., Chornyi H., Nehrebetskyi V., and Slobodeniuk I. Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues. International Annals of Criminology, 2025. Pp. 1–19. DOI: https://doi.org/10.1017/cri.2025.10090

2. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. Kriminalistikairteismo ekspertologija : mokslas, studijos, praktika. 2022, 18, 32.

3. Федоров М. Технології з розпізнавання облич та штучний інтелект дозволяють знайти кожного / SUNDRIES. 09.04.2022. URL: https://sundries.com.ua/tekhnolohii–z–rozpiznavannia–oblych–ta–shtuchnyi–intelekt–dozvoliaiut–znaity.

4. Konovalova V.O., Shevchuk V.M. Application of digital technologies in criminalistics in the conditions of war. Цифрова трансформація кримінального провадження в умовах воєнного стану: матеріали круглого столу, присвяч. Всеукр. тижню права (м. Харків, 23 груд. 2022 р.) : НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2022. С.141–146.

5. Freeman, L. Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials. Fordham International Law Journal, 2018, 41 (2), 284−336. C. 335. Available at: https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1 .

6. Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, – LIGA.net URL: https://tech.liga.net/ua/ukraine/novosti/iskusstvennyy–intellekt–mintsifry–razoblachil–okkupanta–popavshego–v–gospital–v–krivom–roge

7. Дуфенюк О.М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції: матеріали науково–практ. семінару (22 травня 2020). Львів: ЛьвДУВС, 2020. С. 56–61.

8. Шевчук В. М. Використання інформації із соціальних інтернет–мереж при розслідувані кіберзлочинів: криміналістичні проблеми. Кримінальні загрози в секторі безпеки: практики ефективного реагування: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Я. Мудрого. Х.: Право, 2019. С.142 –146.

9. Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL:. https://hromadske.ua/posts/pid–izyumom–znajshli–bratsku–mogilu–ukrayinskih–vijskovih–ta–ponad–460–novih–mogil–foto.

10. Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. Теорія та практика судової експертизи і криміналістики. Вип. 4 (29). 2022. С.12–46. С. 37. URL: https://khrife–journal.org/index.php/journal/issue/view/18/4–22

DOI https://doi.org/10.32837/11300.33520

Шепітько Валерій
доктор юридичних наук, професор,
академік Національної академії правових наук України,
заслужений діяч науки і техніки України, Заслужений професор
Національного юридичного університету імені Ярослава Мудрого,
Почесний професор Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»,
професор кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого,
м. Харків, Україна
ORCID: https://orcid.org/0009-0007-0252-7569
e–mail: shepitko.valery@gmail.com

Шепітько Михайло
доктор юридичних наук, професор,
член–кореспондент Національної академії правових наук України,
професор кафедри кримінального права Національного юридичного університету імені Ярослава Мудрого,
м. Харків, Україна
ORCID: https://orcid.org/0000-0002-7164-8037,
e–mail: shepitko.michael@gmail.com

ПРОБЛЕМИ ФОРМУВАННЯ ТА МІСЦЕ КРИМІНАЛІСТИЧНОЇ ІНЖЕНЕРІЇ В СТРУКТУРІ КРИМІНАЛІСТИКИ

Тези присвячені проблемам формування та визначення місця криміналістичної інженерії в структурі криміналістики. Аргументовано, що криміналістична інженерія може бути розглянута як галузь криміналістичної техніки, вид судових експертиз або галузь судових наук. Криміналістична інженерія – це практичне розроблення певних моделей, приладів, пристроїв, пристосувань, обладнання та матеріалів, що використовуються в розслідуванні кримінальних правопорушень. Звернено увагу, що свого часу в Україні були розроблені науково–технічні засоби та інші наукові продукти для слідчої практики. На підставі положень криміналістичної інженерії сформувався й окремий клас інженерно–технічних експертиз.

Ключові слова: криміналістика, судові науки, судова експертиза, криміналістична інженерія, інженерно–технічна експертиза, криміналістична техніка, науково–технічні засоби, інноваційні технології.

Valery Shepitko
Doctor of Law, Professor,
Academician of the National Academy of Law Sciences of Ukraine,

Honoured Researcher for Science and Technology of Ukraine,
Honoured Professor of the Yaroslav Mudryi National Law University,
Emeritus Professor of the National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute»,
Professor of the Criminalistic Department of Yaroslav Mudryi National Law University,
Kharkov, Ukraine

Mykhaylo Shepitko
Doctor of Law, Professor,
Associate Member of the National Academy of Law Sciences of Ukraine,
Professor of the Criminal Law Department of Yaroslav Mudryi National Law University,
Kharkov, Ukraine

PROBLEMS OF FORMATION AND THE PLACE OF FORENSIC ENGINEERING IN THE STRUCTURE OF CRIMINALISTICS

The theses are devoted to the problems of formation and determination of the place of forensic engineering in the structure of criminalistics. It is argued that forensic engineering can be considered as a branch of criminalistic technique, a type of forensic examination or a branch of forensic science. Forensic engineering is the practical development of certain models, devices, equipment and materials used in the investigation of criminal offenses. It is noted that at one time in Ukraine, scientific and technical means and other scientific products for investigative practice were developed. Based on the provisions of forensic engineering, a separate class of engineering and technical examinations was formed.

Key words: criminalistics, forensic sciences, forensic examination, forensic engineering, engineering and technical examination, criminalistic technique, scientific and technical means, innovative technologies.

Криміналістика має інноваційний характер. Вона спрямована на створення наукового «продукту» для практики боротьби зі злочинністю. Це та наука, яка має реагувати на змінення злочинності, її витончений характер, появу нових видів і способів злочинів. Впровадження інновацій у слідчу діяльність може здійснюватися за такими напрямами: 1) розробка та використання нових науково–технічних засобів для виявлення, збирання і попереднього дослідження доказів; 2) пропонування новітніх інформаційних технологій та їх використання в роботі слідчого; 3) створення (розробка) і пропонування до застосування нових прийомів, методів, методик проведення слідчих (розшукових) дій і розслідування злочинів в цілому [1, с. 78–81].

На сьогодні проблеми судової (криміналістичної) інженерії потребують свого дослідження. Постановку проблеми існування та розвитку криміналістичної інженерії в сучасних умовах здійснив В. Туляков, який справедливо вказує, що криміналістика, у класичному розумінні, завжди була інженерною дисципліною, виступаючи як система інженерних рішень, яка дозволяє реконструювати механізм злочину, оптимізувати слідчі дії, моделювати структуру криміналістично значущих подій та створити технічні засоби протидії злочинності [2, с. 424]. Виникають питання про місце криміналістичної інженерії в структурі криміналістики або судових наук, про її сутність, предмет, завдання та межі дослідження.

Інженерія – це практика використання природничих наук. Розрізняють галузі сучасної інженерії: будівельну інженерію (Civil engineering), інженерію машинобудування (Mechanical enginiring), хімічну інженерію (Chemical engineering), інженерію нафтовидобування (Petroleum engineering), едектротехнічну інженерію (Electrical engineering), аерокосмічну інженерію (Aerospace engineering), комп'ютерну інженерію або IT інженерію (Computer engineering). Окрім того, в сучасних джерелах приділяється також увага соціальній інженерії (Social engineering), генетичній інженерії (genetic engineering), медичній чи біомедичній інженерії (Medical or Biomedical engineering) тощо.

Криміналістична інженерія може бути розглянута як галузь криміналістичної техніки, вид судових експертиз або галузь судових наук. Криміналістика (Criminalistics) та судові науки (Forensic Sciences) є відображенням різного розвитку науки, що формувалася в різних школах і відповідно – наукових напрямах із використанням тих правових, технічних, тактичних та методичних можливостей, які були в арсеналі її кращих представників [3, с.89–97]. Судові науки мають велику кількість галузей та напрямів (судова медицина, судова токсикологія, судова генетика, судовою археологія, судовою психологія, судова психіатрія, судова біологія, судова хімія та ін.)… [4, с. 188, 189]. Важливою галуззю судових наук є й судова (або криміналістична) інженерія. Криміналістична інженерія – це практичне розроблення певних моделей, приладів, пристроїв, пристосувань, обладнання та матеріалів, що використовуються в розслідуванні кримінальних правопорушень.

Криміналістична інженерія посідає суттєве місце в криміналістичній техніці, яка виникла у результаті впровадження досягнень природничо–технічних наук у практику боротьби зі злочинністю. Прикладом «продуктів» криміналістичної інженерії є розроблені та впроваджені в практику правозастосовної діяльності комплекти науково–технічних засобів. Одним із таких науково–технічних засобів боротьби зі злочинністю свого часу постало створення Гансом Гроссом слідчої валізи (портфеля). Він був створений з метою пошуку та фіксації слідів на місці події та за деякими даними був представлений на виставці криміналістичної техніки в Дрездені (1903) [5, с. 37]. Ганс Гросс є винахідником слідчої валізи або портфеля (Tatortkoffer).

В Україні (підприємством «Крімтех», Харків, 2007–2012) були розроблені комплекти науково–технічних засобів для слідчої практики вузької спрямованості: комплект пошукових засобів слідчого (набір–пошук); комплект науково–технічних засобів огляду місця дорожньо–транспортної події; комплект науково–технічних засобів для огляду місця пожежі (набір–пожежа); комплект науково–технічних засобів для огляду вибухових пристроїв і місця вибуху (набір–вибух); комплект науково–технічних засобів для роботи з мікрооб'єктами (набір «Мікро» або «Молекула» [6, с. 495]); комплект науково–технічних засобів для роботи зі слідами рук (дактилоскопічний набір); комплект слідчого для огляду документів; оперативний одорологічний комплект та ін. [7, с. 299, 300; 8, с. 53] Окрім того, до «продуктів» криміналістичної інженерії можуть бути віднесено розроблення «Пристрою для виміру швидкості балістичного об'єкта» [9], «Автоматизоване робоче місце слідчого «Інсайт» [10], «Спосіб формування суб'єктивного портрету «RAIPS–портрет» [11], «База даних «Практика слідчого» [12], «База даних «Слідчий прецедент» [13] та ін.

Розвиток криміналістичної інженерії відображається у застосуванні спеціальних знань та проведенні судових експертиз. На сьогодні існує клас інженерно–технічних експертиз в основу генези яких покладено застосування спеціальних знань у галузі техніки та інженерії, як гармонійне поєднання прикладної науки і технічних навичок з математикою та сучасними технологіями, що має на меті пошук актуальних рішень технічних проблем, які виникають у судочинстві [14, с. 241]. У спеціальних джерелах справедливо звернено увагу на те, що з'являються нові види інженерно–технічних та інженерно–технологічних експертиз. Зокрема, тільки за 2 роки (2020–2022) започатковано 24 нові судово–експертні спеціальності, ініційовані НДУСЕ Міністерства юстиції України («Дослідження технічного стану та умов експлуатації машин та механізмів», «Дослідження подій на водному транспорті», «Дослідження авіаційних подій та інцидентів» і «Теплотехнічні дослідження») і Центром судових і спеціальних експертиз Українського науково–дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України («Дослідження безпілотних літальних апаратів (БПЛА), які призначені для радіоконтролю і перехоплення систем мобільного зв'язку, фото–, відеоконтролю за об'єктами на місцевості», «Дослідження радіоелектронного обладнання прийому, обробки та передачі інформації», «Дослідження робототехнічних систем спеціального призначення» і «Інженерно–технологічна експертизи об'єктів критичної інфраструктури») [15, с. 116].

Перелік використаних джерел:

1. Коновалова В., Шепітько В. Криміналістика в системі наукового знання: сучасний стан та деякі тенденції. Криміналістика у протидії злочинності: тези доп. наук,–практ. конф. (Київ, 16 жовтня 2009 р.). Київ: Хай–Тек Прес, 2009. С. 78–81.

2. Туляков В. Криміналістична інженерія: методологія майбутнього. Нове століття криміналістики та судових наук: Liber Amicirum на честь академіка В. Ю. Шепітька: монографія / [за ред. М. В. Шепітька]. 2–ге вид., допов. Харків: Право, 2026. С. 423–434.

3. Шепітько М. В. Концептуальні засади розвитку криміналістики та судових наук. Архів кримінології та судових наук. 2020. № 1. С. 89–97.

4. Shepitko V., Shepitko M. Criminal Law, Criminalistics and Forensic Sciences: Encyclopedia. Kharkiv: Pravo, 2021. С. 188–189.

5. Тарнавська Л. М. Слідча валіза як науково–технічний засіб: візія Ганса Гросса та сучасність. ІІ Наукові читання пам’яті Ганса Гросса: зб. тез міжнар. наук.–практ. конф. (м. Чернівці, 09 грудня 2022 р.). Чернівці: Чернівец. нац. ун–т ім. Ю. Федковича, 2023. С. 37–41.

6. Набір портативний «Молекула». Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертизи, юридична психологія / редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 495.

7. Засоби науково–технічні (техніко–криміналістичні). Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертизи, юридична психологія / редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 299, 300.

8. Криміналістика: підручник: у 2 т. Т. 1 / [В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.]; за ред. В. Ю. Шепітька. Харків: Право, 2019. 456 с.

9. Шепітько В. Ю., Когут С. А. Пристрій для виміру швидкості балістичного об’єкта. Патент на винахід № 78847 від 25 квітня 2007 р. зареєстрований в Державному реєстрі патентів України від 25 квітня 2007 р. Бюлетень державного департаменту інтелектуальної власності МОН України, 2007. № 1.

10. Шепітько В. Ю., Авдєєва Г. К. Опис бази знань «Автоматизоване робоче місце слідчого «Інсайт». АРМ слідчого «Інсайт». Свідоцтво № 22566 про реєстрацію авторського права на твір від 6 листопада 2007 р. Бюлетень державного департаменту інтелектуальної власності МОН України, 2007. № 2.

11. Шепітько В. Ю., Фурса В. І. Спосіб формування суб’єктивного портрету «RAIPS–портрет» (комп’ютерного фотороботу). Патент на корисну модель № 69248 від 24 квітня 2012 р.

12. Шепітько В. Ю., Авдєєва Г. К. База даних «Практика слідчого». Свідоцтво № 49389 про реєстрацію авторського права на твір від 30 травня 2013 р.

13. Шепітько В. Ю., Авдєєва Г. К. База даних «Слідчий прецедент». Свідоцтво № 60084 про реєстрацію авторського права на твір від 9 червня 2015 р.

14. Експертиза інженерно–технічна. Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертизи, юридична психологія / редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 241.

15. Богданюк І. Загальна система завдань інженерно–технічних судових експертиз.Теорія та практика судової експертизи і кримі налістики. 2022. Вип. 4

(29). С. 110–123. URL: https://khrife–journal.org/index.php/journal/article/download/550/620/

Секція 2
ЦИФРОВІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОСУДДЯ

DOI https://doi.org/10.32837/11300.33526
Афанасенко Світлана
кандидат юридичних наук, доцент,
судовий експерт відділу науково–методичного та інформаційно–аналітичного забезпечення експертної діяльності Одеського науково–дослідного інституту судових експертиз Міністерства юстиції України,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0008–3017–1683
e–mail: afanasenkosvitlana@gmail.com

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОСУДДЯ

У роботі розглянуто роль цифрових технологій та штучного інтелекту в експертному забезпеченні правосуддя. Показано їх значення для аналізу цифрових доказів, протидії кіберзлочинності та використання віртуальних активів. Визначено основні виклики та перспективи інтеграції інноваційних технологій у судово–експертну діяльність.

Ключові слова: цифровізація, штучний інтелект, експертиза, правосуддя, кіберзлочинність.

Afanasenko Svitlana
PhD in Law, Associate Professor,
Forensic Expert of the Department of Scientific–Methodological and Information–Analytical Support of Expert Activity, Odesa Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine,
Odesa, Ukraine

DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF EXPERT SUPPORT FOR JUSTICE

The paper examines the role of digital technologies and artificial intelligence in forensic support of justice. It highlights their importance for analyzing digital evidence, combating cybercrime, and addressing challenges of virtual assets. The study outlines key risks and prospects of integrating innovative technologies into forensic practice.

Keywords: digitalization, artificial intelligence, forensic expertise, justice, cybercrime.

В Україні приклади використання цифрових доказів можна побачити у справах, пов'язаних із незаконним обігом криптовалют та шахрайством у сфері електронної комерції. Кіберполіція України активно застосовує технології аналізу блокчейн–транзакцій для виявлення злочинних схем [1].

У сучасних кримінальних провадженнях дедалі більшого значення набувають цифрові сліди: електронна переписка може підтвердити факти змови чи шахрайства. Метадані файлів дозволяють встановити час і місце створення документів. Транзакції у віртуальних активах дають змогу простежити рух коштів у криптовалюті.

Штучний інтелект у сучасних дослідженнях розглядається як універсальний інструмент для забезпечення інформаційної безпеки та підвищення ефективності цифрових систем. Його застосування охоплює розпізнавання підроблених документів, виявлення маніпуляцій із цифровими зображеннями та аудіо (deepfake), класифікацію великих масивів даних, аналіз поведінкових моделей користувачів, а також відстеження транзакцій у блокчейні. Такий комплексний підхід сприяє формуванню надійних механізмів протидії кіберзагрозам і забезпечує високий рівень захисту цифрового середовища.

В Україні вже використовуються системи автоматичного аналізу великих масивів даних у кримінальних провадженнях. Наприклад, у справах про фінансові махінації застосовуються алгоритми для виявлення аномалій у банківських операціях.

Міжнародна практика показує, що у США та Великій Британії AI використовується для аналізу цифрових доказів у справах про кіберзлочини, а також для прогнозування ризиків рецидиву злочинців.

Європейський Союз у 2019 році розробив Ethics Guidelines for Trustworthy AI, які передбачають прозорість алгоритмів, захист персональних даних та недопущення дискримінації [2]. Їх інтеграція у національну практику сприятиме гармонізації експертних процедур та підвищенню довіри до результатів досліджень.

Interpol та Europol активно застосовують AI для аналізу транскордонних злочинів, створюючи спільні бази даних і протоколи співпраці. Наприклад, Europol використовує алгоритми для виявлення джерел поширення забороненого контенту [3].

Попри очевидні переваги, інтеграція штучного інтелекту у сферу правосуддя супроводжується низкою суттєвих ризиків. До них належать алгоритмічна упередженість, що може призводити до дискримінаційних рішень; складність перевірки достовірності отриманих результатів, яка ускладнює процес їх використання як доказової бази; можливість маніпуляцій із даними, що створює загрозу для об'єктивності судових процесів; а також потреба у чіткому правовому регулюванні застосування цифрових технологій у доказуванні. Сукупність цих факторів зумовлює необхідність розробки комплексних механізмів контролю та етичних стандартів використання AI у правовій практиці.

Подальші дослідження у сфері застосування штучного інтелекту в правосудді мають бути спрямовані на розробку національних стандартів використання AI у судово–експертній діяльності, створення єдиних баз даних цифрових доказів, впровадження систем незалежної верифікації результатів, а також поглиблення міжнародної співпраці з такими інституціями, як Interpol та Europol. Реалізація зазначених напрямів дозволить забезпечити належний рівень достовірності цифрових доказів, підвищити ефективність судових процедур та зміцнити глобальні механізми протидії кіберзлочинності.

Цифрові технології та штучний інтелект є ключовими чинниками трансформації системи експертного забезпечення правосуддя. Вони забезпечують швидке реагування на нові виклики кіберзлочинності та використання віртуальних активів. Водночас їх застосування потребує чітких правових рамок, етичних стандартів та міжнародної координації. Експертне забезпечення правосуддя у цифрову епоху має стати не лише технічним процесом, а й гарантією дотримання принципів справедливості та прав людини.

Перелік використаних джерел:

1.Головченко Л.М., Лозовий А.І., Сімакова–Єфремян Е.Б. та ін. Основи судової експертизи: навч. посіб. Харків: Право, 2016. 928 с.

2.European Commission. Ethics Guidelines for Trustworthy AI. Brussels, 2019.

3.Interpol. Artificial Intelligence in Policing: Opportunities and Challenges. Lyon, 2021.

DOI https://doi.org/10.32837/11300.33527

Батіг Андрій
старший науковий співробітник лабораторії залізнично–транспортних досліджень Львівського науково–дослідного інституту судових експертиз
м. Львів, Україна
ORCID: https://orcid.org/0000–0003–1205–6004
e–mail: ashabatig1992@gmail.com

ЦИФРОВІ ТЕХНОЛОГІЇ PYTHON У СУДОВІЙ ЗАЛІЗНИЧНО–ТРАНСПОРТНІЙ ЕКСПЕРТИЗІ

Розглянуто перспективи використання Python у судовій залізнично–транспортній експертизі для математичного моделювання, аналізу динаміки рухомого складу та дослідження причин залізнично–транспортних пригод.

Ключові слова: Python, експертиза, моделювання, рухомий склад.

Batig Andriy
Senior researcher at the laboratory of railway transport research,
Lviv research institute of forensic examinations
Lviv, Ukraine

APPLICATION OF PYTHON DIGITAL TECHNOLOGIES IN FORENSIC RAILWAY TRANSPORT EXPERTISE

The prospects of using Python in forensic railway transport examination for mathematical modeling, analysis of rolling stock dynamics, and investigation of the causes of railway transport accidents are considered.

Key words: Python, forensic examination, modeling, rolling stock.

Використання сучасних цифрових технологій у сфері судової залізнично–транспортної експертизи є одним із пріоритетних напрямів розвитку експертної діяльності в умовах стрімкого розвитку інформаційних технологій, програмування та широкого використання систем штучного інтелекту. Значні обсяги технічної інформації, необхідність виконання складних інженерних розрахунків, аналізу параметрів руху поїздів та встановлення причин залізнично–транспортних пригод зумовлюють необхідність застосування ефективних програмних засобів, здатних забезпечити високу точність, швидкість та об’єктивність досліджень. Одним із найбільш перспективних інструментів у цій сфері є мова програмування Python, яка широко використовується для наукових обчислень, аналізу даних та математичного моделювання [1, с. 23]. Завдяки простоті синтаксису, відкритому програмному коду та великій кількості спеціалізованих бібліотек Python дозволяє автоматизувати значну частину

експертних досліджень, що має особливе значення під час проведення судових залізнично–транспортних експертиз.

Актуальність використання програмних засобів у сфері залізнично–транспортної експертизи підтверджується результатами наукових досліджень працівників Львівського науково–дослідного інституту судових експертиз (далі – ЛНДІСЕ), у яких особлива увага приділяється математичному та комп'ютерному моделюванню динаміки рухомого складу, а також застосуванню сучасного програмного забезпечення для аналізу взаємодії рухомого складу і рейкової колії [2, с. 50]. Це свідчить про те, що сучасна судова експертиза поступово переходить від традиційних методів аналізу до цифрових технологій, які забезпечують більш глибоке і змістовне дослідження.

Окрім випадків сходу рухомого складу з рейкової колії, Python може застосовуватися для дослідження випадків травмування людей рухомим складом, зіткнення з автотранспортом, зокрема для аналізу параметрів руху поїздів, розрахунку гальмівного шляху поїзда, моделювання механізму виникнення пригоди тощо. Використання програмного забезпечення дозволяє значно скоротити час виконання розрахунків та мінімізувати ризик виникнення помилок, пов'язаних із людським фактором. Важливе значення мають бібліотеки Python, зокрема NumPy для математичних обчислень, Pandas для обробки великих масивів даних, Matplotlib і Plotly для графічної візуалізації результатів, SciPy для інженерних та статистичних розрахунків, а також OpenCV для аналізу відеоматеріалів [3, с. 17].

За допомогою Python експерт може швидко виконувати багатоетапні розрахунки та перевіряти декілька варіантів розвитку пригод, що суттєво підвищує якість експертного дослідження. Крім того, програмні алгоритми дають можливість створювати інтерактивні моделі руху поїздів і прогнозувати наслідки певних технічних або організаційних помилок.

У наукових дослідженнях експертів ЛНДІСЕ були розроблені розрахункові моделі рухомого складу, у межах яких окремо розглядалися механічні, математичні та комп'ютерні моделі дизель–поїздів і вантажних вагонів, що використовуються для аналізу динаміки руху та причин втрати стійкості рухомого складу [2, 4]. Розробка зазначених моделей здійснювалася із використанням програмного середовища Maple, яке забезпечувало виконання складних математичних розрахунків та моделювання динамічних процесів. Водночас такі розрахункові моделі можуть бути адаптовані та реалізовані за допомогою мови програмування Python, що відкриває ширші можливості для створення універсальних програмних комплексів, автоматизації окремих етапів експертного дослідження, візуалізації результатів розрахунків та подальшого вдосконалення методів судової залізнично–транспортної експертизи.

Особливо важливим є те, що результати, отримані за допомогою Python, можуть бути збережені у вигляді програмного коду, що забезпечує можливість повторної перевірки та підтвердження правильності виконаних розрахунків.

Використання Python також дозволяє автоматизувати формування графіків, схем, таблиць і звітів, що значно спрощує представлення результатів експертизи. Важливою перевагою є можливість інтеграції Python із сучасними базами даних, системами моніторингу руху поїздів та цифровими реєстраторами, що забезпечує комплексний підхід до аналізу транспортних подій.

У сучасних умовах розвитку штучного інтелекту Python також може використовуватися для прогнозування ризиків виникнення аварійних ситуацій на основі статистичних даних та попередніх випадків залізнично–транспортних пригод. У наукових роботах працівників ЛНДІСЕ зазначається, що для встановлення причин складних випадків сходу рухомого складу з рейкової колії необхідним є аналіз поєднання багатьох факторів силової взаємодії рухомого складу та колії [2, с. 85]. Саме програмне моделювання дає можливість враховувати такі фактори комплексно та оцінювати їхній вплив на розвиток пригоди. Крім того, застосування комп’ютерних моделей дозволяє досліджувати вплив технічних несправностей, зокрема зазорів у ходових частинах вагонів, дефектів вузлів тертя, особливостей конструкції рухомого складу та стану рейкової колії [4, с. 15].

Водночас впровадження Python у практику судової залізнично–транспортної експертизи потребує належної підготовки експертів, розробки сучасних методичних рекомендацій та вдосконалення існуючих методик проведення експертних досліджень із використанням програмних засобів. Важливим завданням є також подальший розвиток і модернізація розрахункових моделей рухомого складу, їх адаптація до сучасних програмних платформ та розширення можливостей комп’ютерного моделювання під час дослідження механізму залізнично–транспортних пригод. Незважаючи на окремі труднощі, використання Python у судовій залізнично–транспортній експертизі є перспективним напрямом розвитку сучасної експертної діяльності, оскільки забезпечує підвищення ефективності, точності, об’єктивності та наукової обґрунтованості експертних досліджень.

Перелік використаних джерел:

1. McKinney W. Python for Data Analysis : data wrangling with Pandas, NumPy, and Jupyter. 3rd ed. Sebastopol : O’Reilly Media, 2022. 579 p.

2. Батіг А. В., Кузишин А. Я., Кузін М. О., Грицишин П. М. Розробка методичних рекомендацій із створення розрахункових моделей складових одиниць рухомого складу : звіт про НДР IV.2.2–2020/3. Львів : Львівський НДІСЕ Міністерства юстиції України, 2022. 141 с.

3. Van Rossum G., Drake F. L. Python 3 Reference Manual. Scotts Valley : CreateSpace, 2009. 242 p.

4. Батіг А. В., Кузишин А. Я. Розробка методичних рекомендацій з удосконалення підходів щодо розрахунку критеріїв безпеки руху на залізничному транспорті : звіт про НДР IV.1.3–2018/2. Львів, 2019. 113 с.

DOI https://doi.org/10.32837/11300.33528

Бачило Тетяна
старший судовий експерт Миколаївського відділення Одеського науково–дослідного інституту судових експертиз Міністерства юстиції України
м.Одеса, Україна
ORCID: https://orcid.org/0009–0005–1057–3050
e–mail: mantikorka@ukr.net

ПРОБЛЕМА ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

У тезах проаналізовані сучасні напрями державної політики у сфері цифрового розвитку інноваційної діяльності та наголошено на необхідності нормативно–правового регулювання впровадження та використання штучного інтелекту у судово–експертній діяльності.

Ключові слова: судова експертиза, штучний інтелект, державна політика, законодавство.

Bachylo Tetiana
Senior Forensic Expert of the Mykolaiv Branch of the Odesa Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine
Odesa, Ukraine

THE PROBLEM OF LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ACTIVITY

The theses analyze current directions of state policy in the field of digital development and innovation activity, as well as outline the problem of legal regulation of the implementation and use of artificial intelligence in forensic expert activity.

Keywords: forensic examination, artificial intelligence, public policy, legislation.

Дух дослідництва та прагнення до нових відкриттів завжди відігравали провідну роль у розвитку людства. Сфера судово–експертної діяльності, як і будь–яка інша галузь науки, є динамічною системою, що постійно розвивається та удосконалюється разом із глобальним розвитком суспільства, науки і техніки. На кожному етапі розвитку криміналістики та судочинства з'являлись нові експертні методи та підходи, зумовлені технологічним прогресом. Із розвитком сучасних передових комп'ютерних технологій перед судовими експертами постають нові виклики, що зумовлюють необхідність удосконалення експертної методології з метою розширення спектру розв'язуваних експертних завдань та підвищення ефективності експертної роботи. Одним із допоміжних інструментів досягнення означеної мети є штучний інтелект.

У схваленій розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556–р Концепції розвитку штучного інтелекту в Україні (далі – Концепція) наведене наступне визначення терміну «штучний інтелект»: організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань. Пріоритетними сферами, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, є: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя [1].

Для досягнення мети Концепції за допомогою технологій штучного інтелекту у сфері правосуддя передбачено забезпечення виконання завдань, що стосуються впровадження юридичних консультативних програм для населення, попередження суспільно небезпечних явищ, визначення необхідних заходів ресоціалізації засуджених, винесення судових рішень у справах незначної складності [1]. При цьому виконання завдань, що стосуються судово–експертної діяльності, яка є невід'ємною частиною сфери правосуддя, у Концепції не передбачено.

Розпорядженням Кабінету Міністрів України від 31 грудня 2024 р. № 1351–р схвалена Стратегія цифрового розвитку інноваційної діяльності України на період до 2030 року (далі – Стратегія), прийняття якої обумовлене наступними проблемами.

На початок 2021 року цифровий розвиток в Україні демонстрував позитивні зміни, проте загальний рівень цифровізації залишався нижчим порівняно з провідними європейськими країнами. Показники доступу до швидкісного Інтернету, інтеграції цифрових інструментів у бізнесі та публічних послугах свідчили про необхідність значних інвестицій і реформ. Під час нового етапу збройної агресії Російської Федерації проти України цифрова інфраструктура зазнала численних ударів, що погіршило ситуацію. Новий етап збройної агресії Російської Федерації проти України у 2022 році поглибив довгострокову тенденцію недостатнього інвестування в наукові дослідження та розробки, що завдало шкоди інфраструктурі та послабило людський капітал. З лютого 2022 року по січень 2024 року було пошкоджено або зруйновано 1443 будівлі, що належать 177 науковим установам та закладам вищої освіти. Інженерна інфраструктура науково–дослідних установ також зазнала втрат: 188 інженерних споруд, включаючи лабораторні комплекси та експериментальні майданчики, були пошкоджені або зруйновані. Через пошкодження та руйнування будівель було повністю знищено або виведено з ладу понад 750 одиниць наукового обладнання, яке використовується в широкому спектрі досліджень [2].

Незважаючи на бар'єри, з якими стикаються суб'єкти інноваційної діяльності, державна політика спрямована на підтримку інноваційної діяльності та створення нових можливостей для громадян, підприємців, інвесторів, науковців, дослідників та інноваторів. Проте аналіз Операційного плану заходів з реалізації у 2025–2027 роках Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року [2] та Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки [3], свідчить про те, що визначені в них пріоритетні стратегічні цілі насамперед стосуються сфери вищої освіти та оборони. Сфера судово–експертної діяльності наразі залишається поза увагою зазначених державних програм.

Разом з тим впровадження сучасних технологій для підвищення ефективності діяльності експертних установ потребує від законодавців внесення змін до чинного законодавства, яке регулює судово–експертну діяльність, а також розроблення й ухвалення додаткових нормативно–правових актів, які мають визначати можливості та межі використання моделей та алгоритмів штучного інтелекту, залежно від видів (підвидів) експертної діяльності, а також передбачати шляхи забезпечення конфіденційності обробки і зберігання даних та унеможливлення несанкціонованого втручання в роботу електронних систем.

Поряд із пріоритезацією розвитку інноваційної екосистеми в закладах освіти доцільною є імплементація цифрових інновацій в судово–експертну діяльність. Це сприятиме підвищенню ефективності експертної роботи завдяки досягненню більш високої точності та швидкості обробки великих обсягів даних. За такого підходу стане можливим підвищення привабливості судово–експертної галузі шляхом створення умов для реалізації молодими фахівцями здобутих знань та залучення їх судово–експертними установами.

На нашу думку, судово–експертна діяльність повинна стати однією з пріоритетних галузей державної підтримки стимулювання досліджень, розробок та впровадження цифрових інновацій для того, щоб експерти мали реальну змогу бути озброєними потужним інструментом для підвищення якості та швидкості проведення експертиз та експертних досліджень.

Перелік використаних джерел:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556–р.. URL: https://zakon.rada.gov.ua/laws/show/1556–2020–%D1%80#n137

2. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках : Розпорядження Кабінету Міністрів України від 31.12.2024 № 1351–р.. URL: https://zakon.rada.gov.ua/laws/show/1351–2024–%D1%80#Text

3. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки : Розпорядження Кабінету Міністрів

України від 09.05.2025 № 457–р.. URL: https://zakon.rada.gov.ua/laws/show/457–2025–%D1%80#Text

DOI https://doi.org/10.32837/11300.33529

Білінський Маркіян
судовий експерт лабораторії почеркознавчих та технічних досліджень документів, Львівський науково–дослідний інститут судових експертиз Міністерства юстиції України,
Львів, Україна
ORCID: https://orcid.org/0009–0002–8136–2961
e–mail: mark.19544@gmail.com

ВИКОРИСТАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕХНІКО–КРИМІНАЛІСТИЧНОМУ ДОСЛІДЖЕННІ ДОКУМЕНТІВ

У тезах розглянуто перспективи використання алгоритмів штучного інтелекту для автоматизації аналізу реквізитів документів та ідентифікації друкарських форм у судово–експертній практиці.

Ключові слова: штучний інтелект, судова експертиза, дослідження документів, цифровий аналіз.

Bilinskyi Markiyan
Forensic Expert of the Laboratory of Handwriting and Technical Document Examination, Lviv Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine,
Lviv, Ukraine

APPLICATION OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN TECHNICAL FORENSIC EXAMINATION OF DOCUMENTS

The abstract considers prospects for applying artificial intelligence algorithms to automate document requisites analysis and printing form identification in forensic examination.

Keywords: artificial intelligence, forensic examination, document analysis, digital processing.

Сучасний розвиток судово–експертної діяльності характеризується активним впровадженням цифрових технологій у процес дослідження доказової інформації. Особливо актуальним це є для техніко–криміналістичного дослідження документів, де об’єктивність висновків значною мірою залежить від точності аналізу графічних, морфологічних та спектральних характеристик досліджуваних об’єктів.

Цифрова трансформація судово–експертної діяльності зумовила переосмислення підходів до технічного дослідження документів як складової криміналістичного забезпечення правосуддя. Якщо раніше ключовим

інструментом аналізу залишалося безпосереднє візуальне спостереження експерта, то сучасна практика дедалі більше орієнтується на комплексну цифрову обробку зображень, що дає змогу здійснювати багаторівневу фіксацію ознак документа, їх спектральне розмежування, математичне моделювання контрастності та реконструкцію прихованих або частково втрачених реквізитів. Такий підхід істотно розширює межі доказової інформативності об'єктів дослідження та підвищує об'єктивність експертних висновків.

Традиційні методи експертного аналізу документів базуються на використанні оптичного збільшення, спектральної візуалізації, цифрової мікроскопії та професійної інтерпретації отриманих результатів експертом. Водночас навіть сучасне обладнання не усуває повністю суб'єктивного чинника, оскільки остаточна оцінка ознак здійснюється людиною на основі спеціальних знань та практичного досвіду. Застосування алгоритмів штучного інтелекту відкриває нові можливості автоматизації такого аналізу. Системи машинного навчання здатні обробляти значні масиви цифрових зображень, виявляти закономірності у структурі штрихів, аналізувати мікродефекти друкарських форм, класифікувати спектральні характеристики барвників та визначати ступінь подібності між порівнюваними об'єктами [1, с. 15].

Особливу практичну цінність такі алгоритми мають під час дослідження слабовидимих, частково згаслих або фрагментарно відображених реквізитів. У подібних випадках програмні моделі здатні ідентифікувати статистичні патерни, що можуть залишатися поза межами візуального сприйняття експерта .

Практична цінність цифрових криміналістичних технологій полягає також у можливості повторної верифікації отриманих результатів. Оцифровані спектральні дані можуть бути збережені у незмінному вигляді, що дозволяє здійснювати їх повторний аналіз, незалежну експертну перевірку та комп'ютерне порівняння із контрольними масивами зразків. У кримінальному провадженні це створює додаткові процесуальні гарантії достовірності дослідження, мінімізує суб'єктивний вплив людського фактора та забезпечує відтворюваність результатів, що має особливе значення під час оцінки доказів судом.

Перспективним напрямом є автоматизоване виділення ідентифікаційних ознак друкарських форм. Аналіз локальних дефектів, конфігурації контурів, розподілу фарбувальної речовини та особливостей мікрорельєфу дозволяє формувати цифрові профілі відтисків, придатні для подальшого алгоритмічного порівняння [3, с. 330].

Водночас впровадження штучного інтелекту в судово–експертну практику потребує наукової верифікації алгоритмів, створення репрезентативних навчальних баз та стандартизації процедур оцінки достовірності результатів. Принципово важливим є збереження провідної ролі експерта у формуванні остаточного висновку, оскільки алгоритмічний аналіз має виконувати допоміжну, а не визначальну функцію.

Ще одним цікавим напрямком подальшого розвитку є інтеграція алгоритмів штучного інтелекту в автоматизовані комплекси технічного дослідження документів. Використання методів машинного навчання дає можливість формувати електронні моделі типових спектральних характеристик барвників, автоматично класифікувати ознаки їх деградації та прогнозувати найбільш ефективні режими візуалізації для конкретного об'єкта. У перспективі це сприятиме створенню інтелектуальних експертних систем підтримки прийняття рішень, здатних підвищити швидкість і точність криміналістичного аналізу документів у складних та нестандартних експертних ситуаціях [2, с. 410].

Окремої уваги заслуговує трансформація професійних компетенцій самого експерта в умовах цифровізації. Впровадження інтелектуальних алгоритмів не зменшує вимог до рівня його підготовки, а навпаки – потребує опанування нових навичок роботи з програмними комплексами та розуміння логіки обробки даних машиною. Поєднання традиційних криміналістичних знань із базовим розумінням принципів роботи нейромереж дозволяє фахівцю критично оцінювати результати, отримані автоматизованою системою, та вчасно виявляти можливі технічні похибки чи артефакти цифрової обробки. Таким чином, синергія людського досвіду та обчислювальної потужності стає запорукою мінімізації помилок, які раніше могли бути допущені через втому або обмежені можливості людського ока.

Отже, інтеграція алгоритмів штучного інтелекту в техніко–криміналістичне дослідження документів забезпечує перехід від описової до аналітико–обчислювальної моделі експертизи. Використання машинного навчання дозволяє автоматизувати ідентифікацію мікродефектів друкарських форм та верифікувати спектральні характеристики матеріалів з точністю, що перевищує межі візуального сприйняття. Це мінімізує вплив суб'єктивного фактора, забезпечує відтворюваність результатів у процесуальному контексті та створює умови для формування об'єктивної доказової бази. Таким чином, цифрова трансформація є необхідним етапом розвитку судової експертизи, спрямованим на підвищення достовірності та швидкості вирішення складних криміналістичних завдань.

Перелік використаних джерел:

1. Ковальов К. М., Коваленко В. В. Методика технічної експертизи відбитків печаток та штампів. Київ: ДНДЕКЦ МВС України, 2008. 19 с.

2. Moorthy N., Narayanan K. Selected Charred Documents Using Video Spectral Comparator (VSC). Arab Journal of Forensic Sciences and Forensic Medicine. 2016. Vol. 1 (4). P. 406–413.

3. Бірюков В. В., Коваленко В. В., Бірюкова Т. П., Ковальов К. М. Криміналістичне документознавство : практ. посіб. Київ : ПАЛИВОДА А. В., 2007. 332 с.

DOI https://doi.org/10.32837/11300.33530

Возовик Юрій
начальник відділу Центру судових і спеціальних експертиз Українського науково–дослідного інститут спеціальної техніки та судових експертиз Служби безпеки України, м. Київ, Україна
ORCID https://orcid.org/0009–0009–2977–4038
e–mail: amonium@ssu.gov.ua

ОСОБЛИВОСТІ ЦИФРОВОЇ ФІКСАЦІЇ СЛІДІВ ТЕРМІЧНОГО ВПЛИВУ В СУДОВО–ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

У тезах розглянуто особливості цифрової фіксації слідів термічного впливу під час проведення судових пожежно–технічних експертиз та експертних досліджень. Проаналізовано впровадження цифрових технологій та інноваційні підходи. Визначено проблеми та перспективи розвитку.

Ключові слова: цифрова фіксація, термічний вплив, судова експертиза, фотофіксація, пожежно–технічна експертиза, сліди горіння.

Vozovyk Yurii
head of section of the Center of forensic and special expertise of the Ukrainian scientific and research institute of special equipment and forensic expertise of the Security service of Ukraine,
Kyiv, Ukraine

FEATURES OF DIGITAL RECORDING OF TRACES OF THERMAL IMPACT IN FORENSIC EXPERTISE

The abstracts consider the features of digital recording of traces of thermal exposure during forensic fire technical expertise. There introduction of digital technologies and approaches are analyzed here.

Key words: digital fixation, thermal effect, forensic expertise, foto fixation, forensic fire technical expertise, traces of burning.

Сучасна судово–експертна діяльність характеризується активним впровадженням цифрових технологій у процеси дослідження об’єктів, що зазнали термічного впливу. Особливої актуальності це питання набуває в умовах збройної агресії рф проти України, коли значна кількість об’єктів інфраструктури, транспортних засобів, промислових споруд та цивільних будівель піддаються впливу високих температур унаслідок пожеж, вибухів і застосування боєприпасів.

На теперішній час судово–експертна діяльність перебуває на етапі технологічної трансформації [1, с. 396]. Застосування сучасних методів і цифрових технологій сприяє підвищенню ефективності та якості досліджень, зменшенню часу на підготовку висновків та забезпеченню їх об’єктивності,

оскільки традиційні методи фіксації слідів термічного впливу вже не забезпечують повноцінного відображення просторових, температурних та морфологічних характеристик пошкоджень. Саме тому цифрова фіксація стає одним із ключових елементів судово–експертного дослідження.

Аналіз цифрових слідів на місці пожежі, створених наявними електронними пристроями, може надати високоточну інформацію [2, с. 2] під час встановлення осередку пожежі, причини її виникнення та механізму поширення. В першу чергу це стосується електронних пристроїв, які були присутні під час пожежі або в безпосередній близькості від неї, та на яких потенційно створені цифрові сліди під час самої пожежі. Проте, під час досліджень судовий експерт–пожежотехнік

Відомими методами цифрової фіксації слідів термічного впливу на місці пожежі є цифрова фотозйомка, тепловізійна зйомка та 3D–сканування.

Цифрова фотозйомка є найпоширенішим методом цифрової фотофіксації. При її проведенні слід приділяти особливу увагу правильному освітленню та дотримання геометрії зйомки. Перевагами цифрової фотозйомки над іншими методами є її оперативність, доступність, відсутність потреби в додатковому обладнанні та програмному забезпеченні, проте недоліком є те, що не завжди в повній мірі можливо відобразити всі криміналістично значущі характеристики досліджуваного об’єкта. На відміну від тепловізійної фіксації, цифрова фотозйомка передає лише видимий спектр світла та не дозволяє фіксувати залишкові температурні аномалії.

Тепловізійна фіксація забезпечує отримання температурних карт об’єкта, що значно підвищує точність подальшого експертного аналізу. Перевагами тепловізійної фіксації є можливість виявлення залишкових температурних осередків, прихованих зон горіння, ділянок з нерівномірним розподілом температур. Недоліками методу є можливість його застосування в короткий проміжок після пожежі, що робить його не досить ефективним, так як з моменту призначення судової експертизи до огляду місця пожежі проходить деякий час.

3D–сканування є досить інноваційним методом цифрової фіксації, який дозволяє створювати цифрові моделі місця пожежі та відтворювати просторове розташування пошкоджень. Перевагами вказаного методу є висока точність, збереження геометрії пошкоджень, можливість виконання якісного дистанційного аналізу. Недоліками методу є надзвичайно висока вартість обладнання, необхідність застосування спеціалізованого програмного забезпечення, відсутність достатньої кількості фахівців, спроможних проводити 3D–сканування саме місця пожежі.

Загальними проблемними питаннями застосування цифрової фіксації слідів термічного впливу на місці пожежі можливо виділити різний рівень технічного забезпечення експертних установ, складність забезпечення автентичності цифрових файлів, ризики втрати метаданих та потреба у спеціальній підготовці судових експертів. Шляхами покращення діяльності за вказаним напрямом є вдосконалення напрямів підготовки судових експертів, розроблення методичної

літератури з питань інноваційних методів цифрової фіксації на місці пожежі, придбання необхідного обладнання та програмного забезпечення, а також залучення міжнародної допомоги.

Таким чином, розвиток напрямів цифрової фіксації слідів термічного впливу на місці пожежі є одним із найважливіших кроків вдосконалення сучасної судово–експертної діяльності за напрямом дослідження пожеж. Це дозволяє максимально повно відобразити морфологічні, просторові та термічні характеристики на місці пожежі, а в разі комплексного застосування різних методів цифрової фіксації – забезпечити надзвичайно високу точність, об’єктивність та відтворюваність результатів досліджень.

Перелік використаних джерел:

1. Bengtsson J., Delémont O., Jonsson F., Souvignet T. R. Integrating digital forensics into fire scene investigation: Enhancing reconstruction and analysis. *Forensic Science International*. 2026. Vol. 384. Article 112924. DOI: 10.1016/j.forsciint.2026.112924.

2. Олександр Подус. Сучасні методи та технології в судово–експертній діяльності: інтеграція інновацій. *Актуальні питання судової експертизи і криміналістики* : зб. мат–лів Міжнар. наук.–практ. конф., присвяч. пам’яті видатн. вчен., д–ра юрид. наук, проф. Владислава Федоренка («Федоренківські читання») (Харків, 15.10.2025). Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2025. С. 394–396.

DOI https://doi.org/10.32837/11300.33622

Vozian Viorica
Expert judiciar al Centrului Naţional de Expertize Judiciare Ministerul Justiţiei, mun. Chişinău, Republica Moldova,
ORCID: https://orcid.org/0009–0000–0553–1650
E–mail: vozianviorica79@gmail.com

METODE DE CERCETARE ȘI ANALIZĂ A LIMBAJULUI INVECTIV ÎN CADRUL EXPERTIZEI JUDICIARE DE AUTOR

Tema abordată, în acest articol, este de mare actualitate, fiind un subiect de interes pentru specialiștii din diverse arii de cercetare, odată cu creșterea cazurilor de litigii privind limbajul ofensator. În epoca digitală, discursul agresiv și injurios este prezent, atât în spațiul public, cât și în mediul online. În acest context, analiza lingvistică joacă un rol esențial în determinarea intenției autorului, a gravității injuriilor și a impactului acestora. Cercetarea subiectului dat va contribui la dezvoltarea unor metode precise și obiective pentru analiza discursului invectiv.

Astfel, limbajul invectiv este un fenomen lingvistic complex, cu un impact semnificativ asupra relațiilor interpersonale, reputației și imaginii publice a indivizilor sau instituțiilor. În cadrul expertizei judiciare de autor, expertul va adopta o metodologie obiectivă și riguroasă pentru a determina dacă anumite declarații/ texte constituie atacuri verbale sau acte de defăimare.

Analiza lingvistică nu se limitează la identificarea expresiilor jignitoare, ci implică și evaluarea contextului. Expertul judiciar trebuie să fie conștient de implicațiile legale și morale ale limbajului invectiv, tratând fiecare caz cu imparțialitate, respectând principiile fundamentale ale normelor legale și ale eticii judiciare.

Cuvinte – cheie: expertiză judiciară, limbaj invectiv, defăimare, lingvistică, metodă, evaluare contextuală, etc.

Viorica Vozian
Forensic expert at the National Center for Judicial Expertise of the Ministry of Justice, Chişinău Municipality, Republic of Moldova

METHODS FOR RESEARCHING AND ANALYZING INVECTIVE LANGUAGE IN FORENSIC AUTHORSHIP

This topic is highly topical for a number of reasons relevant to the legal, linguistic and social fields, being a subject of interest for specialists in various areas of research, with the increase in litigation cases concerning offensive language. In the digital age, aggressive and offensive speech is present, both in the public space and online. In this context, linguistic analysis plays a key role in determining the intent of the author, the

severity of the insult and its impact. Research on the given topic will contribute to the development of precise methodologies for analyzing invective discourse.

Thus, invective is a complex linguistic phenomenon with a significant impact on interpersonal relations, reputation and public image of individuals or institutions. In forensic authorship expertise, the expert will adopt an objective and rigorous methodology to determine whether certain statements/texts constitute verbal attacks or acts of defamation.

Linguistic analysis is not limited to the identification of offensive expressions, but also involves context assessment. The forensic expert must be aware of the legal and moral implications of invective language, treating each case with impartiality, respecting the fundamental principles of legal rules and judicial ethics.

Key words: forensic expertise, invective language, defamation, linguistics, method, contextual assessment, etc.

INTRODUCERE

Limbajul invectiv este o formă de comunicare agresivă, caracterizată prin utilizarea unor expresii jignitoare, ofensatoare sau defăimătoare, cu scopul de a discredita, intimida sau afecta reputația unei persoane/ instituții. [2, p. 102] Într–o societate, în care interacțiunile verbale se desfășoară atât în spațiul public, cât și în mediul online, fenomenul invectivelor capătă o amploare tot mai mare, generând conflicte juridice și sociale. Prin urmare, analiza textelor în litigiu devine esențială pentru delimitarea libertății de exprimare de discursul injurios, instigator la ură sau defăimător.

În acest context, expertiza judiciară de autor joacă un rol crucial în evaluarea limbajului invectiv, aplicându–se metode riguroase de analiză lingvistică și juridică pentru a determina dacă un anumit text sau discurs poate fi considerat ofensator sau defăimător și dacă există elemente care să probeze intenția autorului. Expertul lingvist nu se limitează doar la identificarea cuvintelor cu conotații negative, ci studiază și contextul în care acestea au fost utilizate, relația dintre emițător și receptor, tonul, stilul textului și impactul acestuia asupra persoanelor vizate. [5, p. 78]

Expertiza judiciară trebuie să fie obiectivă, imparțială și să respecte principiile fundamentale ale dreptului și eticii judiciare. În acest sens, expertul ține cont de criterii clare în evaluarea limbajului defaimator, evitând interpretările subiective și asigurând o analiză bazată pe dovezi lingvistice solide. De asemenea, cercetările trebuie să fie adaptate noilor realități ale comunicării, având în vedere expansiunea discursului injurios în mediul digital și rețelele sociale, unde astfel de manifestări sunt tot mai frecvente și mai dificil de controlat.

Importanța studierii limbajului invectiv în expertiza judiciară de autor rezidă în necesitatea de a proteja atât dreptul la liberă exprimare, cât și demnitatea și reputația persoanelor. O reglementare clară și o aplicare consecventă a normelor juridice pot contribui la prevenirea abuzurilor și la sancționarea adecvată a textelor ce conțin limbaj injurios.

REZULTATE OBȚINUTE, DISCUȚII

În sistemul judiciar, expertiza de autor joacă un rol esențial, având ca scop analiza limbajului scris al unui text pentru a identifica particularitățile acestuia și ale autorului. Încadrată în domeniul criminalisticii tradiționale, expertiza include o evaluare detaliată a textelor din perspectivă lingvistică, stilistică și gramaticală. [4, p. 98]

În acest context, unul dintre aspectele frecvent analizate este limbajul invectiv, adică utilizarea unui discurs agresiv și denigrator, caracterizat prin insulte, atacuri sau denigrări directe, având scopul de a răni, înjosi sau discredita o persoană. Lexemul «invector» desemnează persoana care emite atacuri verbale, în timp ce «invectum» este cel care le primește. Expertul va stabili în ce măsură un text conține elemente injurioase și dacă se încalcă normele eticii verbale sau au un impact juridic. Astfel, acest gen de expertiză nu identifică doar trăsăturile lingvistice ale unui text, ci ajută instanțele să stabilească limitele dintre libertatea de exprimare și conținutul ofensator cu impact legal. [5, p. 97]

Limbajul invectiv se manifestă sub diferite forme: insulte directe, cuvinte vulgare, jigniri care pun în pericol imaginea unei persoane, atacuri asupra caracterului, onorabilității sau reputației unui individ sau grup social, de exemplu:

Insulte directe: «Ești un mincinos!» sau «Nu ești bun de nimic!»;

Atacuri asupra caracterului: «Niciodată nu vei reuși nimic în viață!»;

Vulgarități și cuvinte jignitoare: «Fii liniștit, prostule!» sau «Ești o rușine!»;

Mai întâi de toate, se analizează aspectele esențiale: dacă textul conține insulte, jigniri, atacuri personale sau expresii ce pot avea o conotație negativă («Ești un incompetent care nu înțelege nimic!» «Acel politician este un mincinos ordinar și un escroc.» «Nu merită să fie profesor, habar nu are de materia pe care o predă.»). Se identifică lexeme tabu, vulgarisme sau termeni cu o încărcătură emoțională puternic ofensatoare («Este un idiot notoriu, un dobitoc care nu ar trebui să vorbească.»; «O adunătură de hoți și escroci care își bat joc de oameni.»; «Ăsta nu e jurnalism, e doar niște mizerii scrise de niște gunoaie.»). De asemenea, se examinează dacă textul conține ironii, sarcasm sau insinuări, care ar putea fi percepute ca o formă indirectă de atac, de exemplu: «A, da, sigur că el e cel mai mare expert! Tocmai el să ne dea lecții?»; «Ce politician onest! Păcat că nu–l mai crede nimeni.»; «Nu știu cum reușește să conducă o echipă cu atâta incompetență, dar iată că o face.» Exemplele, sus–menționate, demonstrează modul în care limbajul invectiv poate fi utilizat pentru a submina reputația și statutul unei persoane sau instituții. În cercetare, se ține cont și de factori precum normele sociale, cultura lingvistică și sensibilitățile existente într–un anumit mediu. De exemplu, într–o conversație informală între prieteni, expresia «Ești nebun!» – poate fi folosită cu o conotație amicală și jucăușă, însă, într–un context formal sau profesional, aceeași expresie poate fi interpretată ca o insultă gravă; lexemul «țigan» este considerat ofensator în multe contexte, dar, în anumite comunități rome, e un termen neutru de autoidentificare.

Interpretarea limbajului invectiv trebuie făcută ținând cont de contextul în care a fost utilizat. Cuvintele și expresiile au sensuri diferite în funcție de comunitatea

lingvistică, normele sociale și stilul comunicării. Prin urmare, expertiza de autor analizează nu doar lexicul utilizat, ci și modul în care este perceput de audiența căreia îi este adresat. Se evaluează dacă textul a fost redactat într–un context artistic, umoristic sau publicistic, caz în care sensul cuvintelor poate varia – într–un spectacol de standup comedy, o glumă poate conține termeni jignitori, dar intenția este de a stârni râsul, nu de a denigra pe cineva; un alt exemplu sunt articolele de satiră politică, expresii precum: «Guvernul doarme» sau «Ministrul X e un dezastru ambulant», pot fi folosite pentru a critica guvernarea, fără a avea neapărat o intenție calomnioasă. În astfel de situații, se evaluează dacă expresiile sunt parte a unui stil artistic/ publicistic, unde libertatea de exprimare are un rol important, sau dacă ele depășesc limitele și devin injurioase.

Metode și instrumente utilizate în analiza limbajului invectiv:

Expertul judiciar utilizează o serie de tehnici și metode lingvistice pentru a evalua nivelul de agresivitate și potențialul ofensator al unui text. Printre acestea, se numără analiza semantică și pragmatică a textului, studiindu–se sensul cuvintelor, relația acestora cu contextul în care sunt utilizate pentru a determina intenția comunicativă a autorului și impactul asupra receptorului. [3, p. 149]. Analiza se desfășoară pe două niveluri:

1. Semantică – studiul sensului cuvintelor și relația acestora cu contextul

Analiza semantică se concentrează pe înțelesul strict al cuvintelor și expresiilor utilizate într–un text: examinarea sensului denotativ și conotativ. Denotativ (propriu, literal) – se analizează dacă termenii folosiți au un sens obiectiv, clar și lipsit de ambiguitate: «Persoana X este incompetentă»– afirmă direct lipsa de competență a cuiva într–un domeniu. Conotativ (subiectiv, figurat) – se studiază dacă expresiile au un sens figurat sau metaforic, care ar putea influența interpretarea textului: «Persoana X este o cârpă în politică», are o conotație negativă și poate fi interpretată ca o insultă.

Următorul pas al cercetării este identificarea termenilor cu încărcătură negativă sau ofensatoare, analizându–se dacă textul conține epitete depreciative, hiperbole sau termeni agresivi, de exemplu: «Acest individ este un escroc»– are o încărcătură semantică gravă, sugerând un comportament ilegal; «E doar un măscărici»– poate fi o exprimare depreciativă menită să discrediteze pe cineva. Se detectează inclusiv ambiguitățile și insinuările din enunțuri: «Nu știu dacă X a furat, dar toată lumea vorbește despre asta» – sugerează o acuzație fără a o formula direct; «Oricine ar trebui să fie atent în preajma lui Y» – se referă la comportamentul suspect al cuiva.

2. Analiza pragmatică – examinarea tonului discursului și intenției comunicative

Prin analiză pragmatică, se are în vedere modul în care un mesaj este înțeles în funcție de contextul comunicativ și de relația dintre autor și destinatari. Se determină nu doar sensurile explicite, ci și mesajele implicite sau manipulatoare care pot influența percepția publicului. În primul rând, se ține cont dacă tonul este agresiv, sarcastic, ironic sau neutru, vom da câteva exemple în acest sens: «Bravo, ai făcut o treabă excelentă» – poate fi un compliment sau o ironie, în funcție de context; «Ești un geniu al greșelilor» – exprimă sarcasm, chiar dacă aparent include un cuvânt cu sens pozitiv. În continuare, se analizează dacă scopul autorului este de a informa, de a influența opinia publică sau

de a denigra o persoană: «Persoana X a fost condamnată pentru corupție» – transmite o informație obiectivă; «Toată lumea știe că X este corupt» – sugerează o opinie generală fără a aduce dovezi, bineînțeles că se ține cont de locul unde a fost publicat textul (presă, rețele sociale, discurs public etc.) și de publicul țintă. [3, p. 140]

În expertiza judiciară de autor, un pas esențial este analiza lingvistică cantitativă a textului, care presupune identificarea și măsurarea frecvenței cuvintelor cu caracter denigrator. Acest proces ajută la stabilirea intenției comunicative a autorului și la compararea stilului acestuia cu alte texte cunoscute. În asemenea situații, se identifică și se cuantifică prezența cuvintelor cu caracter denigrator într–un text, se compară aceste frecvențe cu alte texte cunoscute pentru a determina dacă utilizarea termenilor respectivi este o trăsătură specifică stilului autorului. Înainte de a cuantifica frecvența utilizării unui limbaj ofensator, expertul va identifica termenii care au sau pot avea o conotație denigratoare. Aceștia pot fi clasificați astfel: insulte și epitete («mincinos», «incompetent», «escroc», «trădător»); expresii care sugerează inferioritate sau lipsă de valoare («Nu valorează nimic», «nu are nicio calitate», «e doar un parazit»); vulgarisme și expresii obscene, adesea folosite în atacuri verbale directe («prost», «cretin», «jegos»); ironii și sarcasm, care pot avea efect denigrator («Ce mare specialist… dacă greșelile ar fi o meserie»); expresii insinuante, care scot în evidență un defect fără a–l menționa direct («Toți știu ce fel de om este X»). După identificarea acestor termeni, se creează o bază de date cu posibile cuvinte și expresii invective, care este folosită pentru analiza frecvenței lor în textul investigat.

Pentru a determina, dacă un text conține un număr semnificativ de termeni cu caracter denigrator, se utilizează metode cantitative, precum: analiza frecvenței absolute – se numără de câte ori apar anumite cuvinte denigratoare într–un text. [3, pag. 148] Dacă într–un articol de 500 de cuvinte apare de 15 ori cuvântul «incompetent», se poate considera o utilizare excesivă. Altă metodă este analiza frecvenței relative – se calculează raportul dintre numărul de cuvinte denigratoare și numărul total de cuvinte din text, exprimat în procente. De exemplu, dacă 5% din cuvintele unui text sunt jignitoare, se poate concluziona că tonul este puternic denigrator. De o importanță deosebită e și analiza distribuției termenilor – se analizează dacă termenii denigratori sunt distribuiți uniform în text sau concentrați în anumite părți (de exemplu, în concluzie, unde impactul este maxim). În caz că termenii ofensatori apar preponderent în introducere și concluzie, există o intenție clară de influențare a cititorului. Pentru a stabili dacă utilizarea unui limbaj denigrator este o trăsătură specifică stilului autorului sau dacă–i o excepție, expertul compară frecvența termenilor care îl interesează, cu alte texte scrise de același autor. Se cercetează dacă scriptorul utilizează frecvent termeni denigratori sau dacă acest stil este atipic pentru el. De exemplu, dacă într–un alt text al aceluiași autor rata de utilizare a cuvântului «incompetent» este de 0,5%, iar, în textul în litigiu, este de 5%, se poate concluziona că acesta are un ton mai agresiv decât în mod obișnuit. Se recomandă compararea cu texte similare din același domeniu, care se încadrează în același stil. Odată cu dezvoltarea tehnicii informaționale, există programe ce analizează frecvența cuvintelor și tiparelor stilistice, pentru a face acest lucru automat.

Prin urmare, identificarea și cuantificarea cuvintelor denigratoare într–un text sunt etape esențiale în expertiza judiciară de autor. Aceste metode permit stabilirea unui profil lingvistic al autorului, evaluarea intenției comunicative și determinarea impactului asupra imaginii persoanei vizate. Compararea frecvențelor cu alte texte oferă o perspectivă obiectivă asupra tonului și stilului utilizat, contribuind la o evaluare corectă în cadrul proceselor judiciare.

Altă metodă, utilizată de către experții lingviști, este analiza stilistică și discursivă. În primul rând, se examinează structura frazelor, alegerea cuvintelor și strategiile retorice utilizate pentru a determina dacă textul are o tentă agresivă. [3, p. 178] Se analizează dacă limbajul invectiv este utilizat într–o manieră directă (insultă explicită) sau indirectă (insinuare, ironie, sarcasm). Limbajul invectiv poate fi identificat prin analiza modului în care sunt construite frazele și prin alegerea deliberată a anumitor termeni care sugerează atac sau discreditare, de exemplu:

Frazele scurte și imperative – pot sugera un ton agresiv, abrupt, lipsit de nuanțare («Minte! E un escroc!» – afirmație directă și categorică, fără explicații);

Utilizarea excesivă a propozițiilor exclamative și interogative retorice – crește impactul emoțional și poate sugera o intenție polemică («Cum poate cineva să creadă asemenea prostii?!»);

Conectivele adversative și concesive – Cuvinte precum «dar», «totuși», «în realitate» sunt adesea folosite pentru a submina afirmații sau persoane («Se pretinde expert, dar nu înțelege nimic.»);

Repetiția unor termeni peiorativi – subliniază intenția de atac («E un incompetent total! Absolut nimic nu face bine! Zero profesionalism!»);

Utilizarea construcțiilor pasiv–agresive – se evită atacul direct, dar se sugerează un mesaj denigrator («Nu vreau să spun că e corupt, dar toți știm cum obține contractele.»).

Autorii, care folosesc un limbaj invectiv, recurg la diverse tehnici retorice pentru a–și atinge scopul, folosind insulte explicite («Este un impostor și un mincinos dovedit.») sau implicite, fără a afirma direct («Mulți s–ar întreba dacă are vreo competență reală…»). Deseori, ironia și sarcasmul sunt folosite pentru a ataca subtil, făcând ca mesajul să pară inofensiv la suprafață, dar jignitor în esență («Sigur, el e cel mai mare specialist… dacă greșelile ar fi o meserie.»; «Felicitări! Ai reușit să fii cel mai incompetent om din echipă.»). Textele cu tentă agresivă folosesc adesea hiperbole și apeluri emoționale pentru a intensifica atacul («Nu a făcut în viața lui nimic util!»; «Această persoană este un pericol pentru societate!». [5, p. 320]

Prin analizarea tuturor acestor elemente, expertul apreciază dacă textul are o tentă agresivă și dacă limbajul invectiv este folosit intenționat pentru a discredita o persoană. Această apreciere este esențială în procese de defăimare sau calomnie.

În sec. al XXI–lea, în expertiza de autor, se folosesc softwarurilor de analiză textuală, programe informatice specializate pentru identificarea modelelor de limbaj ofensator. Aceste instrumente ajută la evidențierea expresiilor problematice și a asocierilor de termeni care ar putea indica un atac verbal.

Una dintre provocările principale în evaluarea limbajului invectiv în cadrul expertizei judiciare este subiectivitatea percepției asupra cuvintelor jignitoare. În anumite cazuri, un cuvânt sau o frază poate fi perceput ca o simplă opinie, în timp ce în altele poate fi interpretat ca un atac direct și deliberat.

Pentru a rezolva aceste ambiguități, expertul judiciar trebuie să adopte o metodă obiectivă și riguroasă de analiză, care să includă:

Analiza contextului: Contextul, în care este utilizat un lexem, are un rol decisiv în interpretarea sa.

Compararea cu textele similare: Expertul are posibiliateta de a compara limbajul invectiv din text cu alte exemple din literatură sau din practică, pentru a stabili dacă lexemele/expresiile utilizate au un caracter defăimător.

Cercetarea vine în sprijinul organelor de drept ca să distingă insultele directe de o exprimare liberă a opiniilor.

CONCLUZIE

Limbajul invectiv reprezintă un fenomen lingvistic complex, care poate afecta grav relațiile interumane, reputația și imaginea publică a unei persoane sau instituții. În cadrul expertizei judiciare de autor, este esențial ca expertul să aplice metode obiective pentru a putea oferi niște concluzii bine argumentate din punct de vedere științific. Analiza expresiilor/termenilor defăimători presupune nu doar identificarea lor, dar și evaluarea contextului, impactul acestora asupra celor vizați.

Expertul judiciar trebuie să fie conștient de implicațiile legale, morale ale limbajului invectiv, să abordeze fiecare caz cu imparțialitate, respect față de principiile fundamentale ale dreptului și ale eticii judiciare.

Bibliografie

1. Stilistica limbii române / I. Iordan, , Editura Ştiinţifică, Bucureşti, 1975.

2. Elemente de lingvistică structurală / I. Coteanu, Ed. didactică și pedagogică, Bucureşti, 1973.

3. Diversitate stilistică în româna actuală / R. Zafiu, Editura Universității din Bucureşti, 2001.

4. Expertiza judiciară / O.Cataraga, Editura Pro Universitaria, București, 2022.

5. The Idea of progress in forensic authorship analysis / T. Grant, Cambridge University Press, Marea Britanie, 2022.

6. Despre libertate (On Liberty) / Mill J. S., Editura Humanitas, București, 2014.

DOI https://doi.org/10.32837/11300.33531

Галайко Марина
судовий експерт Львівського науково-дослідного інституту судових експертиз Міністерства юстиції України,
м. Рівне, Україна
ORCID: https://orcid.org/0009–0007–2389–0623
e–mail: marinkaexpert2024@gmail.com

ІНТЕГРАЦІЯ ЦИФРОВИХ ІННОВАЦІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ В БУДІВЕЛЬНО–ТЕХНІЧНУ ЕКСПЕРТИЗУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У тезах розглянуто інтеграцію цифрових інновацій та штучного інтелекту в будівельно–технічну експертизу. Доведено, що поєднання класичних методів зі штучним інтелектом та георадарним зондуванням є ключовим інструментом протидії фальсифікаціям у судовому процесі.

Ключові слова: судова експертиза, цифрові інновації, штучний інтелект, нерухоме майно, криміналістика.

Marina Halayko
forensic expert at the Lviv Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine,
Rivne, Ukraine

INTEGRATION OF DIGITAL INNOVATIONS AND ARTIFICIAL INTELLIGENCE IN CONSTRUCTION AND TECHNICAL EXPERTISE: CHALLENGES AND DEVELOPMENT PROSPECTS

The theses consider the integration of digital innovations and artificial intelligence in construction and technical expertise. It is proven that the combination of classical methods with artificial intelligence and ground–penetrating radar is a key tool to combat falsifications in the judicial process.

Key words: forensic expertise, digital innovations, artificial intelligence, real estate, criminology.

Розвиток сучасної криміналістики нерозривно пов’язаний із цифровізацією всіх сфер суспільного життя, що породжує як нові можливості, так і глобальні виклики. У сфері будівельно–технічної експертизи цифрова трансформація стає необхідним інструментом для забезпечення доказової достовірності та питання класифікації нерухомого майна набуває нових вимірів. Цифрові інновації змінюють підходи до збору, обробки та аналізу даних під час проведення будівельно–технічних експертиз, що прямо впливає на обґрунтованість висновків щодо класифікації об’єктів як рухомого чи нерухомого майна. [6; 8].

У процесі європейської інтеграції України судово–експертна практика щодо класифікації нерухомого майна поступово узгоджується з європейськими стандартами та передбачає впровадження принципів оцінки технічного стану об'єктів, використання цифрових технологій для збору та аналізу даних, а також підвищення прозорості й доказової достовірності експертних висновків. Застосування міжнародних методик – стандартів ISO, рекомендацій Ради Європи та принципів Європейської комісії з питань нерухомості – сприяє покращенню якості експертиз, зменшенню правових суперечок і наближенню української практики до європейських вимог. Це підвищує професійний рівень експертів і забезпечує відповідність результатів судово–експертних досліджень стандартам ЄС у сфері оцінки та управління нерухомим майном.

Цивільний кодекс України визначає, що до нерухомих речей належать земельні ділянки, а також об'єкти, переміщення яких без знецінення або втрати призначення є неможливим (ст. 181) [1]. Законодавче визначення, хоч і є базовим, однак часто вимагає експертного тлумачення при розгляді конкретних об'єктів. Наприклад, питання щодо тимчасових споруд, кіосків, павільйонів або модульних будівель викликають дискусії як у науковому середовищі, так і серед практикуючих експертів та юристів.

У судово–експертній практиці це означає необхідність врахування технічних, правових та функціональних характеристик об'єкта, серед яких ключовими є наявність фундаменту, зв'язок із землею, підключення до інженерних мереж, капітальність споруди тощо [8; 5].

З позиції судового експерта, ідентифікація об'єкта як нерухомого майна передбачає об'єктивний аналіз технічних характеристик, нормативної бази та фактичного стану. Зокрема, враховуються:

спосіб кріплення до землі (на фундаменті чи без нього);

наявність комунікацій (електрика, водопостачання, каналізація);

можливість демонтажу без порушення цілісності;

наявність дозвільної документації (права власності, введення в експлуатацію тощо);

ознаки капітальності будівництва.

У цьому контексті важливим є дотримання принципу індивідуального підходу до кожного випадку експертизи. Наприклад, вагончик для тимчасового проживання, встановлений на бетонних блоках без фундаменту, не матиме ознак нерухомості, якщо його можна демонтувати без знищення конструктивних елементів. Водночас аналогічна за виглядом споруда з фундаментом, інженерними мережами та незнімною конструкцією розглядається як нерухоме майно.

У процесі встановлення, чи є об'єкт нерухомим майном, ключове значення має дослідження наявності, типу та глибини фундаменту, що безпосередньо впливає на висновок про капітальність споруди та її зв'язок із землею.

Фундамент – частина будівлі чи споруди, переважно підземна, яка сприймає навантаження від споруди і передає їх на основу, складену ґрунтами (природну) чи штучну.

Фундаменти малозаглиблені, мілкого закладання – передають навантаження на ґрунт переважно через підошву фундаменту.

Фундаменти заглиблені – передають навантаження на ґрунт через підошву і бічну поверхню фундаменту, враховується тиск ґрунту на бічну поверхню заглибленої (стінової) частини споруди.

Фундаменти глибокого закладання – передають навантаження на ґрунт просторової основи за допомогою тертя чи зчеплення по всіх поверхнях контакту конструкції фундаменту з основою (вертикальні, похилі поверхні і підошва). [4]

Наявність капітального фундаменту, зазвичай свідчить про капітальність споруди, а отже – про її нерухомий характер.

Для встановлення факту наявності фундаменту та його глибини проводиться візуально–інструментальне обстеження об’єкта. Основні етапи включають:

Візуальний огляд: зовнішній огляд будівлі, аналіз технічної документації (проєкт, техпаспорт, акти виконаних робіт, план БТІ), аналіз конструктивних елементів, типу стикування з землею, наявності бетонної основи або підпірних елементів. [3]

Застосування георадарного зондування GPR – Ground Penetrating Radar) це дозволяє без розкопок визначити наявність та глибину залягання фундаменту, його контури, щільність та порушення структури. Використовується портативний георадар типу ОКО–2, StructureScan, SIR–3000. Його похибка становить 5–10 см., а перевага в тому, що не пошкоджує об’єкт та дає швидкий результат.

Штучний інтелект (ШІ): Перспективним є використання нейронних мереж для аналізу великих масивів даних: порівняння супутникових знімків різних часових періодів, аналіз BIM–моделей на відповідність фактичному стану та автоматичне виявлення невідповідностей у технічній документації.

Суть BIM–технологій полягає у розробленні та спільному використанні будівельної інформаційної моделі об’єкта будівництва, що представляє собою набір структурованих і неструктурованих інформаційних контейнерів у рамках цілісної інформаційної системи, що містять необхідні геометричні, фізичні, функціональні та інші характеристики об’єкта, на основі яких розробляється документація, що супроводжує життєвий цикл об’єкта (проектна та кошторисна документація, рекомендації щодо експлуатації). [2]

Шурфування – найбільш достовірний метод встановлення типу і глибини фундаменту. Це ручне або механізоване розкриття ґрунту вздовж зовнішньої стіни споруди з метою візуального виявлення фундаменту, його матеріалу, глибини залягання та стану.

Шурфування є рекомендованим методом у разі, коли доступ до проектної документації відсутній, або коли фактична конструкція може не відповідати технічному паспорту об’єкта. У більшості випадків, саме шурфування дає

можливість експерту достовірно визначити, чи має об'єкт фундамент, чи він встановлений, наприклад, на тимчасових опорах покладених на ґрунт без заглиблення, що не дають підстав для визнання об'єкта нерухомим майном.

Таким чином, проведення технічного обстеження із можливістю шурфування є необхідною передумовою для підготовки якісного висновку судового експерта у справах, що стосуються правового статусу об'єкта. Недостатня перевірка фундаменту може призвести до неправильного висновку, що вплине на права власності, реєстрацію об'єкта або правомірність його демонтажу.

У контексті цифрової трансформації судово–експертної діяльності все частіше застосовуються цифрові іноваційні джерела даних: геоінформаційні системи, електронні кадастрові карти, знімки з дронів і супутників, BIM–моделі, електронні технічні паспорти тощо. [8; 7]. Їх використання суттєво підвищує оперативність, охоплення та деталізацію аналізу об'єктів нерухомості.

Однак, незважаючи на переваги, цифрові джерела не можуть на 100% замінити класичні методи дослідження, особливо коли йдеться про доказову базу у судовому процесі. [7; 5].

Виходячи з цього можемо сказати, що рекомендований підхід це – комбінований аналіз. Шурфування залишається критично важливим методом верифікації, оскільки воно забезпечує матеріальний зв'язок експертного висновку з дійсністю, тоді як ШІ та цифрові інновації виконують роль аналітичного інструментарію. Найбільш надійним є підхід, за якого цифрові джерела використовуються як допоміжний інструмент, а не основний доказ.

Таким чином, майбутнє судово–будівельної експертизи полягає у комбінованому підході. Штучний інтелект та цифрові технології є потужними допоміжними інструментами, які значно покращують точність та зручність проведення експертизи, але не можуть повністю замінити фізичну перевірку та класичні методи дослідження, особливо коли йдеться про складні чи спірні об'єкти. Впровадження цифрових інновацій має супроводжуватися розробкою чітких протоколів їх використання, що забезпечить відповідність доказів європейським вимогам.

Перелік використаних джерел:

1. Цивільний кодекс України : Закон України від 16 січня 2003 р. № 435–IV. URL: https://zakon.rada.gov.ua/laws/show/435–15

2. Про схвалення Концепції впровадження технологій будівельного інформаційного моделювання (BIM–технологій) в Україні та затвердження плану заходів з її реалізації : Розпорядження Кабінету Міністрів України від 17.02.2021 № 152–р // База даних «Законодавство України» / Верховна Рада України. URL: Законодавство України

3. ДСТУ 9273:2024. Настанова щодо обстеження будівель і споруд для визначення та оцінювання їхнього технічного стану. – Київ : Мінрегіон України, 2024.

4. ДБН В.2.1–10:2009. Основи та фундаменти споруд. – Київ : Мінрегіонбуд України, 2009.

5. Методичні рекомендації з питань проведення будівельно–технічної експертизи : затв. наказом Міністерства юстиції України від 08 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/rada/show/v0053323–98

6. Діджиталізація судово–експертної науки в умовах воєнного стану : збірник матеріалів Міжнародної науково–практичної конференції (м. Харків, 08.11.2024). – Харків : ННЦ «ІСЕ ім. Засл. Проф. М. С. Бокаріуса», 2024. –439 с. URL: https://drive.google.com/file/d/1cDRJ14KDOGIXe5Y6HdNVBzqAS7gbR–ML/view

7. Ковальчук В. С. Доказове значення цифрових матеріалів у судовому процесі: проблеми допустимості // Право України. – 2022. – № 11. С. 68–76.

8. Примак І. І., Іванченко О. Г. Цифрова трансформація у сфері технічної інвентаризації нерухомості // Технічні науки та технології. – 2023. – № 4. – С. 120–127.

DOI https://doi.org/10.32837/11300.33532

Головач Ростислав
судовий експерт Київського науково–дослідного інституту судових експертиз
Міністерства юстиції України,
м. Київ, Україна
ORCID: https://orcid.org/0009–0004–7902–7560
e–mail: vekvnnc@gmail.com

Шереметов Сергій
завідувач лабораторії військових досліджень
Київського науково–дослідного інституту судових експертиз
Міністерства юстиції України,
м. Київ, Україна
ORCID: https://orcid.org/0009–0003–3381–5003
e–mail: s.sheremetov60@gmail.com

ЦИФРОВІ НОСІЇ ІНФОРМАЦІЇ ЯК ОБ'ЄКТИ СУДОВОЇ ВІЙСЬКОВОЇ ЕКСПЕРТИЗИ: ПРОБЛЕМИ МЕТОДОЛОГІЇ ТА НОРМАТИВНОГО РЕГУЛЮВАННЯ

У тезах розглянуто актуальні питання необхідності оновлення науково–методичних рекомендацій з військової експертизи в контексті цифрових викликів. Акцентовано увагу на важливості визначення предмета та об'єктів експертизи для дослідження злочинів у кіберпросторі та операцій з віртуальними активами.

Ключові слова: судова військова експертиза, кіберпростір, віртуальні активи, управлінські документи, інформаційна безпека.

Holovach Rostislav
Forensic Military Expert, Military Research Laboratory
Kyiv Scientific Research Institute of Forensic Expertise
of the Ministry of Justice of Ukraine,
Kyiv, Ukraine

Sheremetov Serhii
Head of the Military Research Laboratory
Kyiv Scientific Research Institute of Forensic Expertise
of the Ministry of Justice of Ukraine,
Kyiv, Ukraine

DIGITAL DATA MEDIA AS OBJECTS OF FORENSIC MILITARY EXPERT EXAMINATION: METHODOLOGICAL AND REGULATORY ISSUES

The theses examine current issues related to the need to update the scientific and methodological recommendations for military forensic examination in the context of digital challenges. Particular attention is paid to the importance of defining the subject matter and objects of examination for the investigation of cybercrime and transactions involving virtual assets.

Keywords: forensic military examination, cyberspace, virtual assets, administrative documents, information security.

Забезпечення інформаційної безпеки держави відповідно до Конституції України є однією з найважливіших функцій держави. [1, ст. 17] В умовах стрімкої цифровізації військової сфери, розвитку інформаційно–комунікаційних технологій та появи нових загроз у кіберпросторі судова військова експертиза потребує системного вдосконалення методологічних підходів до дослідження діяльності військових формувань і військових службових (посадових) осіб.

Сучасний розвиток сектору безпеки і оборони України супроводжується активним впровадженням електронного документообігу, автоматизованих систем управління, цифрових платформ обліку та інформаційно–комунікаційних систем у діяльність військових формувань. Одночасно зростає кількість кримінальних проваджень, у межах яких виникає необхідність дослідження діяльності військових службових (посадових) осіб в умовах використання цифрових засобів управління, передачі інформації, планування, логістики та обліку ресурсів.

За таких умов чинні Науково–методичні рекомендації з питань підготовки та призначення судових експертиз [2, p. VIII] потребують адаптації до сучасних викликів, зокрема у частині визначення предмета, об’єктів та основних завдань судової військової експертизи. Особливого значення набуває дослідження цифрових носіїв інформації, електронних управлінських документів, автоматизованих систем військового управління, інформаційно–телекомунікаційних систем та інших електронних джерел доказової інформації у кримінальному провадженні.

Чинна редакція розділу VIII «Військова експертиза» Науково–методичних рекомендацій не містить нормативно визначених положень щодо предмета та об’єктів судової військової експертизи, що створює ризики неоднакового підходу до визначення меж компетенції експерта, формування об’єктів дослідження та оцінки цифрової доказової інформації.

Предмет судової військової експертизи в умовах цифровізації процесів військового управління охоплює сукупність фактів та обставин щодо діяльності військових службових (посадових) осіб, пов’язаної з прийняттям управлінських рішень, організацією застосування сил і засобів, використанням інформаційних систем, цифрових ресурсів та електронних засобів обміну інформацією. Це дозволяє встановлювати відповідність дій або бездіяльності посадових осіб

вимогам нормативно–правових і керівних документів, а також оцінювати обґрунтованість прийнятих рішень та їх наслідки.

Ключовим аспектом є належне визначення об'єктів судової військової експертизи. В умовах цифровізації військового управління значна частина управлінських рішень, службових комунікацій, планувальних документів, логістичних операцій та облікових процедур фіксується в електронній формі. Такі відомості можуть міститися в автоматизованих системах управління, електронних журналах обліку, інформаційно–телекомунікаційних системах, електронному листуванні, базах даних, геоінформаційних сервісах та інших цифрових середовищах.

Об'єктами судової військової експертизи є матеріальні та матеріалізовані носії інформації, зокрема управлінські документи, що фіксують відомості про підготовку, ведення бойових дій, перегрупування та дислокацію військ, рух ресурсів, матеріальних цінностей, коштів, організацію управління, планування та виконання завдань. У сучасних умовах до таких об'єктів можуть належати також цифрові записи щодо використання електронних платіжних систем, електронного обліку ресурсів та операцій із віртуальними активами, якщо вони мають значення для встановлення обставин кримінального провадження.

Управлінські документи (організаційно–розпорядчі, фінансові, планові, облікові тощо) є повноцінними об'єктами дослідження судової військової експертизи, оскільки містять зафіксовані факти реалізації функцій військового управління та розпорядження ресурсами. Їх дослідження з позиції відповідності статутам, наказам, директивам та іншим нормативно–правовим актам дає змогу встановлювати причинні зв'язки між діями або бездіяльністю військових службових (посадових) осіб і наслідками, що настали.

Відсутність належного методологічного визначення статусу цифрових даних та електронних документів як об'єктів дослідження судової військової експертизи ускладнює їх використання під час проведення експертних досліджень та може негативно впливати на повноту, обґрунтованість і процесуальну допустимість експертних висновків.

Таким чином, удосконалення науково–методичної бази судової військової експертизи, зокрема конкретизація її предмета, об'єктів дослідження та орієнтовного переліку питань, сприятиме підвищенню правової визначеності, наукової обґрунтованості та ефективності експертного забезпечення кримінальних проваджень, пов'язаних із використанням цифрових технологій, інформаційних систем та електронних доказів.

Удосконалення методологічних засад судової військової експертизи в умовах цифровізації процесів військового управління є необхідною умовою забезпечення належного експертного супроводу кримінальних проваджень, пов'язаних із діяльністю військових формувань, використанням інформаційних технологій та сучасних цифрових засобів управління.

Подальший розвиток методичного забезпечення судової військової експертизи має здійснюватися з урахуванням сучасних кіберзагроз, цифрової трансформації сектору безпеки і оборони та розширення використання електронних доказів у кримінальному провадженні.

Перелік використаних джерел:

1. Конституція України : Конституція України; Верховна Рада України від 28.06.1996 № 254к/96–ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96–%D0%B2%D1%80. (ст. 17)

2. Про затвердження Науково–методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України; Інструкція, Форма типового документа, Картка, Рекомендації від 08.10.1998 № 53/5 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0705–98. (p. VIII)

3. Інформаційний лист міжнародної науково–практичної конференції «Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози». Одеса, 2026.

DOI https://doi.org/10.32837/11300.33615

Grecu Polixenia
Expert, Legal Adviser, Department of Legal and Administrative Sciences,
Faculty of Legal and Administrative Sciences,
Spiru Haret University,
Bucharest, Romania
ORCID: https://orcid.org/0009–0003–5075–2374
Adresa electronică: polixenia.grecu@spiruharet.ro

CORELAREA DATELOR MEDICO–LEGALE ŞI A REZULTATELOR EXPERTIZEI BALISTICE ÎN RECONSTITUIREA MECANISMULUI MORŢILOR PRIN ÎMPUŞCARE

Investigarea morților produse prin arme de foc presupune utilizarea unor metode complexe de analiză, bazate pe colaborarea dintre specialiștii din domeniul medicinei legale și al criminalisticii. Stabilirea cu exactitate a împrejurărilor în care s–a produs împușcarea, a poziției victimei și a trăgătorului, a distanței și direcției de tragere, precum și a tipului de armă utilizat necesită coroborarea informațiilor obținute prin autopsia medico–legală cu rezultatele expertizei balistice judiciare.

Prezentul studiu evidențiază importanța abordării interdisciplinare în investigarea morților prin împușcare și analizează principalele categorii de date medico–legale și balistice utilizate în procesul de reconstituire a mecanismului producerii decesului. Sunt examinate aspecte referitoare la caracteristicile leziunilor produse prin arme de foc, identificarea orificiilor de intrare și ieșire, determinarea distanței de tragere, analiza traiectoriei proiectilului și stabilirea relației dintre constatările medico–legale și caracteristicile tehnice ale armei și muniției utilizate.

Totodată, sunt evidențiate situațiile în care interpretarea izolată a datelor poate conduce la concluzii eronate și este subliniată necesitatea evaluării integrate a tuturor elementelor probatorii.

Cuvinte cheie: expertiză balistică, arme de foc, moarte prin împușcare, traiectoria proiectilului, distanța de tragere.

Grecu Polixenia
Expert, Legal Adviser, Department of Legal and Administrative Sciences,
Faculty of Legal and Administrative Sciences,
Spiru Haret University,
Bucharest, Romania

CORRELATION OF FORENSIC MEDICAL FINDINGS AND BALLISTIC EXPERTISE RESULTS IN RECONSTRUCTING THE MECHANISM OF FIREARM DEATHS

Expert, Legal Adviser, Department of Legal and Administrative Sciences, Faculty of Legal and Administrative Sciences, Spiru Haret University, Bucharest, Romania

The investigation of firearm–related deaths requires the use of complex analytical methods based on close cooperation between specialists in forensic medicine and criminalistics. Establishing the exact circumstances of a shooting incident, including the position of the victim and the shooter, the firing distance and direction, as well as the type of firearm used, requires the correlation of information obtained through forensic autopsy with the results of forensic ballistic examinations.

This study highlights the importance of an interdisciplinary approach in the investigation of firearm deaths and analyzes the main categories of forensic medical and ballistic data used in reconstructing the mechanism of death. Particular attention is given to the characteristics of firearm injuries, the identification of entrance and exit wounds, the determination of firing distance, projectile trajectory analysis, and the relationship between forensic findings and the technical characteristics of the firearm and ammunition involved.

The paper also emphasizes situations in which the isolated interpretation of evidence may lead to erroneous conclusions and underlines the necessity of an integrated assessment of all evidentiary elements.

Keywords: ballistic expertise, firearms, death by shooting, projectile trajectory, firing distance.

1. Introducere

Moartea produsă prin utilizarea armelor de foc reprezintă una dintre cele mai complexe categorii de cazuri investigate de organele judiciare, atât prin gravitatea consecințelor sale, cât și prin multitudinea problemelor de ordin tehnic, criminalistic și medico–legal pe care le ridică. Stabilirea împrejurărilor exacte în care s–a produs împușcarea presupune o analiză riguroasă a tuturor elementelor de fapt și de probă, în vederea reconstituirii mecanismului producerii decesului și a identificării persoanelor implicate.

Particularitatea acestor cauze constă în faptul că informațiile relevante sunt furnizate de surse diferite, care trebuie analizate și interpretate în mod coroborat [1, p. 56]. Astfel, datele rezultate din examinarea medico–legală a victimei oferă informații referitoare la natura și caracteristicile leziunilor, direcția de acțiune a proiectilului, distanța probabilă de tragere și mecanismul producerii morții, în timp ce expertiza balistică permite identificarea armei utilizate, analiza muniției, stabilirea traiectoriei proiectilului și evaluarea circumstanțelor tehnice ale împușcării [2, p.24].

În practica judiciară, nici constatările medico–legale și nici concluziile expertizei balistice nu pot fi analizate izolat. Interpretarea separată a acestora poate conduce la concluzii incomplete sau chiar eronate, în special în situațiile în care locul faptei a fost modificat, când există mai multe focuri de armă sau când împrejurările producerii decesului sunt controversate. Din acest motiv, reconstituirea mecanismului morților prin împușcare impune o abordare interdisciplinară, bazată pe integrarea informațiilor

provenite din cercetarea la fața locului, autopsia medico–legală, expertiza balistică și celelalte mijloace de probă administrate în cauză.

Progresele înregistrate în domeniul balisticii judiciare și al medicinei legale au contribuit semnificativ la creșterea gradului de acuratețe a investigațiilor.

2. Contribuția examinării medico–legale la stabilirea mecanismului împușcării

Examinarea medico–legală ocupă un rol central în investigarea morților produse prin arme de foc, întrucât oferă informații esențiale privind mecanismul producerii leziunilor, cauza medicală a decesului și împrejurările în care s–a produs împușcarea. Datele obținute prin examinarea externă și internă a cadavrului constituie un reper fundamental pentru interpretarea celorlalte mijloace de probă și pentru verificarea ipotezelor formulate pe parcursul anchetei [3, p.72].

În cadrul autopsiei medico–legale, una dintre primele preocupări ale expertului este identificarea și descrierea leziunilor produse prin arme de foc. O importanță deosebită o prezintă diferențierea între orificiul de intrare și orificiul de ieșire al proiectilului, deoarece această operațiune permite stabilirea direcției generale de deplasare a glonțului prin corpul victimei. Caracteristicile morfologice ale celor două tipuri de orificii, precum dimensiunile, forma, marginile sau modificările tisulare asociate, oferă informații valoroase pentru reconstituirea traiectului proiectilului.

Determinarea distanței de tragere reprezintă un alt obiectiv important al examinării medico–legale. În funcție de distanța dintre gura țevii și corpul victimei, pot fi identificate elemente specifice, precum urmele de afumare, tatuajul produs de pulberea nearsă, arsuri tegumentare sau efectele gazelor rezultate în urma împușcării. Prezența ori absența acestor modificări permite formularea unor concluzii privind executarea focului cu contact, de la mică distanță, de la distanță intermediară sau de la distanță mare.

De asemenea, analiza traiectului proiectilului în organism furnizează informații importante privind poziția victimei în momentul producerii împușcării.

Corelarea direcției traiectului cu leziunile constatate și cu datele obținute prin cercetarea la fața locului poate contribui la stabilirea poziției relative dintre victimă și trăgător. În numeroase situații, aceste aspecte devin esențiale pentru diferențierea unui omor de un suicid sau de un accident.

Examinarea medico–legală permite și identificarea eventualelor leziuni asociate, produse anterior sau ulterior împușcării. Prezența unor leziuni de apărare, a semnelor de luptă ori a altor traumatisme poate indica existența unei agresiuni și poate modifica semnificativ interpretarea circumstanțelor producerii decesului. Totodată, evaluarea caracterului vital al leziunilor contribuie la stabilirea succesiunii evenimentelor și la aprecierea contribuției fiecărei leziuni la producerea morții [4, p.37].

Prin urmare, autopsia medico–legală nu reprezintă doar o activitate de constatare a cauzei medicale a decesului, ci un proces complex de analiză și interpretare a leziunilor, capabil să furnizeze informații indispensabile pentru reconstituirea mecanismului împușcării.

3. Concluzii

Datele medico–legale rezultate din examinarea cadavrului și din efectuarea autopsiei oferă informații esențiale privind cauza și mecanismul morții, caracteristicile leziunilor produse prin arme de foc, direcția de pătrundere a proiectilului și distanța probabilă de tragere. În același timp, expertiza balistică permite identificarea armei utilizate, analiza muniției, stabilirea traiectoriei proiectilului și evaluarea condițiilor tehnice în care s–a produs împușcarea. Fiecare dintre aceste categorii de informații prezintă o valoare probatorie deosebită, însă relevanța lor maximă este atinsă numai prin interpretarea coroborată a rezultatelor obținute.

Analiza integrată a constatărilor medico–legale și a concluziilor expertizei balistice contribuie în mod direct la reconstituirea mecanismului producerii împușcării, la stabilirea poziției victimei și a trăgătorului, la determinarea circumstanțelor producerii evenimentului și la diferențierea situațiilor de omor, suicid sau accident.

Evoluția tehnologiilor utilizate atât în medicina legală, cât și în balistica judiciară a determinat creșterea semnificativă a posibilităților de analiză și interpretare a probelor.

Lista Sursei Utilizate:

1. DiMaio, V. J. M., DiMaio, D., Patologie medico–legală, ediția a II–a, CRC Press, B oca Raton, 2001, 592 p.

2. Pătru, Alina Daniela, Criminalistică, Editura Sitech, Craiova, 2024, 207 p.

3. Pătru, Alina Daniela, Scenele violenței. Analiza urmelor și reconstituirea faptelor, Editura Sitech, Craiova, 2025, 232 p.

4. Pătru, Alina Daniela, Urmele de sânge. Identificare, tipare și relevanță judiciară, Editura Sitech, Craiova, 2025, 214 p.

DOI https://doi.org/10.32837/11300.33533

Кривоножко Ганна
кандидат технічних наук, старший науковий співробітник, головний судовий експерт, Київське відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України,
м. Київ, Україна,
ORCID: https://orcid.org/0000–0002–7635–541X,
e–mail: krgalina76@gmail.com

Собін Олексій
судовий експерт, Науково–дослідний центр судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України, м. Київ, Україна,
ORCID: https://orcid.org/0000–0003–4653–5986,
e–mail: aksobin@yahoo.com

ШТУЧНИЙ ІНТЕЛЕКТ І СПЕЦІАЛІЗОВАНІ ЦИФРОВІ ІНСТРУМЕНТИ В ЕКСПЕРТНОМУ ЗАБЕЗПЕЧЕННІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ТА ЦИФРОВИХ ПРАВОПОРУШЕНЬ

Анотація: Обґрунтовано модель використання ШІ та forensic–ПЗ: автоматизований пошук є лише орієнтацією, а висновок формує експерт після перевірки.

Ключові слова: ШІ, цифрові докази, кіберзлочини, forensic–ПЗ.

Kryvonozhko Halyna
Candidate of Technical Sciences, Senior Researcher, Chief Forensic Expert, Kyiv Branch of the National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute» of the Ministry of Justice of Ukraine,
Kyiv, Ukraine

Sobin Oleksii
Forensic Expert, Research Center for Forensic Examination in the Field of Information Technologies and Intellectual Property of the Ministry of Justice of Ukraine,
Kyiv, Ukraine

ARTIFICIAL INTELLIGENCE AND SPECIALIZED DIGITAL TOOLS IN EXPERT SUPPORT FOR THE INVESTIGATION OF CYBERCRIMES AND DIGITAL OFFENCES

Abstract: The thesis outlines a model for using AI and forensic software in digital examinations: automated search is preliminary, while the expert conclusion is made after verification.

Key words: AI, digital evidence, cybercrime, forensic software.

Постановка проблеми. Сучасна криміналістика та судова експертиза працюють у середовищі, де значна частина злочинної активності має цифровий вимір. Навіть коли подія відбувається у фізичному просторі, її підготовка, координація, фінансування або приховування можуть залишати цифрові сліди: листування, журнали доступу, платіжні операції, геолокаційні дані, медіафайли, хмарну синхронізацію, телеметрію БПЛА, блокчейн–транзакції, серверні логи та інші технічні артефакти.

Актуальність теми. Кіберзлочинність уже не зводиться до несанкціонованого доступу до комп'ютерної системи. Вона формує ширшу цифрову злочинну екосистему, у якій поєднуються фішинг, онлайн–шахрайство, атаки програм–вимагачів (ransomware), ботоферми, нелегальні цифрові сервіси, криптовалютні перекази, синтетичний deepfake–контент, автоматизовані акаунти, хмарні ресурси та засоби приховування мережевої активності. Звіти Europol фіксують посилення таких загроз через шифрування, проксі–інфраструктури та інструменти штучного інтелекту [5].

Нормативно–методична основа. Цифрові матеріали у кримінальному провадженні можуть набувати значення документів, речових доказів, додатків до протоколів, об'єктів експертизи або інших матеріалів, що містять відомості про обставини події. КПК України відносить до документів, зокрема, інші носії інформації, у тому числі комп'ютерні дані [1]. Закон України «Про судову експертизу» визначає експертизу як дослідження на основі спеціальних знань [2], а Інструкція № 53/5 передбачає застосування експертами методів, методик, стандартів, довідкової літератури та програмних продуктів [3]. Отже, програмний засіб або ШІ–модуль не замінює експерта, а є інструментом реалізації спеціальних знань.

Мета. Визначення місця штучного інтелекту та спеціалізованих цифрових інструментів у системі експертного забезпечення розслідування кіберзлочинів і цифрових правопорушень, а також формування моделі, за якої автоматизований пошук, класифікація та групування даних не підміняють висновок судового експерта, а лише створюють контрольований аналітичний шар для подальшої перевірки.

Цифровий доказ як частина екосистеми. У практичному експертному розумінні цифровий доказ – це не тільки файл, повідомлення або фотографія. Це може бути координата, часова мітка, запис у базі даних, транзакція, технічний стан пристрою, журнал підключення, мережевий запит, метадані зображення, запис камери, телеметрія БПЛА або лог хмарної синхронізації. Тому цифрову експертизу доцільно розглядати як роботу з екосистемою, а не з одиничним

файлом. Експерт має встановити джерело даних, спосіб їх отримання, цілісність, можливість повторення процедури, часові й технічні обмеження, а також зв'язок цифрового об'єкта з іншими даними.

Інструментальна основа дослідження. Спеціалізоване forensic–ПЗ забезпечує доступ до цифрових даних, криміналістичне копіювання, хешування, індексацію, декодування, фільтрацію, пошук, побудову часових ліній, аналіз логів, файлових систем, баз даних, мобільних пристроїв, хмарних джерел і формування технічних звітів. Будь–яке використання цифрових інструментів має бути описане так, щоб інший експерт міг перевірити вихідні дані, параметри обробки та логіку отриманого результату [3].

ШІ як допоміжний аналітичний шар. ШІ у цифровій експертизі доцільно розглядати як допоміжний аналітичний шар над первинними даними і спеціалізованим forensic–ПЗ. Його функціями можуть бути попередній пошук, OCR–розпізнавання тексту, speech–to–text, класифікація зображень, пошук схожих об'єктів, групування повідомлень, виявлення аномалій, побудова графів зв'язків і формування робочих гіпотез. Якщо система позначила об'єкт як релевантний або вказала на аномалію, це є лише сигналом для експертної перевірки.

Український інституційний контекст. Значення цієї проблематики підтверджується проведенням 29 серпня 2025 року в Одесі міждисциплінарної науково–практичної конференції «Цифрова ера розвитку судової експертизи», організованої Одеським науково–дослідним інститутом судових експертиз Міністерства юстиції України. У межах заходу було акцентовано на цифровій трансформації судово–експертної діяльності, впровадженні інноваційних технологій і ШІ, підвищенні об'єктивності та достовірності результатів експертиз, а також на тому, що остаточний висновок має залишатися за людиною–експертом. Окремо заступник Міністра юстиції України А. Гайченко визначив стратегічне впровадження ШІ в судово–експертну діяльність як напрям, що потребує практичних кейсів, оцінки результатів і подальшого методичного розвитку [4].

Кіберпростір і віртуальні активи. Експертне забезпечення розслідування злочинів у кіберпросторі дедалі частіше охоплює серверну інфраструктуру, хмарні ресурси, доменні ідентифікатори, мережеві журнали, криптовалютні гаманці, біржові акаунти, блокчейн–транзакції, транзакційні графи та позаланцюгові (off–chain) дані. FATF наголошує на ризик–орієнтованому підході до віртуальних активів і постачальників відповідних послуг [6]. Для експерта це означає, що блокчейн–адреса, транзакція або транзакційний граф не доводять особу власника без додаткових off–chain–даних і процесуального контексту.

Воєнний і defense–контекст. В умовах воєнного стану коло цифрових об'єктів розширюється за рахунок БПЛА, наземних роботизованих платформ, морських дронів, систем відеоспостереження, засобів радіоелектронної боротьби, OSINT–джерел, супутникових знімків, телеметрії та бойових журналів. 2U Tech Forum 2026 окремо виділяє інновації, народжені на полі бою, і вплив українського

бойового досвіду на еволюцію стандартів [7]. Для експертної практики це означає потребу не лише у впровадженні технологій, а й у здатності фіксувати, зберігати, досліджувати та пояснювати цифрові сліди їх використання у правосудді.

Типові ризики. Найнебезпечнішим методичним ризиком є сприйняття ШІ або спеціалізованого ПЗ як «чарівної кнопки», що автоматично створює доказ. У судово–експертному дослідженні такої кнопки не існує. Є первинний цифровий об’єкт, спосіб його отримання, процедура збереження, інструментальна обробка, аналітичне сортування, експертна перевірка і лише після цього – обґрунтований висновок. До основних ризиків належать хибна позитивна класифікація, неповнота індексації, непрозорість алгоритму, передача даних до неконтрольованих хмарних сервісів і автоматична атрибуція особи за одним цифровим слідом.

Запропонована модель. Доцільною є контрольована людино–машинна модель: надходження об’єкта і визначення меж доручення; збереження та криміналістичне копіювання; індексація і первинний аналіз; ШІ–попередня аналітика; експертна перевірка відібраних об’єктів за первинними файлами, метаданими, логами, хешами, часовими зонами і контекстом; перехресна верифікація іншим модулем або іншим програмним засобом; hostile review як критична перевірка альтернативних пояснень; складання письмового висновку з чітким відокремленням факту, висновку і припущення.

Висновки. ШІ та спеціалізовані цифрові інструменти є необхідною частиною сучасного експертного забезпечення розслідування кіберзлочинів і цифрових правопорушень. Вони дозволяють опрацьовувати великі масиви даних, виявляти потенційно релевантні об’єкти, структурувати цифрові екосистеми та зменшувати ризик пропуску важливих артефактів. Водночас автоматизований результат не є самостійним експертним висновком. Його доказове значення виникає лише після перевірки за первинними цифровими об’єктами, документування процедури, перехресної верифікації та методичної оцінки судовим експертом.

Перелік використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651–VI. URL: https://zakon.rada.gov.ua/laws/show/4651–17

2. Про судову експертизу : Закон України від 25.02.1994 № 4038–XII. URL: https://zakon.rada.gov.ua/laws/show/4038–12

3. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/go/z0705–98

4. Науково–практична конференція «Цифрова ера розвитку судової експертизи» в Одесі. ОНДІСЕ Міністерства юстиції України. 29.08.2025. URL: https://ondise.minjust.gov.ua/naukovo–praktichna–konferenciya–cifrova–era–rozvitku–sudovo%D1%97–ekspertizi–v–odesi/

5. Europol. The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. IOCTA 2026. Luxembourg : Publications Office of the European Union, 2026. DOI: 10.2813/5737847.

6. FATF. Updated Guidance for a Risk–Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris : FATF, 2021. URL: https://www.fatf–gafi.org/en/publications/Fatfrecommendations/Guidance–rba–virtual–assets–2021.html

7. 2U Tech Forum 2026. Програма. URL: https://2utechforum.com/programa

DOI https://doi.org/10.32837/11300.33534

Ляховецький Сергій
аспірант кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
м.Одеса, Україна
ORCID: https://orcid.org/0009–0001–5162–0336
e–mail: 17721772q@gmail.com

ІНСЦЕНУВАННЯ САМОГУБСТВА ЧЕРЕЗ ПОВІШАННЯ ДЛЯ ПРИХОВУВАННЯ УМИСНОГО ВБИВСТВА ТА МОЖЛИВОСТІ АНАЛІТИЧНОЇ ПІДТРИМКИ ШТУЧНОГО ІНТЕЛЕКТУ

У тезах досліджуються криміналістичні особливості інсценування самогубства через повішання як способу приховування умисного вбивства.

На підставі аналізу положень Кримінально процесуального кодексу України та судово–слідчої практики розглядаються характерні ознаки інсценування, особливості огляду місця події, роль судово–медичної експертизи та взаємодія слідчого, прокурора, криміналіста, експерта й оперативних підрозділів під час досудового розслідування. Особлива увага приділяється можливостям використання аналітичної підтримки штучного інтелекту для аналізу обставин події, цифрових слідів, попередньої поведінки потерпілого, його психологічного стану, соціальних зв’язків та взаємовідносин із близьким оточенням.

Обґрунтовується значення комплексного криміналістичного підходу та сучасних інформаційно–аналітичних технологій для виявлення умисних вбивств, замаскованих під самогубство.

Ключові слова: інсценування самогубства, повішання, умисне вбивство, криміналістика, судово–медична експертиза, досудове розслідування, штучний інтелект, судово–слідча практика, Кримінально процесуального кодексу України.

Liakhovetskyi Serhii
Postgraduate Student of the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

STAGING SUICIDE BY HANGING TO CONCEAL INTENTIONAL HOMICIDE AND THE POSSIBILITIES OF ANALYTICAL SUPPORT BY ARTIFICIAL INTELLIGENCE

The theses examine the criminalistic features of staging suicide by hanging as a method of concealing intentional homicide.

Based on the analysis of the provisions of the Criminal Procedure Code of Ukraine and judicial–investigative practice, the paper considers the characteristic signs of

staging, the specific features of crime scene examination, the role of forensic medical examination, and the interaction between the investigator, prosecutor, criminalist, expert, and operational units during pre–trial investigation. Particular attention is paid to the possibilities of using analytical support by artificial intelligence for analyzing the circumstances of the event, digital traces, the victim's previous behavior, psychological state, social connections, and relationships with close surroundings.

The importance of a comprehensive criminalistic approach and modern information–analytical technologies for detecting intentional homicides disguised as suicide is substantiated.

Keywords: staging of suicide, hanging, intentional homicide, criminalistics, forensic medical examination, pre–trial investigation, artificial intelligence, judicial–investigative practice, Criminal Procedure Code of Ukraine.

Сучасна судово–слідча практика свідчить, що одним із найбільш складних видів приховування умисного вбивства є інсценування самогубства через повішання. Такі кримінальні правопорушення характеризуються високим рівнем підготовки злочинця, намаганням приховати справжній механізм смерті та створити уявлення про добровільне позбавлення потерпілим власного життя. У зв'язку з цим особливого значення набувають криміналістичний аналіз обстановки місця події, належна взаємодія між слідчим, прокурором, криміналістом, судово–медичним експертом та оперативними підрозділами, а також використання сучасних аналітичних технологій, включаючи штучний інтелект.

Відповідно до ст. 2 Кримінально процесуального кодексу України завданнями кримінального провадження є забезпечення швидкого, повного та неупередженого розслідування кримінальних правопорушень. При розслідуванні випадків смерті з ознаками повішання першочергового значення набуває перевірка версії про можливе інсценування самогубства.

Судово–слідча практика свідчить, що злочинці нерідко намагаються змінити обстановку місця події, перемістити тіло потерпілого, створити штучні сліди самогубства, підготувати передсмертні записки або інші елементи, спрямовані на введення слідства в оману. Саме тому вже на початковому етапі досудового розслідування особливе значення має діяльність слідчо–оперативної групи та участь судово–медичного експерта під час огляду місця події відповідно до ст. 237 Кримінально процесуального кодексу України.

До найбільш характерних криміналістичних ознак можливого інсценування самогубства через повішання належать:

- невідповідність положення тіла механізму утворення слідів; відсутність типових ознак самостійного повішання;
- суперечності між характером странгуляційної борозни та способом підвішування;

- наявність тілесних ушкоджень, не характерних для самогубства; сліди боротьби в приміщенні;
- неприродне розташування предметів обстановки;
- ознаки переміщення тіла;
- невідповідність вузла, висоти опори або способу кріплення фізичним можливостям потерпілого;
- відсутність психологічних або соціальних передумов до самогубства;
- суперечності між показаннями близьких осіб та фактичними обставинами події.

Важливу роль у встановленні істинного механізму смерті відіграє судово–медична експертиза. Взаємодія слідчого із судово–медичним експертом дозволяє своєчасно виявити ознаки механічної асфіксії, прижиттєвість странгуляційної борозни, інші тілесні ушкодження та можливі ознаки насильницької смерті, що передувала підвішуванню тіла.

Особливого значення у сучасних умовах набуває використання аналітичної підтримки штучного інтелекту під час розслідування таких кримінальних правопорушень. На початковому етапі досудового розслідування системи штучного інтелекту можуть використовуватись для аналізу відеозаписів з камер спостереження, цифрових слідів, телефонних з'єднань, геолокаційних даних та часової послідовності подій.

Окрему увагу доцільно приділяти аналізу попередньої поведінки потерпілого, його способу життя, стану здоров'я, психологічного стану, взаємовідносин із родичами, знайомими, колегами та іншими особами з близького оточення.

Системи аналітичної підтримки можуть допомагати у виявленні конфліктних відносин, погроз, фінансових суперечок, випадків домашнього насильства або інших факторів, які можуть свідчити про насильницький характер смерті.

На подальшій стадії розслідування технології штучного інтелекту можуть застосовуватись для:

- аналітичного зіставлення показань свідків;
- побудови часових моделей події;
- виявлення суперечностей у доказовій інформації; аналізу цифрової активності потерпілого та підозрюваних;
- систематизації висновків експертиз та матеріалів кримінального провадження.

Важливе значення має також алгоритмізація взаємодії між слідчим, прокурором, оперативними працівниками та експертами.

Судово–слідча практика підтверджує, що своєчасне висунення версії про інсценування самогубства, належна фіксація слідів та комплексне використання спеціальних знань значно підвищують ефективність викриття умисних вбивств, замаскованих під самогубство.

Таким чином, інсценування самогубства через повішання є складним способом приховування умисного вбивства, що потребує комплексного криміналістичного підходу, тісної взаємодії суб'єктів досудового розслідування та використання сучасних інформаційно–аналітичних технологій. Впровадження систем аналітичної підтримки штучного інтелекту створює нові можливості для встановлення об'єктивної істини у кримінальному провадженні та підвищення ефективності розслідування насильницьких злочинів.

Перелік використаних джерел:

1.Кримінальний процесуальний кодекс України // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651–17.

2.Про судову експертизу : Закон України // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4038–12.

DOI https://doi.org/10.32837/11300.33618

Pătru Alina Daniela
Conferențiar universitar doctor,
Departamentul de Științe Juridice și Științe Administrative,
Facultatea de Științe Juridice și Științe Administrative,
Universitatea Spiru Haret,
București, Romania
ORCID: https://orcid.org/0009–0004–2558–8549
adresa electronică: alina.pătru@spiruharet.ro

ABORDĂRI MODERNE PRIVIND UTILIZAREA ȘI VALORIFICAREA URMELOR CRIMINALISTICE ÎN IDENTIFICAREA AUTORILOR INFRACȚIUNILOR VIOLENTE

În contextul dezvoltării continue a tehnologiilor de investigare criminalistică, urmele descoperite la locul faptei reprezintă una dintre cele mai importante surse de informații pentru identificarea autorilor infracțiunilor violente. Valorificarea eficientă a acestora contribuie atât la stabilirea împrejurărilor comiterii faptei, cât și la reconstituirea mecanismului infracțional și la individualizarea participanților la activitatea infracțională. Articolul analizează principalele categorii de urme criminalistice utilizate în activitatea de investigare, cu accent asupra urmelor papilare, biologice, digitale și a altor urme materiale cu relevanță probatorie.

Sunt evidențiate metodele moderne de descoperire, fixare, ridicare și examinare a urmelor, precum și contribuția tehnologiilor contemporane la creșterea eficienței procesului de identificare. De asemenea, sunt analizate rolul expertizelor criminalistice și importanța cooperării interdisciplinare dintre specialiștii din domeniul criminalisticii, medicinei legale și tehnologiei informației. Studiul evidențiază faptul că utilizarea unor metode științifice avansate permite obținerea unor rezultate relevante din punct de vedere probator și contribuie la creșterea gradului de certitudine în identificarea autorilor infracțiunilor violente.

Concluziile subliniază necesitatea adaptării permanente a metodelor de investigare la evoluția fenomenului infracțional și la dezvoltarea tehnologiilor utilizate în activitatea criminalistică, pentru asigurarea unei administrări eficiente a probelor și pentru realizarea actului de justiție.

Cuvinte–cheie: urme criminalistice, identificare criminalistică, infracțiuni violente, expertiză criminalistică, mijloace de probă, cercetarea la fața locului.

Pătru Alina Daniela
Associate Professor, PhD, Department of Legal and Administrative Sciences,
Faculty of Legal and Administrative Sciences,
Spiru Haret University,
Bucharest, Romania

MODERN APPROACHES TO THE USE AND EXPLOITATION OF FORENSIC TRACES IN THE IDENTIFICATION OF VIOLENT CRIME OFFENDERS

In the context of the continuous development of forensic investigation technologies, traces discovered at crime scenes represent one of the most important sources of information for identifying perpetrators of violent crimes. Their effective use contributes not only to establishing the circumstances of the offense but also to reconstructing the criminal mechanism and identifying the individuals involved in the criminal activity. This paper analyzes the main categories of forensic traces used in criminal investigations, with particular emphasis on fingerprint, biological, digital, and other material traces with evidentiary value.

The study highlights modern methods of detecting, documenting, collecting, and examining forensic traces, as well as the contribution of contemporary technologies to improving the efficiency of the identification process. Furthermore, it examines the role of forensic expertise and the importance of interdisciplinary cooperation among specialists in forensic science, forensic medicine, and information technology. The research demonstrates that the use of advanced scientific methods enables investigators to obtain highly relevant evidentiary results and increases the level of certainty in identifying offenders involved in violent crimes.

The conclusions emphasize the need for the continuous adaptation of investigative methods to the evolving nature of criminal phenomena and technological advancements in forensic science, in order to ensure effective evidence management and the proper administration of justice.

Keywords: forensic traces, forensic identification, violent crimes, forensic expertise, evidence, crime scene investigation.

1. Introducere

Urmele criminalistice reprezintă una dintre cele mai importante categorii de mijloace tehnico–științifice utilizate în activitatea de descoperire și cercetare a infracțiunilor. Încă de la apariția criminalisticii ca disciplină autonomă, principiul potrivit căruia orice activitate infracțională lasă urme a constituit fundamentul procesului de identificare a autorilor și de stabilire a împrejurărilor în care a fost comisă fapta. În acest context, urmele nu sunt simple consecințe materiale ale unei acțiuni umane, ci veritabile surse de informații capabile să ofere date relevante cu privire la identitatea persoanelor implicate, modul de operare, succesiunea activităților desfășurate și mecanismul producerii evenimentului infracțional.

În cazul infracțiunilor violente, importanța urmelor criminalistice este deosebită, deoarece acestea permit reconstituirea unor activități desfășurate într–un interval de timp redus, caracterizate prin interacțiuni complexe între autor, victimă și mediul înconjurător. Urmele de sânge, urmele papilare, urmele biologice, urmele de încălțăminte, urmele instrumentelor utilizate sau datele digitale rezultate din utilizarea

dispozitivelor electronice constituie elemente esențiale pentru stabilirea adevărului judiciar.

Evoluția tehnologiei a influențat profund modul de valorificare a urmelor criminalistice. Dezvoltarea tehnicilor moderne de analiză ADN, perfecționarea sistemelor automate de identificare a amprentelor, utilizarea tehnologiilor de scanare tridimensională, precum și integrarea instrumentelor informatice în activitatea de investigare au extins considerabil posibilitățile de identificare a autorilor infracțiunilor [1, p.133].

Într–o societate caracterizată de diversificarea formelor de manifestare a criminalității și de utilizarea unor metode tot mai sofisticate de comitere a faptelor penale, urmele criminalistice continuă să reprezinte unul dintre cele mai sigure și obiective mijloace de probă.

2. Rolul urmelor criminalistice în reconstituirea mecanismului infracțional și individualizarea autorului

Reconstituirea mecanismului infracțional presupune stabilirea modului concret în care s–a produs evenimentul cercetat, pe baza interpretării coroborate a tuturor urmelor descoperite. În cazul infracțiunilor contra vieții și integrității corporale, analiza urmelor permite determinarea naturii agresiunii, a succesiunii actelor de violență și a eventualelor acțiuni de apărare sau de disimulare întreprinse de autor [2, p.93].

Un rol deosebit îl au urmele biologice, care permit nu doar identificarea persoanelor implicate, ci și stabilirea contactului dintre acestea și locul faptei. Progresele realizate în domeniul geneticii judiciare au transformat analiza ADN într–unul dintre cele mai eficiente instrumente de identificare criminalistică, capabil să ofere rezultate cu un grad foarte ridicat de certitudine. În numeroase cauze privind infracțiuni violente, urmele biologice descoperite pe corpul victimei, pe obiectele folosite la comiterea faptei sau în perimetrul locului faptei au constituit elemente decisive pentru identificarea autorului [3, p.61].

La fel de importante sunt urmele papilare, care continuă să reprezinte una dintre cele mai utilizate categorii de urme în practica criminalistică. Caracterul lor individual, stabil și inalterabil permite asocierea unei persoane cu un anumit obiect sau cu un anumit loc.

În ultimii ani, dezvoltarea tehnologiilor digitale a determinat apariția unor noi categorii de informații relevante pentru activitatea de identificare. Datele extrase din telefoane mobile, sisteme GPS, camere de supraveghere, rețele sociale sau alte dispozitive electronice completează informațiile furnizate de urmele clasice și permit reconstituirea traseelor, contactelor și activităților desfășurate de autor înainte și după săvârșirea infracțiunii [4, p.45].

Valoarea probatorie a urmelor criminalistice rezultă tocmai din posibilitatea coroborării acestora într–un sistem unitar de dovezi. Cu cât numărul elementelor concordante este mai mare, cu atât crește gradul de certitudine privind identificarea autorului și reconstituirea mecanismului infracțional.

3. Concluzii

Analiza efectuată evidențiază faptul că valoarea probatorie a urmelor criminalistice nu se limitează la simpla lor existență materială, ci depinde în mod direct de modul în care acestea sunt descoperite, fixate, conservate, examinate și interpretate. Utilizarea tehnicilor moderne de investigare, precum analiza ADN, sistemele automate de identificare a amprentelor, tehnologiile digitale și metodele avansate de procesare a informațiilor, a contribuit la creșterea gradului de precizie și obiectivitate în activitatea de identificare a autorilor infracțiunilor violente.

Totodată, rezultatele investigației criminalistice sunt influențate de colaborarea interdisciplinară dintre specialiștii din domeniul criminalisticii, medicinei legale, biologiei judiciare și tehnologiei informației.

În contextul actual, marcat de utilizarea unor metode tot mai sofisticate de comitere și disimulare a faptelor penale, valorificarea eficientă a urmelor criminalistice reprezintă o condiție esențială pentru creșterea eficienței activităților de investigare.

În concluzie, urmele criminalistice își mențin rolul fundamental în identificarea autorilor infracțiunilor violente, iar integrarea tehnologiilor moderne în activitatea de investigare contribuie la consolidarea caracterului științific al procesului de probațiune și la realizarea unui act de justiție bazat pe certitudine și obiectivitate.

Lista Sursei Utilizate:

1.Grecu, Polixenia, Impact of Environmental Conditions on the Persistence and Quality of Fingermarks: Implications for Crime Scene Investigation, în Journal of Law and Public Administration, Volumul XI, Nr. 22, 2025, pp. 132–139.

2.Grecu, Polixenia, Investigating Death by Asphyxia – Correlating Scene Findings with Autopsy Results, în Current Issues in Law and Socio–Economic Relations. Scientific Journal, Nr. 1(7), Volumul 1, Kiev, Ukraine, 2025, pp. 92–99.

3.Pătru, Alina Daniela, Criminalistică, Editura Sitech, Craiova, 2024, 207 p.

4.Pătru, Alina Daniela, Scenele violenței. Analiza urmelor și reconstituirea faptelor, Editura Sitech, Craiova, 2025, 232 p.

DOI https://doi.org/10.32837/11300.33538

Рибалко Андрій
судовий експерт сектору психологічних досліджень лабораторії почеркознавчих, лінгвістичних, психологічних та мистецтвознавчих досліджень
Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»,
м. Харків, Україна
ORCID: https://orcid.org/ 0000–0002–4758–351X
e–mail: ribalko.andrii@gmail.com

Ковкіна Євгенія
кандидатка філологічних наук,
завідувачка лабораторії почеркознавчих, лінгвістичних, психологічних та мистецтвознавчих досліджень
Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»,
м. Харків, Україна
ORCID: https://orcid.org/ 0000–0001–8693–9868
e–mail: evkovkina@gmail.com

ІМПЛІЦИТНІ ТА ГІБРИДНІ СПОНУКАЛЬНІ ВИСЛОВЛЮВАННЯ У ЦИФРОВІЙ КОМУНІКАЦІЇ ЯК ОБ'ЄКТ СУДОВОЇ ПСИХОЛОГО–ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ

У тезах обґрунтовано доцільність виокремлення імпліцитних і гібридних спонукальних висловлювань у цифровій комунікації як самостійного об'єкта судової психолого–лінгвістичної експертизи. Показано, що поведінково спрямований зміст може формуватися не лише прямим наказом, а й через натяк, оцінну рамку, легітимацію бажаної дії та поєднання вербальних і візуальних засобів. Запропоновано триконтурну модель їх аналізу: лінгвопрагматичну, дискурсивно–контекстуальну й психологічну.

Ключові слова: судова психолого–лінгвістична експертиза, цифрова комунікація, імпліцитне спонукання, гібридна спонукальна конструкція, заклик, психологічний вплив, мультимодальність.

Rybalko Andrii
Forensic Expert of the Sector of Psychological Research, Laboratory of Handwriting, Linguistic, Psychological, and Art Studies, Hon. Prof. M. S. Bokarius National Scientific Center «Institute of Forensic Expertise», Kharkiv, Ukraine

Kovkina Yevheniia
PhD in Philology,
Head of the Laboratory of Handwriting, Linguistic, Psychological, and Art Studies,
Hon. Prof. M. S. Bokarius National Scientific Center «Institute of Forensic Expertise», Kharkiv, Ukraine

IMPLICIT AND HYBRID DIRECTIVE UTTERANCES IN DIGITAL COMMUNICATION AS AN OBJECT OF FORENSIC PSYCHOLOGICAL AND LINGUISTIC EXAMINATION

The paper substantiates the need to distinguish implicit and hybrid directive utterances in digital communication as a specific object of forensic psychological and linguistic examination. It is argued that action–oriented meaning may be created not only by direct commands, but also through hints, evaluative framing, legitimisation of a desired action, and the interaction of verbal and visual resources. A three–contour analytical model is proposed: linguo–pragmatic, discourse–contextual, and psychological.

Key words: forensic psychological and linguistic examination, digital communication, implicit inducement, hybrid directive construction, appeal, psychological influence, multimodality.

Цифрова комунікація істотно змінила мовні способи орієнтації адресата на певну дію. У соціальних мережах, месенджерах, коментарях, телеграм–каналах, відеопідписах і мультимодальних публікаціях спонукальний зміст дедалі частіше не збігається з формальною граматичною формою висловлювання. Прямий наказ або відкритий заклик може замінюватися натяком, риторичним запитанням, осудом бездіяльності, схваленням бажаної моделі поведінки чи емоційно забарвленим «очевидним висновком», який адресатові пропонується зробити самостійно. Для судової психолого–лінгвістичної експертизи це створює окремий методичний виклик: у фокусі аналізу має опинятися не лише буквальний зміст фрази, а й її прагматична функція в конкретному цифровому контексті.

Науково–методичні рекомендації з питань підготовки та призначення судових експертиз передбачають дослідження мовленнєвих матеріалів щодо наявності закликів і спонукання до певних дій [1]. Водночас сучасна цифрова комунікація демонструє, що релевантний для експерта поведінково спрямований зміст може формуватися не лише через ізольовану імперативну конструкцію, а через сукупність семантичних, синтаксичних, прагматичних і контекстуальних ознак. У вітчизняних дослідженнях закликів слушно підкреслюється, що для встановлення спонукальності значущими є не лише лексико–граматичні показники, а й адресованість висловлювання, характер передбачуваної дії, оцінна рамка та загальна комунікативна ситуація [2, с. 280–286].

Імпліцитним спонукальним висловлюванням доцільно вважати таке повідомлення, у якому орієнтація адресата на певну дію не виражена прямим імперативом, однак відновлюється з мовленнєвого й позамовмовленнєвого контексту. Його директивність може виникати через пресупозицію необхідності дії, апеляцію до морального обов'язку, репутаційний тиск, порівняння «належних» і «неналежних» учинків. Гібридною спонукальною конструкцією є комунікативний комплекс, у якому директивний ефект формується взаємодією кількох компонентів: вербального тексту, зображення, символу, хештегу, монтажної послідовності, реакційного коментаря, репоста або серії пов'язаних повідомлень. Тому об'єктом експертного аналізу має бути повідомлення в його реальному цифровому функціонуванні, а не лише ізольована фраза.

Імпліцитне й гібридне спонукання не слід змішувати з будь–яким емоційним, переконувальним або оціноціночним висловлюванням. Судова психолого–лінгвістична експертиза має чітко відмежовувати інформаційне повідомлення, оціночне судження, пропагандистський наратив, маніпулятивний вплив і власне спонукальну конструкцію, у якій відновлюється вектор бажаної дії адресата. У працях із проблематики маніпулятивних технологій обґрунтовано, що психологічний вплив може реалізовуватися через навіювання оцінок, емоційне зараження, тиск авторитетом та інші механізми, проте наявність таких ознак ще не є тотожною спонукальному змісту [3, с. 683–684]. Так само пропагандистський контент не завжди містить безпосередню поведінкову орієнтацію; для її встановлення потрібна реконструкція конкретної комунікативної спрямованості матеріалу [4, с. 104–105].

В експертній практиці особливо складними є висловлювання, у яких пряме спонукання замінюється модальністю належності, сорому чи соціальної очікуваності. Конструкції на кшталт «кожен відповідальний має визначитися», «неучасть теж є вибором», «справжні однодумці не залишаються осторонь» можуть виконувати не лише оціночну, а й директивну функцію, якщо вони включені в контекст, де адресатам пропонується конкретна модель поведінки. Аналогічно риторичні запитання здатні слугувати не запитом інформації, а інструментом нав'язування очікуваного рішення. Водночас експерт не має механічно трактувати будь–яку експресивну фразу як спонукальну: необхідною є перевірка того, чи встановлюються поведінково релевантна інтенція, адресність і контекстна доцільність передбачуваної дії.

Цифровий контекст не створює спонукання автоматично, проте істотно змінює умови його актуалізації та інтерпретації. Для експерта мають значення спосіб оприлюднення матеріалу, його серійність, наявність попередніх і наступних повідомлень, реакції аудиторії, репости, коментарі, цитування, маркування групової належності, обрамлення публікації заголовком або заставкою. Те саме речення у приватному листуванні, у відкритому пості й у каналі з численною аудиторією може мати різну прагматичну вагу. Дослідження проблем кваліфікації пропагандистських повідомлень у соціальних мережах

показують, що цифрові платформи модифікують механізми поширення та сприйняття впливового контенту, а тому експертний аналіз не може ігнорувати формат і канали циркуляції висловлювання [5, с. 84–85].

Психолого–лінгвістичний аспект дослідження полягає в установленні того, яким чином мовна форма може актуалізувати мотиваційні, емоційні та групові механізми сприйняття. Імпліцитна директивність часто реалізується не через жорстку вказівку, а через створення умов, за яких адресатові пропонується самостійно «вгадати» соціально схвалюваний крок. У сучасних працях з аналізу incitement підкреслюється, що інтерпретація поведінково спрямованих висловлювань потребує врахування не лише локальної фрази, а й того інтерпретаційного конструкту, який вона вибудовує в аудиторії [6, p. 35–37]. Саме тому експерт має співвідносити форму висловлювання з очікуваним прагматичним ефектом, не підміняючи аналіз суб'єктивними припущеннями.

Окрему групу становлять конструкції з позитивною легітимацією бажаної поведінки та негативною оцінкою альтернативи. Якщо висловлювання представляє одну дію як вияв гідності, належності до «своїх», моральної зрілості або соціальної відповідальності, а відмову від неї – як слабкість, байдужість чи відступ від групової норми, воно може створювати непрямий психологічний примус. У цифровому середовищі така схема часто підсилюється публічністю обговорення: адресат орієнтується не лише на автора, а й на уявну чи реальну реакцію спільноти. Зарубіжні дослідження спонукання у мережевих середовищах підтверджують значення групової афіліації, розмежування «своїх» і «чужих» та морального виправдання передбачуваної дії як складників директивного впливу [7, p. 623–625].

Відповідно, доцільно аналізувати не лише початкове повідомлення, а й комунікативний ланцюг, у якому воно функціонує. У низці випадків спонукальний сенс виникає поступово: перша публікація формує негативну оцінку ситуації, друга – персоніфікує суб'єкта відповідальності, третя – демонструє схвалюваний зразок реакції, четверта – подає його як норму для аудиторії. Окремо жоден із фрагментів може бути недостатнім для висновку, проте в сукупності вони створюють структурований сценарій поведінки. Тому експерт має фіксувати межі досліджуваного мовленнєвого матеріалу, критерії об'єднання фрагментів у єдиний дискурсивний комплекс та підстави, з яких окремі елементи розглядаються як взаємопов'язані.

Для судової психолого–лінгвістичної експертизи продуктивною є триконтурна модель аналізу імпліцитних і гібридних спонукальних висловлювань. Перший контур – лінгвопрагматичний: він охоплює аналіз семантики, синтаксису, модальності, оцінки, пресупозицій, мовленнєвих актів і прихованої адресації. Другий – дискурсивно–контекстуальний: він спрямований на визначення місця повідомлення в комунікативній послідовності, аналіз аудиторії, жанру, каналу поширення, полікодової організації й фактичного інформаційного оточення. Третій – психологічний: він дає змогу виявити, чи

створюється тиск через сором, солідаризацію, авторитет джерела, моральну безальтернативність або інші механізми поведінкового спрямування. Лише узгодження результатів цих контурів створює належну аргументаційну базу для експертного висновку.

У межах практичного дослідження послідовність аналізу може бути вибудувана від встановлення меж матеріалу до реконструкції його спонукального вектора. Спершу визначаються цільова або передбачувана аудиторія, канал поширення та жанрова природа повідомлення. Далі виокремлюються змістові одиниці, що задають оцінну рамку, модель бажаної поведінки, засоби адресації та мовні індикатори необхідності чи схвалюваності дії. Після цього аналізується роль візуальних і супровідних компонентів, а також місце матеріалу в комунікативному ланцюзі. Завершальним етапом стає узгодження лінгвістичних, дискурсивних і психологічних ознак із формулюванням висновку про наявність або відсутність імпліцитного чи гібридного спонукального змісту.

Водночас експерт має враховувати чинники, що можуть знижувати або змінювати спонукальну інтерпретацію. До них належать цитування чужого висловлювання, переказ новини, іронічне чи пародійне використання директивної формули, навчальний або аналітичний контекст, критичне відтворення чужої позиції, дискусійний характер повідомлення. Формальна наявність риторичного запитання, оцінного контрасту чи модальності обов’язку в таких випадках не є достатньою підставою для висновку. Кваліфікований аналіз потребує перевірки контекстуальної узгодженості всіх ознак і відмови від автоматичних висновків за одиничними словами або конструкціями.

Як допоміжний орієнтир у випадках, коли досліджуються висловлювання з потенційно значним суспільним резонансом, може враховуватися Рабатський пороговий тест, який пропонує брати до уваги контекст, статус мовця, намір, зміст і форму повідомлення, масштаб його поширення та ймовірність шкоди [8, p. 1]. Хоча цей тест не підміняє національні експертні методики й не є універсальною формулою для будь–якого психолого–лінгвістичного дослідження, він корисний як структурована рамка оцінювання комунікативної значущості висловлювання. Його застосування особливо виправдане тоді, коли необхідно відмежувати емоційно різке, але загальне повідомлення від матеріалу, що в конкретному контексті містить чітко відновлюваний поведінковий імпульс.

Отже, імпліцитні та гібридні спонукальні висловлювання у цифровій комунікації доцільно розглядати як самостійний і методично значущий об’єкт судової психолого–лінгвістичної експертизи. Їхня специфіка полягає в тому, що поведінково спрямований зміст може бути прихований у підтексті, розподілений між різними семіотичними елементами або сформований через послідовність повідомлень, а не через окремий прямий наказ. Для обґрунтованого експертного висновку необхідно встановити наявність вектора бажаної поведінки, адресованість повідомлення, лінгвопрагматичні засоби непрямої директивності, дискурсивний контекст, мультимодальне посилення та психологічні механізми

потенційного впливу. Такий підхід дозволяє уникнути як надмірного розширення поняття спонукання, так і недооцінки складних цифрових форм поведінкової орієнтації адресата.

Перелік використаних джерел:

1. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково–методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 № 53/5 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0705–98

2. Ковкіна Є. В., Свиридова Л. В., Дідушок Н. Я. Семантико–текстуальні дослідження закликів. Теорія та практика судової експертизи і криміналістики. 2020. Вип. 22. С. 280–292. DOI: 10.32353/khrife.2.2020.22.

3. Литвиненко Е. С., Стромило А. П. Визначення ознак використання маніпулятивних технологій у мовленнєвій діяльності підекспертних осіб у судових психолого–лінгвістичних експертизах у кримінальних провадженнях щодо злочинів проти основ національної безпеки. Криміналістика і судова експертиза. 2024. Вип. 69. С. 679–689. DOI: 10.33994/kndise.2024.69.60.

4. Ажнюк Л. Концепт «пропаганда» з позицій прагматичної та юридичної лінгвістики. Мовознавство. 2025. № 4. С. 92–110. DOI: 10.33190/0027–2833–343–2025–4–006.

5. Загиней–Заболотенко З. А., Пилипець А. Ю. Пропаганда з використанням соціальних мереж: окремі проблеми кваліфікації. Науковий вісник Ужгородського національного університету. Серія Право. 2026. Вип. 93. Ч. 4. С. 84–91. DOI: 10.24144/2307–3322.2026.93.4.12.

6. Danziger R. Interpretive constructs: The case of incitement to violence and terror. Journal of Pragmatics. 2025. Vol. 245. P. 35–49. DOI: 10.1016/j.pragma.2025.06.004.

7. Etaywe A., Zappavigna M. The role of social affiliation in incitement: A social semiotic approach to far–right terrorists' incitement to violence. Language in Society. 2024. Vol. 53. No. 4. P. 623–648. DOI: 10.1017/S0047404523000404.

8. Office of the United Nations High Commissioner for Human Rights. One–pager on «incitement to hatred»: The Rabat threshold test. 2020. 1 p. URL: https://www.ohchr.org/sites/default/files/Rabat_threshold_test.pdf

DOI https://doi.org/10.32837/11300.33540

Столярова Ірина
завідувач відділу фізичних, хімічних, біологічних досліджень
Одеського науково–дослідного інституту судових експертиз
Міністерства юстиції України,
м. Одеса, Україна,
ORCID: https://orcid.org/0009–0000–2255–9719,
e–mail: irina.stoliarov@gmail.com

Пагурець Ольга
головний судовий експерт відділу фізичних, хімічних, біологічних досліджень Одеського науково–дослідного інституту судових експертиз
Міністерства юстиції України,
м. Одеса, Україна,
ORCID: https://orcid.org/0009–0004–7918–6211,
e–mail: olga.pahurets@gmail.com

Макарова Олександра
головний судовий експерт відділу фізичних, хімічних, біологічних досліджень Одеського науково–дослідного інституту судових експертиз
Міністерства юстиції України,
м. Одеса, Україна,
ORCID: https://orcid.org/0009–0005–2664–9814,
e–mail: matveevskaaaleksandra@gmail.com

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ДЛЯ РОЗШИФРУВАННЯ СПЕКТРІВ У СУДОВІЙ ЕКСПЕРТИЗІ МАТЕРІАЛІВ, РЕЧОВИН ТА ВИРОБІВ

У тезах проаналізовано роль штучного інтелекту (далі – ШІ) у спектральному аналізі при проведенні судової експертизи матеріалів, речовин та виробів. Розглянуто переваги автоматизації розшифровки складних спектрів, ідентифікації сумішей та подолання суб'єктивізму. Особливу увагу приділено недолікам, що виникають при застосуванні ШІ: проблемі «чорної скриньки», залежності від вибірок, юридичним ризикам та іншім.

Ключові слова: Штучний інтелект, спектроскопія, криміналістична експертиза, експертиза матеріалів, речовин та виробів, нейронні мережі, алгоритм, доказова база.

Stoliarova Irina
Head of the department of physical, chemical and biological research of the Odesa Research Institute of Forensic expertise of the Ministry of Justice of Ukraine, Odesa, Ukraine

Pahurets Olha
Chief forensic expert of the department of physical, chemical and biological research of the Odesa Research Institute of Forensic expertise of the Ministry of Justice of Ukraine, Odesa, Ukraine

Makarova Oleksandra
Chief forensic expert of the department of physical, chemical and biological research of the Odesa Research Institute of Forensic expertise of the Ministry of Justice of Ukraine, Odesa, Ukraine

ARTIFICIAL INTELLIGENCE AS A TOOL FOR SPECTRUM DECODING IN FORENSIC EXAMINATION OF MATERIALS, SUBSTANCES AND PRODUCTS

The theses analyze the role of artificial intelligence (hereinafter referred to as AI) in spectral analysis during forensic examination of materials, substances and products. The advantages of automating the decoding of complex spectra, identifying mixtures, and overcoming subjectivity are considered. Particular attention is paid to the shortcomings arising from the application of AI, including the «black box» problem, dependence on datasets, legal risks, and others.

Key words: Artificial intelligence, spectroscopy, forensic examination, examination of materials, substances and products, neural networks, algorithm, evidentiary basis.

Сучасна експертиза матеріалів, речовин та виробів стикається з викликами, що вимагають не лише високої точності результатів, а й оперативного опрацювання значних масивів даних. Спектроскопічні методи дослідження, зокрема ІЧ–Фур'є–спектроскопія, мас–спектроскопія, рентгенофлуоресцентний аналіз та інші, генерують складні цифрові профілі, інтерпретація яких потребує високого рівня фахової підготовки [1]. В цьому контексті ШІ виступає інструментом, здатним трансформувати спектральні дані у доказову базу та мінімізувати вплив суб'єктивного чинника під час проведення експертного дослідження.

Традиційний підхід до аналізу спектрів ґрунтується на порівнянні отриманих спектральних графіків з бібліотечними етанолонами та пошуку характерних піків або смуг поглинання чи випромінювання. Однак зазначений підхід має низку обмежень:

складність аналізу багатокомпонентних сумішей, у яких відбувається накладання спектральних піків, що ускладнює ідентифікацію окремих компонентів;

наявність шуму і дрейфу базової лінії, спричинених технічними недосконалостями обладнання або станом досліджуваного зразка;

вплив людського фактора, за якого експерт може не враховувати мало виражені піки, що мають важливе значення для визначення походження матеріалу.

Для подолання зазначених проблем застосування ШІ передбачає реалізацію багатоступеневого алгоритмічного підходу. На етапі попередньої обробки (preprocessing) нейронні мережі забезпечують очищення спектрів від фонового шуму, виконують нормалізацію та автоматичну корекцію базової лінії, що дає змогу стандартизувати результати, отримані на різному аналітичному обладнанні.

На етапі розпізнавання образів (pattern recognition) спектр розглядається як цілісний «спектральний відбиток», а не як сукупність окремих піків. Згорткові нейронні мережі (CNN) здатні виявляти складні закономірності та приховані кореляції, які є малопомітними або недоступними для візуального аналізу людиною.

Практичним прикладом є використання портативних ІЧ–Фур'є–спектрометрів для ідентифікації вибухових і наркотичних речовин у польових умовах. У таких випадках ШІ забезпечує миттєве порівняння отриманих спектрів із хмарними базами даних. За наявності домішок або навмисного «розбавлення» наркотичних речовин алгоритми деконволюції, спрямовані на розділення змішаних сигналів, дозволяють виділити спектр активного компонента. Крім того, застосування методів предиктивного аналізу дає можливість ідентифікувати модифіковані молекули, які відсутні у наявних базах даних, шляхом визначення їх належності до певних груп речовин, зокрема синтетичних канабіноїдів або похідних фентанілу.

Особливого значення набуває застосування ШІ під час дослідження нафтопродуктів і пально–мастильних матеріалів у справах, пов'язаних із підпалами. Алгоритми машинного навчання дають можливість класифікувати тип палива та виявляти сліди нафтопродуктів у складних сумішах із продуктами піролізу, які часто маскують цільові компоненти.

Інтеграція технологій ШІ в аналіз даних, отриманих методами ІЧ–спектроскопії та мас–спектрометрії, створює передумови для формування універсальної системи комплексного аналізу речовин. Такий підхід дозволяє:

підвищити точність і комплексність досліджень, а також скоротити строки проведення експертиз;

мінімізувати суб'єктивізм експертного оцінювання завдяки використанню математичних моделей і алгоритмів;

забезпечити постійне вдосконалення системи шляхом накопичення та аналізу нових спектральних даних, що сприяє підвищенню точності моделей у процесі їх навчання.

Водночас застосування ШІ не може повністю замінити спеціальні знання та професійний досвід судового експерта. Достовірність результатів, отриманих за допомогою ШІ, безпосередньо залежить від якості та повноти даних, використаних для навчання нейромереж. У разі внесення до навчальної вибірки спектрів із помилковими або некоректними описами система здатна відтворювати ці помилки у подальшому, формуючи хибні результати на системному рівні.

Інтеграція технологій ШІ в практику судової експертизи характеризується значним потенціалом щодо інтенсифікації дослідницького процесу. Водночас впровадження автоматизованих алгоритмів у таку консервативну та юридично відповідальну сферу супроводжується низкою критичних викликів, які потребують детального аналізу.

Однією з ключових проблем є ефект «чорної скриньки». Складні нейромережеві алгоритми здатні генерувати високоефективні результати, проте механізм формування логічного висновку всередині архітектури моделі часто залишається неперсонізованим та непрозорим, що в свою чергу може спровокувати деградацію професійних компетенцій. Надмірне делегування аналітичних функцій нейронним мережам може спричинити втрату фахівцями навичок самостійної інтерпретацій спектрограм, що створює ризик професійної безпорадності експерта у разі виникнення технічних збоїв або при дослідження нестандартних об'єктів. Верифікація доказової бази, відсутність пояснення того, які саме ознаки чи піки спектра були визначенні алгоритмом як релевантні, ставить під сумнів доказову силу отриманого висновку в межах судового процесу. Адже відповідно до чинного законодавства, суб'єктом судової експертизи є фізична особа, яка володіє спеціальними знаннями, тому саме експерт зобов'язаний науково обґрунтувати свій висновок і несе персональну відповідальність за його достовірність [2].

Функціональне призначення ШІ в судовій експертизі має обмежуватись роллю допоміжного інструментарію. Найбільшу ефективність ШІ демонструє на етапах первинного скринінгу, систематизації та фільтрації великих масивів даних. Кінцева верифікація та інтерпретація результатів мають залишатися виключно прерогативою кваліфікованого експерта, що забезпечує дотримання принципів об'єктивності, повноти дослідження та наукової обґрунтованості експертного висновку.

На сьогодні застосування штучного інтелекту для розшифрування та інтерпретації спектрів фундаментально змінює методологічні підходи до експертизи матеріалів, речовин та виробів. Перехід від суб'єктивного візуального зіставлення спектрограм до інтелектуального аналізу цифрових масивів даних є

високовалідним, особливо в умовах правового режиму воєнного стану. Такий підхід забезпечує генерацію інформативно насичених даних, аналіз яких дає змогу отримати об'єктивно достовірні результати дослідження. Це істотно підвищує верифікованість висновку експерта як процесуального джерела доказів та мінімізує ризики оскарження доказової бази.

Перелік використаних джерел:

1.Сучасні методи дослідження матеріалів, речовин та виробів: огляд / [уклад.: Барікова О.М., Остапюк Ю.М., Повійчук А.О., Шалига М.В.]. Київ : ДНДЕКЦ МВС України, 2022. 55 с.

2.Закон України «Про судову експертизу» від 25.02.1994 № 4038а–XII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/4038–12#Text

DOI https://doi.org/10.32837/11300.33541

Ткаченко Наталія
кандидат юридичних наук,
директор Департаменту експертного забезпечення правосуддя
Міністерства юстиції України, м. Київ, Україна,
ORCID: https://orcid.org/0000–0002–0589–0191,
e–mail: tnm_77@ukr.net

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА РОЗВИТОК СУДОВО–ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ

Досліджено напрями трансформації судово–експертної діяльності в умовах цифровізації суспільства. Проаналізовано проблеми дослідження цифрових слідів, оновлення методичного забезпечення, розвитку цифрових компетентностей експертів та використання сучасних технічних засобів.

Ключові слова: судово–експертна діяльність, судова експертиза, цифрові технології.

Tkachenko Nataliia
Candidate of Legal Sciences,
Director of the Department for Expert Support of Justice,
Ministry of Justice of Ukraine,
Kyiv, Ukraine

THE IMPACT OF DIGITAL TECHNOLOGIES ON THE DEVELOPMENT OF FORENSIC EXPERT ACTIVITY

The article examines the main directions in which forensic expert activity is being transformed under the conditions of societal digitalisation. It analyses the issues connected with the examination of digital traces, the renewal of methodological support, the development of experts' digital competencies, and the use of modern technical tools.

Key words: forensic expert activity, forensic examination, digital technologies.

Розвиток цифрових технологій, активне їх впровадження та використання в усіх сферах діяльності суспільства та держави трансформує також і сучасні підходи до здійснення судово–експертної діяльності, спонукаючи відповідну її адаптацію до сучасних реалій. Такі процеси обумовлені, з однієї сторони, новими запитами з боку ініціаторів проведення судових експертиз (слідчих, прокурорів, детективів, адвокатів тощо), пов'язаних з потребами судочинства у дослідженні цифрової інформації, технічних засобів, баз даних тощо, а з іншої – необхідністю оновлення підходів до організації та проведення судових експертиз, удосконалення науково–методичного забезпечення, модернізації матеріально–

технічної бази, впровадження цифрових інструментів та засобів, автоматизованих інформаційних систем, а також посилення кадрових ресурсів.

Поява цифрових слідів вчинення правопорушень, використання штучного інтелекту, інформаційних технологій з протиправною метою обумовлює необхідність у дослідженні нових об'єктів судової експертизи та вирішення завдань, з якими судові експерти раніше не стикалися. Це стосується, зокрема, дослідження інформації, що міститься у мобільних пристроях, комп'ютерних системах, хмарних сервісах, месенджерах, соціальних мережах, електронних документах, системах відеоспостереження, базах даних, а також цифрових слідів, які залишаються внаслідок використання програмного забезпечення, автоматизованих систем або алгоритмів штучного інтелекту. Тобто якщо раніше межі традиційних судових експертиз здебільшого були пов'язані з необхідністю дослідження матеріальних об'єктів, документів, слідів біологічного походження тощо, то сучасні способи вчинення правопорушень передбачають нові види слідів відповідних діянь у вигляді цифрової інформації різного характеру, для яких характерні зовсім інші способи ідентифікації, зміни змісту, фальсифікації. Тобто перед судовими експертами постають завдання щодо дослідження, зокрема, цифрових носіїв інформації з різною метою: встановлення факту наявності певної інформації на конкретному носії, змісту таких даних, джерела походження, ознак змін, копіювання тощо.

Окрему увагу необхідно звернути на якість методичного забезпечення судово–експертної діяльності. У зв'язку з тим, що цифрові дані мають іншу природу, зокрема, цифрові сліди відрізняються від інших видів слідів за своєю природою, механізмом утворення, особливостями зберігання, зміни змісту та знищення, а також способом та порядком їх виявлення [1, с. 20], потребує сучасних підходів і їх дослідження. Проте сучасні експертні методики не завжди здатні забезпечити належне вирішення завдань, що виникають при проведенні таких судових експертиз. В першу чергу це пов'язано зі швидкістю розвитку цифрових технологій, появою нових програмних продуктів, засобів комунікації, способів зберігання інформації та технічних механізмів приховування або зміни цифрових даних. У таких умовах методичне забезпечення судово–експертної діяльності потребує активного реагування шляхом розроблення, оновлення та впровадження сучасних методик дослідження, які б відповідали потребам практики.

Вирішення судовим експертом питань, пов'язаних з використанням цифрових технологій потребує не лише наявності відповідних спеціальних знань, а й постійного та безперервного їх оновлення у зв'язку з активною модернізацією технологій. Тому важливе значення у такому аспекті має підвищення кваліфікації судових експертів для забезпечення високого рівня якості проведених досліджень та зменшення ризиків допущення експертних помилок. Рівень професійної підготовки судових експертів повинен відповідати не лише їх здатності ефективно працювати з сучасними технологічними викликами під час проведення

досліджень, а й використовувати технології в інших напрямах судово–експертної діяльності, в тому числі застосовувати цифрові інструменти при організації та плануванні експертної роботи, підвищуючи тим самим її результативність. Тому підвищення кваліфікації судових експертів повинно бути спрямоване як на розвиток галузевих знань, умінь та навичок, а також загальних цифрових компетентностей.

Особливого значення набувають також питання інтеграції цифрових технологій у експертну практику. Використання сучасного програмного забезпечення, автоматизованих інформаційних систем, електронних баз даних, цифрових інструментів аналізу, моделювання та візуалізації результатів дослідження на сьогодні є необхідним елементом удосконалення судово–експертної діяльності. Наприклад, відомим випадком є використання штучного інтелекту при проведенні портретної судової експертизи у справі щодо розстрілу українського військовослужбовця російськими військовими, що була проведена Київським науково–дослідним інститутом судових експертиз. В результаті її проведення було встановлено особу загиблого Героя України Олександра Мацієвського. Це був перший випадок застосування штучного інтелекту під час таких досліджень в Україні. Перед судовими експертами поставили завдання встановити тотожність загиблого українського воїна, зображеного на відео. Фахівцям КНДІСЕ було передано відеозапис інциденту, оприлюднений 6 березня 2023 року. Крім того, надійшли порівняльні зразки – фотографії осіб, які, на думку правоохоронних органів, могли бути зображені на відео. Проблемою стала низька якість досліджуваного відеоматеріалу і розмиті фотографії, на що експерти звернули окрему увагу. Експерти КНДІСЕ підтвердили, що український військовий на відео – це снайпер 163–го батальйону 119–ї бригади територіальної оборони Чернігівської області Олександр Мацієвський. У результаті застосування штучного інтелекту продемонструвало, як сучасні технології можуть ефективно використовуватися для встановлення особи [2, с. 141]. Набуває розповсюдження також застосування 3D–технологій під час проведення досліджень. Наприклад, при проведенні судових портретних експертиз судовий експерт може самостійно привести 3D–модель обличчя людини до необхідного масштабу, повернути під правильним кутом, виміряти розмірні характеристики окремих ознак, порівняти їх, а також, за результатами експертизи, ефективно проілюструвати його результати [3, с. 91]. Таким чином, інтеграція цифрових технологій в експертну практику є необхідною умовою подальшого розвитку судово–експертної діяльності.

Таким чином, вплив цифрових технологій на розвиток судово–експертної діяльності має комплексний, системний характер. Цифровізація суспільства не лише спричиняє появу нових об’єктів та завдань судової експертизи, а також висуває нові вимоги до експертних кадрів, зумовлює необхідність удосконалення методичного забезпечення судово–експертної діяльності та впровадження сучасних засобів до її здійснення. Лише за умови узгодженого розвитку всіх цих

складових можливо забезпечити належну якість, об'єктивність і ефективність судових експертиз у сучасних умовах.

Перелік використаних джерел:

1.Вступ до цифрової криміналістики : навчальний посібник / В.Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова; за ред. В. Ю. Шепітька ; Нац. юрид. ун–т ім. Ярослава Мудрого. Харків : Право, 2025. 124 с.

2.Shepitko V., Shepitko M., Latysh K., Kapustina M., Demidova E. Artificial intelligence in crime counteraction: From legal regulation to implementation. Social & Legal Studios. 2024. Vol. 7, No. 1. P. 135–144. DOI: 10.32518/sals1.2024.135

3.Коваленко А. В. Перспективи запровадження 3D–технологій в судово–експертну діяльність. Криміналістика та судова експертиза у XXI столітті : матеріали всеукр. наук.–практ. семінару (Київ, 30 травня 2024 р.). Київ : ДНДЕКЦ МВС України, 2024. С. 89–91.

DOI https://doi.org/10.32837/11300.33544

Целуйко Михайло
кандидат юридичних наук, доцент, начальник Чернігівського територіального управління Державної судової адміністрації, м.Чернігів, Україна
ORCID: https://orcid.org/ 0000–0002–9689–4445
e–mail: chernihiv@kndise.gov.ua

Усенко Олена
кандидат юридичних наук, доцент, судовий експерт, завідувач Чернігівського відділення Київського науково–дослідного інституту судових експертиз Міністерства юстиції України, м.Чернігів, Україна
ORCID https://orcid.org/ 0000–0003–0534–5422
e–mail: chernihiv@kndise.gov.ua

ПЕРСПЕКТИВНІ НАПРЯМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ СУДОВОЇ ЕКСПЕРТИЗИ В УКРАЇНІ

У тезах досліджено перспективні напрями впровадження технологій штучного інтелекту у сферу судово–експертної діяльності України. Проаналізовано можливості застосування інтелектуальних алгоритмів під час проведення криміналістичних, цифрових, економічних, почеркознавчих, будівельно–технічних та земельно–технічних експертиз.

Ключові слова: штучний інтелект, судова експертиза, судово–експертна діяльність, цифровізація, криміналістика, цифрові докази, автоматизовані системи, інформаційні технології.

Tseluyko Mykhailo
Ph.D. in Law, Associate Professor, associate professor, head of the Chernihiv Territorial Administration of the State Judicial Administration, Chernihiv, Ukraine

Olena Usenko
Ph.D. in Law, Associate Professor, Forensic Expert, Head of the Chernihiv Branch of the Kyiv Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine, Chernihiv, Ukraine

THEORETICAL AND LEGAL FOUNDATIONS OF THE ORGANIZATION OF REMUNERATION FOR FORENSIC EXPERTS IN UKRAINE

The abstract examines promising directions for the implementation of artificial intelligence technologies in forensic expert activity in Ukraine. The possibilities of applying intelligent algorithms in criminalistic, digital, economic, handwriting, construction and land examinations are analyzed.

Keywords: artificial intelligence, forensic examination, forensic expert activity, digitalization, criminalistics, digital evidence, automated systems, information technologies.

На сучасному етапі в Україні лише формується система практичного застосування технологій штучного інтелекту у сфері правосуддя та судово–експертної діяльності. Водночас міжнародний досвід свідчить про значний потенціал інтелектуальних алгоритмів у процесі автоматизації аналітичних процедур, обробки цифрових даних та систематизації інформації [1, с. 81]. Використання подібних технологій у перспективі може стати одним із ключових напрямів модернізації вітчизняної системи судових експертиз.

Значна частина сучасної доказової інформації існує в електронній формі та потребує спеціалізованих методів дослідження. Йдеться про електронні документи, дані мобільних пристроїв, листування у месенджерах, інформацію із соціальних мереж, відеозаписи та інші цифрові сліди. Використання алгоритмів машинного навчання дозволяє автоматизувати процес пошуку релевантної інформації, класифікувати цифрові файли, встановлювати взаємозв’язки між інформаційними об’єктами та виявляти ознаки несанкціонованого втручання у комп’ютерні системи [2, с. 112].

Особливої актуальності використання технологій штучного інтелекту набуває у процесі документування та дослідження воєнних злочинів. У сучасних умовах постійно збільшується кількість фото–, відео– та супутникових матеріалів, які можуть мати доказове значення у кримінальних провадженнях. У перспективі інтелектуальні алгоритми можуть застосовуватися для автоматизованого аналізу відеозаписів, визначення географічного місця події, ідентифікації військової техніки, фіксації масштабів руйнувань та аналізу відкритих джерел інформації [3, с. 43]. Подібні технології здатні суттєво прискорити процес опрацювання доказових матеріалів та забезпечити більш ефективну систематизацію інформації.

Перспективним напрямом розвитку судово–експертної діяльності в Україні може стати створення єдиної інформаційно–аналітичної платформи судових експертиз із використанням елементів штучного інтелекту. Функціонування такої системи дозволило б автоматизувати пошук аналогічних експертних досліджень, накопичення методичних матеріалів, аналіз судової практики та пошук нормативно–правових джерел. Крім того, подібна платформа могла б забезпечити уніфікацію окремих підходів до проведення судових експертиз та сприяти підвищенню якості експертної практики.

Однією з перспективних новел у сфері судово–експертної діяльності є створення спеціалізованих мовних моделей штучного інтелекту, адаптованих до

української юридичної та експертної термінології. Використання подібних систем може бути доцільним під час аналізу значних обсягів текстових матеріалів, структурування інформації, пошуку нормативних джерел та підготовки проєктів окремих процесуальних документів. Крім того, інтелектуальні алгоритми можуть застосовуватися для виявлення типових помилок у підготовці експертних висновків та систематизації судової практики.

Перспективним є також використання технологій штучного інтелекту у сфері технічної експертизи документів. Автоматизовані системи можуть застосовуватися для аналізу метаданих електронних файлів, встановлення фактів редагування документів, виявлення ознак цифрового монтажу та перевірки справжності електронних підписів і реквізитів документів. У подальшому можливим є створення автоматизованої системи виявлення підроблених документів із інтеграцією до державних реєстрів та електронних інформаційних ресурсів.

У почеркознавчих дослідженнях алгоритми машинного навчання можуть використовуватися для автоматизованого аналізу графічних ознак письма, порівняння рукописних текстів та встановлення індивідуальних особливостей почерку. Водночас використання подібних технологій доцільно розглядати виключно як допоміжний інструмент аналітичної підтримки, оскільки остаточне формування експертного висновку повинно залишатися компетенцією судового експерта.

Суттєві перспективи використання технологій штучного інтелекту існують також у сфері будівельно–технічних та земельно–технічних експертиз. Поєднання геоінформаційних систем із технологіями автоматизованого аналізу дозволить здійснювати просторове моделювання об’єктів, дослідження меж земельних ділянок, реконструкцію механізму руйнування будівель та аналіз наслідків бойових дій. Подібні технології можуть суттєво підвищити точність експертних досліджень та оптимізувати процес аналізу просторових даних.

У сфері економічних досліджень штучний інтелект може використовуватися для аналізу бухгалтерської документації, моніторингу фінансових операцій та виявлення ознак економічних правопорушень. Автоматизовані алгоритми здатні виявляти нетипові фінансові операції, аналізувати взаємозв’язки між суб’єктами господарювання та встановлювати ознаки фіктивної діяльності. Подібні підходи вже використовуються міжнародними аудиторськими компаніями.

Разом із позитивними аспектами використання технологій штучного інтелекту існує низка проблем, які потребують належного нормативного врегулювання. Насамперед це стосується перевірки достовірності результатів автоматизованого аналізу, забезпечення прозорості алгоритмів, захисту персональних даних та визначення меж відповідальності експерта у разі використання інтелектуальних систем [2, с. 119]. Окремої уваги потребує питання розроблення єдиних методичних стандартів використання технологій штучного інтелекту під час проведення судових експертиз.

У зв'язку із цим подальший розвиток технологій штучного інтелекту у сфері судово–експертної діяльності повинен супроводжуватися формуванням комплексного нормативно–правового механізму регулювання їх застосування. Доцільним видається розроблення спеціалізованих методик використання інтелектуальних алгоритмів, порядку сертифікації програмних комплексів та процесуальних правил оцінки результатів автоматизованого аналізу у судовому провадженні.

Таким чином, використання технологій штучного інтелекту відкриває значні перспективи для розвитку судово–експертної діяльності в Україні. Інтеграція автоматизованих систем аналізу інформації, створення спеціалізованих цифрових платформ та використання інтелектуальних алгоритмів у різних видах експертиз здатні підвищити ефективність експертної практики та оптимізувати процес дослідження доказової інформації. Водночас упровадження таких технологій повинно здійснюватися із дотриманням принципів законності, процесуальної допустимості та належного контролю за результатами автоматизованого аналізу.

Перелік використаних джерел:

1.Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. – 4–е вид., перероб. і доп. – Х.: Право, 2008. С. 301

2.Білоус В. В. Цифрова криміналістика: сучасний стан та перспективи розвитку в Україні // Юридична наука. 2024. № 3. С. 374.

3.Калюжний Р. А., Гуцалюк М. В. Інформаційні технології у правоохоронній діяльності : монографія. Київ : Атіка, 2021. С. 217.

DOI https://doi.org/10.32837/11300.33550

Цільмак Олена
доктор юридичних наук, професор, завідувач кафедри психології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID ID: https://orcid.org/0000–0001–7348–4876
e–mail:cilmalen@gmail.com

КОГНІТИВНІ ВИКРИВЛЕННЯ У МЕХАНІЗМІ ФОРМУВАННЯ ЦИФРОВИХ СЛІДІВ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ

У тезах досліджено вплив когнітивних викривлень на механізм формування цифрових слідів злочинної діяльності. Проаналізовано роль психологічних помилок у поведінці правопорушника та їх значення для цифрової криміналістики.

Ключові слова: когнітивні викривлення, цифрові сліди, криміналістика, психологічна помилка, цифрова криміналістика, злочинна діяльність, поведінка правопорушника.

Tsilmak Olena
Doctor of Law, Professor, Head of the Department of Psychology,
National University «Odesa Law Academy»,
Odesa, Ukraine

COGNITIVE BIASES IN THE MECHANISM OF FORMING DIGITAL TRACES OF CRIMINAL ACTIVITY

This paper examines the influence of cognitive biases on the mechanism by which digital traces of criminal activity are formed. It analyses the role of psychological errors in an offender's behaviour and their significance for digital forensics.

Key words: cognitive biases, digital traces, forensic science, psychological errors, digital forensics, criminal activity, offender behaviour.

Стрімкий розвиток цифрових технологій, активне впровадження електронних комунікацій у повсякденне життя та розширення сфери використання інформаційно–комунікаційних систем істотно трансформували механізм вчинення кримінальних правопорушень. Сучасна злочинна діяльність дедалі частіше супроводжується використанням цифрових пристроїв, соціальних мереж, месенджерів, хмарних сервісів, а також спеціалізованого програмного забезпечення для приховування або модифікації інформації. У зв'язку з цим особливого значення набуває дослідження цифрових слідів як джерел криміналістично значущої інформації. Водночас формування таких слідів не є виключно технічним процесом, оскільки воно значною мірою обумовлюється

психічною діяльністю особи, її особливостями сприйняття, оцінки ризиків, прогнозування наслідків та прийняття рішень. Саме тому аналіз когнітивних викривлень у поведінці правопорушників дозволяє глибше зрозуміти закономірності виникнення цифрових слідів та механізм їх відображення у цифровому середовищі.

Когнітивні викривлення являють собою систематичні помилки мислення, які виникають у процесі обробки інформації та впливають на прийняття рішень. Вони обумовлюються обмеженістю людської уваги, дефіцитом часу, емоційним станом, попереднім досвідом, стереотипами та особливостями функціонування пам'яті. У криміналістичному аспекті когнітивні викривлення мають подвійне значення. З одного боку, вони впливають на поведінку слідчого та інших суб'єктів розслідування, а з іншого – визначають особливості дій правопорушника під час підготовки, вчинення та приховування злочину. Саме останній аспект набуває особливої актуальності в умовах цифровізації злочинної діяльності.

Механізм формування цифрових слідів нерозривно пов'язаний із поведінковими моделями особи, яка використовує цифрові технології [1]. Навіть за умови застосування анонімізаторів, VPN–сервісів, шифрування даних чи спеціалізованих засобів кіберзахисту правопорушник нерідко залишає значний обсяг інформації, яка може бути використана для його ідентифікації. Причиною цього часто є не технічна недосконалість засобів маскування, а саме когнітивні помилки, які виникають у процесі прийняття рішень. Злочинець може переоцінювати власні можливості, недооцінювати потенціал правоохоронних органів, неправильно оцінювати ризики викриття або помилково вважати окремі дії безпечними.

Одним із найбільш поширених когнітивних викривлень є ефект надмірної впевненості. Особи, які мають певний досвід використання цифрових технологій або раніше уникали викриття, часто починають переоцінювати власний рівень підготовки. У результаті вони допускають необережні дії, які формують стійкі цифрові сліди. Наприклад, кіберзлочинець може використовувати один і той самий псевдонім на різних платформах, повторно застосовувати однакові паролі, залишати характерні мовні конструкції у листуванні або входити до акаунтів із пристроїв, що раніше вже використовувалися для інших дій. Такі поведінкові особливості нерідко стають основою для криміналістичної ідентифікації особи.

Важливе значення має також ефект ілюзії контролю, який проявляється у переконанні особи в можливості повністю контролювати ситуацію та уникнути викриття. У цифровому середовищі це викривлення проявляється у впевненості правопорушника, що використання окремих технічних засобів автоматично гарантує анонімність. Унаслідок цього особа може нехтувати елементарними правилами цифрової безпеки, здійснювати авторизацію з особистих пристроїв, використовувати власні платіжні реквізити або підтримувати зв'язок із співучасниками через персональні акаунти. Формування цифрових слідів у такому

випадку відбувається через суперечність між наміром приховати діяльність та фактичними поведінковими звичками особи.

Окрему роль у механізмі цифрового слідоутворення відіграє евристика доступності, відповідно до якої людина оцінює ймовірність події на основі найбільш доступної або емоційно значущої інформації. Якщо правопорушник не стикався з реальними випадками викриття за певною схемою, він може вважати її безпечною. Така помилкова оцінка ризиків призводить до повторного використання однакових способів комунікації, електронних гаманців, IP–адрес або програмних рішень. Повторюваність дій створює характерний цифровий профіль, який може бути виявлений шляхом аналітичної обробки великих масивів даних.

Не менш важливим є ефект підтвердження, який полягає у схильності людини сприймати лише ту інформацію, яка підтверджує її попередні переконання. У контексті злочинної діяльності це може проявлятися у вибірковому аналізі інформації про методи викриття кіберзлочинів. Правопорушник концентрується на прикладах успішного уникнення відповідальності та ігнорує випадки затримання осіб за аналогічних умов. У результаті він формує викривлене уявлення про власну безпеку та допускає помилки, що призводять до накопичення цифрових доказів.

Суттєвий вплив на формування цифрових слідів має когнітивне перевантаження. Багатоепізодна злочинна діяльність, використання численних акаунтів, необхідність постійного контролю за технічними засобами приховування інформації створюють високий рівень психічного напруження [2]. В умовах перевтоми або дефіциту часу особа може помилково активувати геолокацію, випадково здійснити вхід без використання VPN, переплутати акаунти або залишити у відкритому доступі файли з персональною інформацією. Такі помилки є типовими для організованих злочинних угруповань, учасники яких здійснюють тривалу координацію дій через цифрові засоби зв’язку.

Когнітивні викривлення особливо помітні у поведінці осіб, які намагаються приховати сліди злочину після його вчинення. На стадії посткримінальної поведінки правопорушник часто діє в умовах стресу, страху викриття та емоційного напруження, що істотно знижує здатність до раціонального мислення. У таких умовах виникає ефект тунельного мислення, коли особа концентрується лише на окремих аспектах ситуації та ігнорує інші загрози. Наприклад, знищуючи повідомлення у месенджері, правопорушник може не враховувати автоматичне резервне копіювання даних у хмарному сховищі або залишення метаданих на сервері провайдера. Аналогічно особа може видалити файл із комп’ютера, але не врахувати існування тимчасових копій, кешованих даних чи слідів активності у системних журналах.

У криміналістичному аспекті важливим є те, що когнітивні викривлення формують не хаотичні, а відносно закономірні поведінкові патерни. Саме це дозволяє прогнозувати можливі помилки правопорушника та будувати ефективні

алгоритми пошуку цифрових доказів. Наприклад, якщо встановлено, що особа активно використовує певний стиль комунікації або конкретні цифрові платформи, слідчий може припустити повторне застосування аналогічних моделей поведінки в інших епізодах діяльності. Аналіз цифрових слідів у поєднанні з поведінковим профілюванням дозволяє виявляти приховані зв'язки між окремими подіями, встановлювати роль учасників організованих груп та реконструювати механізм злочинної діяльності.

Особливого значення набуває дослідження когнітивних викривлень у контексті організованої кіберзлочинності. У межах злочинних угруповань формується колективна впевненість у власній невразливості, що сприяє нехтуванню заходами конспірації. Групове мислення нерідко призводить до ігнорування альтернативних точок зору та критичної оцінки ризиків. Учасники угруповання починають сприймати власну схему як безпечну та ефективну, що знижує рівень обережності. У результаті відбувається накопичення великої кількості цифрових слідів, пов'язаних із внутрішньою комунікацією, фінансовими операціями, координацією дій та розподілом ролей.

Когнітивні викривлення можуть проявлятися також у використанні соціальних мереж. Багато правопорушників схильні недооцінювати обсяг інформації, який вони добровільно публікують у відкритому доступі. Навіть за умови створення анонімних акаунтів вони можуть використовувати однакові фотографії, повторювані фрази, специфічний стиль написання текстів або характерні часові інтервали активності. Такі ознаки створюють цифровий поведінковий портрет особи. Сучасні методи криміналістичного аналізу дозволяють зіставляти ці дані між собою та виявляти приховані закономірності.

Важливим напрямом сучасної криміналістики є використання штучного інтелекту та систем аналітики великих даних для виявлення когнітивно обумовлених моделей поведінки у цифровому середовищі. Алгоритми машинного навчання здатні аналізувати великі обсяги інформації та встановлювати повторювані патерни дій, які можуть свідчити про діяльність конкретної особи або групи осіб. При цьому враховуються часові характеристики активності, особливості комунікації, структура соціальних зв'язків, способи використання технічних засобів та інші поведінкові маркери. Таким чином, когнітивні викривлення стають не лише об'єктом психологічного аналізу, а й важливим елементом сучасної цифрової криміналістики.

Окремої уваги заслуговує проблема взаємозв'язку когнітивних викривлень та інсценування цифрової активності. Деякі правопорушники намагаються навмисно створювати хибні цифрові сліди для введення в оману правоохоронних органів. Однак такі дії також супроводжуються когнітивними помилками. Особа може переоцінювати власну здатність моделювати поведінку іншого користувача або не враховувати технічні аспекти функціонування цифрових систем. Унаслідок цього штучно створені сліди нерідко містять суперечності, які дозволяють встановити факт інсценування. Наприклад, часові параметри активності,

географічна невідповідність IP–адрес, особливості цифрового підпису пристрою чи відмінності у стилі мовлення можуть свідчити про фальсифікацію даних.

Дослідження когнітивних викривлень у механізмі формування цифрових слідів має важливе практичне значення для підвищення ефективності розслідування кримінальних правопорушень. Розуміння закономірностей поведінки правопорушника дозволяє більш точно прогнозувати його дії, визначати ймовірні напрями пошуку доказів та формувати оптимальну тактику проведення гласних і негласних слідчих (розшукових) дій. Крім того, аналіз когнітивних аспектів цифрової поведінки сприяє розвитку криміналістичного профілювання та удосконаленню методик цифрової криміналістики.

Отже, когнітивні викривлення є важливим фактором, який впливає на механізм формування цифрових слідів злочинної діяльності. Помилки мислення, викликані надмірною впевненістю, ілюзією контролю, когнітивним перевантаженням, ефектом підтвердження та іншими психологічними чинниками, безпосередньо відображаються у цифровому середовищі та формують систему криміналістично значущої інформації. Саме тому сучасна криміналістика повинна розглядати цифрові сліди не лише як технічний результат функціонування інформаційних систем, а і як поведінкове відображення психічної діяльності правопорушника. Комплексне поєднання цифрової криміналістики, психології та поведінкового аналізу створює передумови для підвищення ефективності протидії сучасній злочинності та вдосконалення методів виявлення, фіксації й аналізу цифрових доказів.

Перелік використаних джерел:

1. Караман К. В. Виявлення цифрових слідів: особливості й алгоритм. Вісник Харківського національного університету внутрішніх справ. 2025. Вип. 3 (110). С. 141–150.

2. Авдєєва Г. К. Сутність цифрових слідів в криміналістиці. Актуальні питання судової експертизи та криміналістики : зб. матеріалів міжнар. наук.–практ. конфер., присвяч. 95–річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90–93.

DOI https://doi.org/10.32837/11300.33556

Шанигін Антон
доктор філософії з медицини, доцент,
кафедри гігієни, медичної екології та громадського здоров'я
Одеського національного медичного університету,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–2644–4542
e–mail: anton.shanyhin@onmedu.edu.ua

Волошина Владлена
кандидат юридичних наук, доцент, доцент кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–8772–4172
e–mail:vkvoloshyna@gmail.com

Аль–Файюми Халед
доктор філософії з кібербезпеки
Державний університет інтелектуальних технологій і зв'язку,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–4624–2569
e–mail:khaled@alfaiomi.com

ЦИФРОВІ ТЕХНОЛОГІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я: ВИКЛИКИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ МЕДИЧНИХ ДАНИХ

У тезах розглянуто сучасні виклики цифровізації системи громадського здоров'я, пов'язані із кібербезпекою та захистом медичних даних. Проаналізовано ризики використання цифрових медичних систем і штучного інтелекту, а також правові механізми захисту персональної інформації.

Ключові слова: цифровізація, громадське здоров'я, кібербезпека, медичні дані, штучний інтелект.

Shanyhin Anton
PhD in Medicine, Associate Professor, of the
Department of Hygiene, Medical Ecology and Public Health,
Odesa National Medical University,
Odesa, Ukraine

Voloshyna Vladlena
Candidate of Law, Associate Professor, Associate Professor of the
Department of Criminal Procedure,
National University «Odesa Law Academy»,
Odesa, Ukraine

Al–Faiyomi Khaled
PhD in Cybersecurity, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine

DIGITAL TECHNOLOGIES IN PUBLIC HEALTH: CHALLENGES OF CYBERSECURITY AND PROTECTION OF MEDICAL DATA

The theses examine current challenges of digitalization in the public health system related to cybersecurity and protection of medical data. The risks associated with digital medical systems and artificial intelligence, as well as legal mechanisms for personal data protection, are analyzed.

Key words: digitalization, public health, cybersecurity, medical data, artificial intelligence.

The modern public health system is characterized by the active implementation of digital technologies, including artificial intelligence, Big Data, telemedicine, cloud services, and the Internet of Medical Things (IoMT) [1, p. 36; 2, p. 258]. Digitalization contributes to the automation of medical processes, improvement of epidemiological monitoring, and increased accessibility of healthcare services, particularly under the conditions of the COVID–19 pandemic and martial law [2, p. 256; 3, p. 215].

In Ukraine, healthcare digitalization is being implemented through the development of the national eHealth system, electronic prescriptions, medical information systems, and telemedicine services [2, p. 258]. At the same time, the expansion of digital infrastructure is accompanied by increasing cybersecurity risks, since healthcare systems accumulate large volumes of confidential information, including personal identifiers, clinical records, laboratory results, genetic, and financial data [2, p. 259; 4, p. 64].

Medical information belongs to the category of highly sensitive data, and its compromise may lead to discrimination, insurance fraud, blackmail, and violations of patients' rights [5, p. 42]. A particularly dangerous threat is the modification of clinical information, which may result in diagnostic and treatment errors. In recent years, additional risks have emerged due to the use of artificial intelligence technologies. Among the most significant threats are deepfake technologies and Prompt Injection attacks aimed at manipulating AI algorithms and obtaining unauthorized access to confidential information through medical chatbots or digital assistants.

The scale of cybersecurity threats in healthcare is confirmed by several global cyber incidents. One of the largest attacks targeted Change Healthcare in the United States in 2024, affecting the data of more than 100 million individuals and temporarily disrupting a significant part of the healthcare system [2, p. 262]. Significant consequences were also caused by cyberattacks on the Ascension hospital network, the

MediSecure data breach in Australia, and the WannaCry attack, which seriously disrupted the operation of hospitals in the United Kingdom [6].

For Ukraine, cybersecurity of medical infrastructure has strategic importance under conditions of war, as cyberattacks are increasingly combined with attacks on critical infrastructure facilities [7, p. 497]. Disruptions of healthcare information systems may result in delays in medical care, reputational losses, and threats to patients' lives [7, p. 496].

Legal regulation of medical data protection in Ukraine is based on the Law of Ukraine «On Personal Data Protection», the Law of Ukraine «On Protection of Information in Information and Communication Systems», and international legal instruments [8; 9]. An important direction of legislative development is harmonization with the requirements of the European Union General Data Protection Regulation (GDPR), which establishes high standards for personal data processing and protection [10].

Particular attention is currently paid to the regulation of artificial intelligence in medicine. The European Union AI Act defines medical AI systems as high–risk technologies and establishes mandatory requirements regarding algorithm transparency, human oversight, and safety assessment [11]. International organizations also emphasize the implementation of the principles of «Security by Design» and «Privacy by Design», according to which cybersecurity mechanisms should be integrated into digital systems from the earliest stages of development.

Therefore, digitalization of public health creates significant opportunities for improving healthcare accessibility and efficiency; however, it is simultaneously associated with substantial cybersecurity risks. Ensuring cyber resilience of healthcare infrastructure, improving legal regulation, and increasing digital literacy among healthcare professionals are essential conditions for the safe development of digital medicine.

List of sources used:

1. Bachuk O. Digital transformation in the health care system. Odesa National University Herald. Economy. 2024. Vol. 29, 3(101). c. 36–41 URL: https://doi.org/10.32782/2304–0920/3–101–6

2. Романенко С. В. Впровадження електронної медицини в управлінні медичними закладами: переваги та виклики. Інвестиції: практика та досвід. 2025. № 4. с. 256–264. URL: https://doi.org/10.32702/2306–6814.2025.4.256

3. Опанасюк М. Світові тенденції цифрової трансформації системи охорони здоров'я як об'єкта публічного управління. Економіка, управління та адміністрування. 2026. № 1(115). с. 212–222. URL: https://doi.org/10.26642/ema–2026–1(115)–212–222

4. Security of medical cyber–physical systems. Bulletin of V.N. Karazin Kharkiv National University, series «Mathematical modeling. Information technology.

Automated control systems». 2025. No. 66. P. 63–72. URL: https://doi.org/10.26565/2304–6201–2025–66–06

5. Bryhinets O. Legal security of protection personal data in the field of health care. Economics. Finances. Law. 2024. Vol. 5/2024, no. –. P. 41–43. URL: https://doi.org/10.37634/efp.2024.5.8

6. A retrospective impact analysis of the WannaCry cyberattack on the NHS / S. Ghafur et al. npj Digital Medicine. 2019. Vol. 2, no. 1. URL: https://doi.org/10.1038/s41746–019–0161–6

7. Tokarieva K. S. The problem of personal data protection in the field of health protection in the conditions of informatization. Juridical scientific and electronic journal. 2022. No. 11. P. 496–499. URL: https://doi.org/10.32782/2524–0374/2022–11/120

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297–VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297–17#Text

9. Про захист інформації в інформаційно–телекомунікаційних системах : Закон України від 05.07.1994 № 80/94–ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94–%D0%B2%D1%80#Text

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. URL: https://eur–lex.europa.eu/eli/reg/2016/679/oj

11. Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI News European Parliament. URL: https://www.europarl.europa.eu/news/en/press–room/20231206IPR15699/artificial–intelligence–act–deal–on–comprehensive–rules–for–trustworthy–ai

Секція 3
ЕКСПЕРТНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У КІБЕРПРОСТОРІ ТА ВИКОРИСТАННЯ ВІРТУАЛЬНИХ АКТИВІВ

DOI https://doi.org/10.32837/11300.33545

Величко Юлія
старший судовий експерт Науково–дослідного центру незалежних судових експертиз Міністерства юстиції України,
м. Київ, Україна
ORCID: https://orcid.org/0009–0008–3642–7977
e–mail: yuliiavelychko7@gmail.com

ПЕРСПЕКТИВИ ПРОВЕДЕННЯ СУДОВИХ ЕКОНОМІЧНИХ ЕКСПЕРТИЗ ТА ДОСЛІДЖЕНЬ З ПИТАНЬ ДЕКЛАРУВАННЯ ТА ОПОДАТКУВАННЯ ДОХОДІВ ФІЗИЧНИХ ОСІБ, ОТРИМАНИХ ВІД ВІРТУАЛЬНИХ АКТИВІВ

У тезах розглянуто статистику використання фізичними особами – резидентами України віртуальних активів (криптовалюти). Проаналізовано нормативно–правові та законодавчі акти, а також законопроєкти, що розглядаються Верховною Радою України, з питань регулювання ринку віртуальних валют та оподаткування доходів за операціями з купівлі–продажу криптоактивів. Змодельовано потенційні напрями дослідження в межах судових економічних експертиз з врахуванням напрямів регулювання ринку криптоактивів.

Ключові слова: віртуальні активи, криптоактиви, оподаткування доходів, судова економічна експертиза, напрями економічних досліджень.

Velychko Yuliia
Senior Forensic Expert of the Scientific research center of independent forensic of the Ministry of justice of Ukraine,
Kyiv, Ukraine

PROSPECTS FOR CONDUCTING FORENSIC ECONOMIC EXPERTISE AND RESEARCH ON THE ISSUES OF DECLARING AND TAXING INCOME OF INDIVIDUALS OBTAINED FROM VIRTUAL ASSETS

The theses consider statistics on the use of virtual assets (cryptocurrencies) by individuals – residents of Ukraine. The regulatory and legislative acts, as well as draft laws considered by the Verkhovna Rada of Ukraine, on the regulation of the virtual currency market and taxation of income from transactions on the purchase and sale of crypto assets are analyzed. Potential areas of research within the framework of forensic

economic examinations are modeled, taking into account the areas of regulation of the crypto asset market.

Key words: virtual assets, cryptoassets, income taxation, forensic economic expertise, areas of economic research.

Відповідно до статистичної інформації, наявної у відкритих джерелах даних, Україна входить до числа країн–лідерів за масштабами використання криптовалюти.

Зокрема, відповідно до Звіту «Регіональні економічні перспективи» Європейського банку реконструкції та розвитку, опублікованого у вересні 2025 року [1] наведено наступну інформацію:

–більше 10% українців володіли криптовалютою у 2023 році;

–з липня 2023 року по липень 2024 року надходження криптовалюти в Україну становили 106 млрд доларів при витратах на придбання біткоіна орієнтовно на суму 882 млн доларів (за оцінкою ЄБРР).

Також, відповідно до статті американської аналітичної компанії Chainalysis «Глобальний індекс впровадження 2024 року: регіон Центральної та Південної Азії та Океанії (CSAO) лідирує у світі за рівнем глобального впровадження криптовалюти» від 11.09.2024р. [2], Україна займала 6–те місце в світі за рівнем впровадження криптовалют у 2024 році після таких країн, як Індія, Нігерія, Індонезія, США та В'єтнам.

Крім того, відповідно до результатів опитування, проведеного міжнародною компанією Ipsos та криптобіржею WhiteBIT, опублікованого 24.09.2025р. ресурсом Incrypted [3], криптовалюти увійшли до п'ятірки найбільш популярних фінансових інструментів в Україні поряд із банківськими рахунками, депозитами та нерухомістю.

Згідно з опитуванням, для багатьох українців криптовалюти вже не є виключно інструментом трейдингу. Найбільш поширені сценарії використання цифрових активів такі:

трейдинг – 57%;

довгострокове зберігання активів – 52%;

захист заощаджень від інфляції – 51%;

щоденні фінансові операції та перекази [3].

Також, за даними Національного агентства з питань запобігання корупції (НАЗК), відповідно до інформації, наведеної в Щорічних деклараціях осіб, уповноважених на виконання функцій держави або місцевого самоврядування, прослідковується тенденція до зростання кількості криптоактивів у декларантів, а саме за період 2022–2024 роки декларувались наступні показники:

–у 2022 році криптоактиви – у 1320 деклараціях на суму 371 млн грн;

–у 2023 році криптоактиви – у 1710 деклараціях на суму 526 млн грн;

–у 2024 році криптоактиви – у 2200 деклараціях на суму 786 млн грн.

Метою використання криптоактивів, виходячи з тенденцій ринку віртуальних активів, є напрямки: зберігання коштів в криптовалюті; проведення розрахунків; отримання доходу від інвестування за результатами операцій купівлі–продажу.

Згідно з положеннями Розділу IV. ПОДАТОК НА ДОХОДИ ФІЗИЧНИХ ОСІБ Податкового кодексу України від 02.12.2010р. №2755–VI [4] визначено, що:

–платниками податку на доходи фізичних осіб є фізичні особи–резиденти, які отримують доходи як з джерела їх походження в Україні, так і іноземні доходи (ст.162);

–об'єктом оподаткування є загальний місячний (річний) оподатковуваний дохід та доходи з джерела їх походження в Україні, які остаточно оподатковуються під час їх нарахування (виплати, надання) (ст.163);

Відповідно до положень статей Кодексу, а саме ст. 164, пп 166.2.1. п. 166.1 ст. 166, п.16[1] підрозділу 10 розділу XX передбачена база оподаткування доходу та податкові знижки, а також порядок оподаткування доходів фізичних осіб військовим збором.

Станом на зараз, положення податкового законодавства України не містять чіткого алгоритму щодо оподаткування доходів, що виникають від операцій з віртуальними активами.

У вересні 2025 року Верховна Рада України прийняла у першому читанні законопроєкт №10225–д, яким пропонується легалізувати володіння та операції з криптовалютами. Відповідно до законопроєкту, визначається роль віртуальних активів, регламентування роботи ринку криптоактивів та порядок їх оподаткування.

Відповідно до даних офіційного сайту Верховної Ради України [5], метою законопроекту є створення правової основи для регулювання обороту віртуальних активів в Україні, забезпечивши їх легальне використання, оподаткування та захист прав учасників ринку.

Також, між Міжнародним валютним фондом та Україною укладено Меморандум (програму) щодо розширеного фінансування України на 2026–2029 роки МВФ, яка 26.02.2026 була затверджена Радою виконавчих директорів МВФ.

Пунктом 21 Меморандуму визначено обов'язок до ухвалення Верховною Радою України у 2026 році пакету податкових заходів, зокрема, щодо оподаткування доходів, отриманих через цифрові платформи.

Таким чином, на сьогодні в Україні розробляються відповідні законодавчі та нормативно–правові акти щодо регулювання ринку криптоактивів, в тому числі з подальшим оподаткуванням доходів фізичних осіб, що отримується від таких операцій.

Згідно з положеннями розділу III Науково–методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, затверджених Наказом Міністерства юстиції України №53/5 від 08.10.1998р. [6],

одним з напрямків досліджень (завданнями) при проведенні судових економічних експертиз та економічних досліджень є наступне:

–документальної обґрунтованості окремих елементів податків та зборів, визначених платником у відповідних деклараціях (розрахунках, звітах).

Таким чином, при внесенні відповідних змін до податкового законодавства та визначення порядку оподаткування доходів фізичних осіб, що отримуються від операцій з криптоактивами, показники, що декларуються суб'єктами декларування, також у випадку необхідності можуть бути предметом дослідження судових економічних експертиз та економічних досліджень.

Положеннями законопроєктів визначено декларування власником криптоактивів такого майна та сплати податків, виходячи не з факту володіння активами, а із прибутку, що виникає за результатами звітного року.

Тобто, підсумовуючи вищевикладене, напрямами дослідження при проведенні економічних експертиз будуть наступні:

–дослідження документальної обґрунтованості об'єкту оподаткування та розміру задекларованого і сплаченого до бюджету податку на доходи фізичних осіб та військового збору за операціями з купівлі–продажу криптоактивів за результатами звітного податкового періоду (року);

–дослідження витрат, понесених платником податків на придбання криптоактиву на підставі розрахункових документів;

–дослідження доходу, отриманого платником податків від реалізації криптоактиву за результатами «виходу у фіат» – продажу за звичайні (не цифрові) гроші;

–дослідження різниці між доходами та витратами (прибутку) у гривневому еквіваленті.

Також, в окремих випадках, з метою забезпечення вихідних даних для проведення економічних експертиз (інформація про рух активів та коштів на електронних гаманцях), попередньо можливими є проведення експертиз з інших галузей знань, зокрема, комп'ютерно–технічних.

Враховуючи вищевикладене, станом на зараз є можливим окреслення потенційних напрямів економічних досліджень та судових економічних експертиз, що будуть проводитися в рамках судових справ та досудових розслідувань з питань повноти декларування та сплати податків фізичними особами за результатами операцій з купівлі–продажу віртуальних активів, при відповідному затвердженні органами законодавчої влади України законів та змін до податкового законодавства.

Перелік використаних джерел:

1.Звіт: «Regional economic prospects» European Bank for Reconstruction and Development. September 2025. Режим доступу: https://www.ebrd.com/home/news–and–events/publications/economics/rep/under–pressure.html.

2.Стаття Chainalysis: The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption. 11.09.2024. Режим доступу: https://www.chainalysis.com/blog/2024–global–crypto–adoption–index/.

3.Стаття Incrypted: Криптоактиви увійшли у топ–5 інвестицій фінансово активних українців – дослідження. 24.09.2025. Режим доступу: https://incrypted.com/ua/kryptoaktyvy–uvijshly–u–top–5–investytsij–finansovo–aktyvnyh–ukrajintsiv–doslidzhennja/.

4.Податковий кодекс України від 02.12.2010р. №2755–VI. Режим доступу: https://zakon.rada.gov.ua/laws/show/2755–17#Text.

5.Результати засідання Комітету з питань цифрової трансформації. Прес–служба Апарату Верховної Ради України. 19.08.2025р. Режим доступу: https://www.rada.gov.ua/news/news_kom/265061.html.

6.Науково–методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень, затверджені Наказом Міністерства юстиції України №53/5 від 08.10.1998р. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0705–98#Text.

DOI https://doi.org/10.32837/11300.33547

Возняк Олег
кандидат технічних наук (PhD), доцент,
провідний науковий співробітник лабораторії залізнично–транспортних досліджень, судовий експерт 2–го класу Львівського науково–дослідного інституту судових експертиз, доцент кафедри транспортних технологій Національного університету «Львівська політехніка»,
м. Львів, Україна,
ORCID: https://orcid.org/0000–0002–7163–9026,
e–mail: ovozom@gmail.com

ОСОБЛИВОСТІ ПРОВЕДЕННЯ КОМПЛЕКСНИХ ЕКСПЕРТИЗ ЗТП НА ПЕРЕЇЗДАХ: НОРМАТИВНО–ТЕХНІЧНИЙ ПОГЛЯД ЕКСПЕРТА–ЗАЛІЗНИЧНИКА

Анотація: Досліжено специфіку проведення експертиз залізнично–транспортних пригод. Виявлено нормативну колізію між ПДР та нормативними документами, що застосовуються на залізничному транспорті. Обґрунтовано авторську модель контролю переїздів.

Ключові слова: залізничний переїзд, залізнично–транспортна експертиза, колізія, автоматика, безпека руху, транспортні технології.

Voznyak Oleh
Candidate of Technical Sciences (PhD), Associate Professor,
Leading Researcher of the Laboratory of Railway Transport Research, 2nd Class Forensic Expert of the Lviv Scientific Research Institute of Forensic Science,
Associate Professor of the Transport Technologies Department of the Lviv Polytechnic National University,
Lviv, Ukraine

FEATURES OF CONDUCTING COMPREHENSIVE FORENSIC EXAMINATIONS OF RAILWAY ACCIDENTS AT CROSSINGS: A REGULATORY AND TECHNICAL PERSPECTIVE OF A RAILWAY EXPERT

The specifics of conducting forensic examinations of railway traffic accidents are investigated. A regulatory conflict between traffic rules and regulatory documents applied in railway transport is identified. The author’s crossing control model is substantiated.

Key words: railway crossing, railway transport expertise, conflict, automation, traffic safety, transport technologies.

Вступ та актуальність проблеми. Залізнично–транспортні пригоди (ЗТП) на перетинах залізничних колій та автомобільних доріг в одному рівні, традиційно належать до категорій транспортних подій із найважчими наслідками. Статистичні дані свідчать про те, що понад 90% аварій на залізничних переїздах стаються внаслідок безпосереднього порушення водіями транспортних засобів Правил дорожнього руху (ПДР) України, зокрема в частині ігнорування заборонних сигналів автоматичної сигналізації, об'їзду закритих шлагбаумів або виїзду на колії в умовах затору [5, с.8–11].

Повне, всебічне та об'єктивне розслідування таких подій, а також розгляд відповідних судових справ вимагають залучення високоспеціалізованих експертних знань. Особливе місце у цьому процесі посідає судова залізнично–транспортна експертиза. Специфіка процесуального статусу експерта–залізничника полягає в тому, що він досліджує інфраструктурні елементи, параметри руху поїзда та алгоритми роботи автоматики, оцінюючи подію з позиції суворих залізничних нормативів, а не лише загальних дорожніх правил [4, с. 128]. Рівень ризику безпосередньо залежить від класифікації об'єкта: нерегульовані переїзди мають найвищий ступінь небезпеки через відсутність активних загороджувальних систем.

Класифікація залізничних переїздів за рівнем ризику та експертний підхід. У межах інженерно–транспортного дослідження експерт–залізничник насамперед аналізує категорійність та тип облаштування переїзду, оскільки це визначає обсяг нормативних вимог до його утримання. Чинна класифікація поділяє переїзди на регульовані та нерегульовані [5, с.53]:

Регульовані переїзди, що обслуговуються черговим працівником. Вони характеризуються найнижчим відносним рівнем аварійності завдяки багаторівневим системам захисту (автоматичні шлагбауми, механізовані пристрої загородження переїзду, ручні сигнали чергового). Експертиза таких пригод включає обов'язкову правову та технічну оцінку дій чергового по переїзду: своєчасність увімкнення загороджувальної сигналізації для поїзда у разі виникнення перешкоди.

Регульовані переїзди без чергового працівника. Безпека на них повністю покладається на автоматичні системи сигналізації (світлофори, акустичні випромінювачі). Експертне дослідження концентрується на аналізі технічної надійності релейних або мікропроцесорних систем.

Нерегульовані переїзди. Вони позбавлені будь–яких автоматичних систем сповіщення і обладнуються виключно дорожніми знаками 2.2 «Проїзд без зупинки заборонено» та знаками наближення. Вони мають найвищий рівень ризику, а експертиза в таких випадках зводиться до детального вивчення умов видимості «поїзд–автомобіль» згідно з нормативними трикутниками видимості.

Дослідження часових параметрів автоматики та авторський внесок. Одним із ключових завдань експертизи є перевірка часових параметрів залізничної автоматики. Експерт здійснює аналіз визначення розрахункової довжини ділянки

наближення до залізничного переїзду, а також необхідного часу сповіщення про наближення поїзда. Залізнична автоматика повинна вмикати заборонні сигнали на переїзді щонайменше за 30–40 секунд до фактичного підходу поїзда до меж переїзду. Цей проміжок часу розраховується з умов гарантованого звільнення зони колій найдовшим і найповільнішим транспортним засобом, який міг розпочати рух через переїзд у момент увімкнення червоного світла світлофора.

У межах попередніх досліджень, результати яких викладено у кандидатській дисертації [6, с. 84], було запропоновано та науково обґрунтовано методи підвищення ефективності контролю рухомих одиниць безпосередньо у системах забезпечення безпеки на переїздах. Отримані результати доводять, що стандартні рейкові кола наближення в умовах сучасного коливання швидкостей поїздів не завжди забезпечують стабільний інтервал сповіщення. Це призводить або до невиправдано тривалого закриття переїзду (що часто провокує водіїв на порушення ПДР), або до критичного дефіциту часу для водія. Врахування розроблених нами підходів щодо автоматизованого усунення хибного зайняття рейкових кіл та оцінки схем автоматики [5, с. 242–250] дозволяє судовому експерту під час розслідування чітко виявити приховані випадки технічних збоїв логіки роботи пристроїв СЦБ (сигналізації, централізації та блокування).

Експертний аналіз пристроїв фіксації параметрів руху поїзда. Важливим етапом інженерного дослідження у практиці лабораторії залізнично–транспортних досліджень НДІСЕ є об’єктивне розшифрування швидкостемірних стрічок та сучасних комплексів КПД. На відміну від свідчень локомотивної бригади, які можуть мати суб’єктивний характер через стресовий стан, бортові самописці фіксують параметри руху поїзда абсолютно об’єктивно.

Експерт–залізничник здійснює детальне геометричне або комп’ютерне розкодування наступних параметрів:

Фактична швидкість руху поїзда безпосередньо перед аварією та в момент зіткнення;

Точна координата (кілометр та пікет) увімкнення машиністом звукового сигналу великої гучності (тифона);

Тиск у гальмівній магістралі локомотива, що дозволяє визначити темп розрядки гальмівної мережі;

Точний момент активації крана машиніста (положення екстреного гальмування) та використання піскоподачі для покращення зчеплення коліс із рейками.

Математичне моделювання та визначення моменту виникнення небезпеки. Особлива увага при проведенні експертизи приділяється визначенню моменту виникнення небезпечної транспортної ситуації (НТС) для машиніста локомотива. У контексті залізничних інструкцій НТС визначається не моментом виїзду автомобіля на переїзд (оскільки водій має право перетинати його, якщо сигналізація це дозволяє), а часом, коли дії водія явно стали не відповідати

вимогам ПДР або коли автомобіль через технічну несправність раптово зупинився в межах габариту рухомого складу. Саме з цього моменту необхідно оцінювати своєчасність дій локомотивної бригади щодо застосування гальм.

Враховуючи значний гальмівний шлях поїздів, який для вантажних складів вагою в кілька тисяч тонн зазвичай становить від 800 до 1200 метрів, залізничний експерт математично оцінює наявність або відсутність технічної можливості зупинки за кінематичною формулою:

(1)

де – повний гальмівний шлях поїзда (м));

– швидкість поїзда на момент переведення крана машиніста в гальмівне положення (м/с);

– час спрацьовування гальмівної системи локомотива та поширення гальмівної хвилі по составу (с);

– величина середнього уповільнення поїзда з урахуванням ухилу колії та типу гальмівних колодок (м/с2).

Паралельно, за методикою, викладеною у [5, с. 89–102], розраховується час, який був необхідний автомобілю для безпечного звільнення зони колій.

Співвідношення цих параметрів дозволяє чітко розмежувати поняття об’єктивної неминучості зіткнення та професійності дій машиніста, виключаючи безпідставні звинувачення на адресу локомотивної бригади.

Аналіз інфраструктурних чинників уповільнення та нормативна колізія. Ключовим аспектом судово–експертного дослідження є розкриття природи системної нормативної дисоціації між стандартами проєктування залізничної інфраструктури та діючими ПДР. При розрахунку мінімальної довжини ділянки наближення поїзда до переїзду інженери–проєктувальники залізниць керуються відомчою Інструкцією з улаштування та експлуатації залізничних переїздів [1]. На сучасному етапі цей документ закладає у математичну модель розрахункову швидкість руху автомобіля через переїзд на рівні 8 км/год, тобто приблизно 2,2 м/с. Варто зауважити, що у попередніх відомчих редакціях інструкції цей параметр був ще жорсткішим і становив усього 5 км/год.

Проте експертна практика доводить, що реальна небезпека криється не у потенційному перевищенні водіями цієї швидкості, а, якраз навпаки – у вимушеному критичному уповільненні транспортного засобу безпосередньо на настилі залізничного переїзду. Найпоширенішою причиною цього може служити незадовільний експлуатаційний стан покриття проїжджої частини настилу (наявність глибоких вибоїн, руйнування асфальтового полотна або критичні напливи біля рейок). Водій важковагового автопоїзда, довгомірного автобуса чи автобуса міського типу з низькою посадкою змушений знижувати швидкість для збереження вантажу чи цілісності підвіски та уникнення зупинки ТЗ на рейко–шпальній решітці.

Коли фактична швидкість перетину падає нижче 8 км/год, реальний час перебування автомобіля у габариті рухомого складу залізничного транспорту

суттєво перевищує розрахунковий час сповіщення, закладений алгоритмами автоматики СЦБ. Як наслідок, водій, який абсолютно законно в'їхав на переїзд за відсутності заборонних сигналів, стає заручником ситуації коли автоматика вмикається і закриває переїзд безпосередньо під час його повільного руху, штучно створюючи аварійну ситуацію.

У судово–експертній практиці це вимагає від експерта–залізничника проведення детального трасологічного та технічного аналізу. Моделювання критичних умов руху довгоскладових автотранспортних засобів, яке описане в нашій монографії [5, с. 210], доводить, що залізнична інфраструктура має оцінюватися комплексно. Проблема не в тому, що водії прагнуть проїхати швидше, а в тому, що зниження ними швидкості перетину переїзду позбавляє їх технічної можливості завершити маневр у розрахункові часові ліміти. Це вимагає обов'язкового переходу від фіксованих параметрів наближення до динамічних адаптивних систем контролю безпеки, розглянутих у дисертаційному дослідженні.

Висновки. Комплексна судова експертиза залізнично–транспортних пригод на переїздах не може обмежуватися виключно констатацією порушення водієм вимог дорожніх знаків чи світлофорів. Професійний підхід експерта–залізничника вимагає детального аналізу логіки роботи пристроїв СЦБ, точного дешифрування засобів об'єктивного контролю параметрів руху локомотива, дії локомотивної бригади, водія авто та врахування міжвідомчих нормативних парадоксів. Впровадження інтелектуальних систем моніторингу та фото– відеофіксації, запропонованих у наших наукових працях, дозволить мінімізувати вплив людського чинника та забезпечити експертів і органи досудового розслідування беззаперечною та об'єктивною доказовою базою.

Перелік використаних джерел:

1.Про затвердження Інструкції з улаштування та експлуатації залізничних переїздів : Наказ Міністерства транспорту та зв'язку України від 26.01.2007 № 54. URL: https://zakon.rada.gov.ua/laws/show/z0162–07

2.Положення про класифікацію транспортних подій на залізничному транспорті : Наказ Міністерства інфраструктури України від 03.07.2017 № 235. URL: https://zakon.rada.gov.ua/laws/show/z0904–17

3.Правила дорожнього руху : Постанова Кабінету Міністрів України від 10.10.2001 № 1306. URL: https://zakon.rada.gov.ua/laws/show/1306–2001–п

4.Основи судової експертизи: навч. посіб. / Л.М. Головченко, А.І. Лозовий, Е.Б. Сімакова–Єфремян та ін. Харків: Право, 2016. 928 с.

5.Возняк, О. М. Забезпечення безпеки руху на залізничних переїздах : Монографія / О. М. Возняк, В. І. Гаврилюк; за заг. ред. В. І. Гаврилюка ; Дніпров. нац. ун–т залізн. трансп. ім. акад. В. Лазаряна. Дніпро: ДНУЗТ, 2019. 282 с. ISBN 978–966–8471–89–6.

6.Возняк О. М. Підвищення ефективності контролю рухомих одиниць у системах безпеки на залізничних переїздах : дис. ... канд. техн. наук: 05.22.20 / О. М. Возняк ; Дніпропетр. нац. ун–т залізн. трансп. ім. акад. В. Лазаряна. Дніпро, 2017. 179 с.

DOI https://doi.org/10.32837/11300.33549

Голова Інна
здобувач 3 рівня освіти
Національного транспортного університету за спеціальністю 051 «Економіка»,
заслужений економіст України,
начальник відділу Центру судових і спеціальних експертиз
Українського науково–дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
м. Київ, Україна
ORCID: https://orcid.org/0000–0001–9717–7109
e–mail: inna.golova@gmail.com

Мензул Оксана
судовий експерт відділу Центру судових і спеціальних експертиз
Українського науково–дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
м. Київ, Україна
e–mail: bellaleksa@ukr.net

ВИЗНАЧЕННЯ ВАРТОСТІ ПОСЛУГ У СУДОВІЙ ЕКСПЕРТИЗІ

У тезах розглянуто проблему визначення вартості послуг при проведенні судових експертиз. Проаналізовано чинну нормативно–правову базу оцінки вартості як в Україні так і на прикладі Міжнародних та Європейських стандартів оцінки.

Ключові слова: послуга, товар, методи оцінки, калькуляція витрат, ціноутворення.

Inna Holova
Third-cycle higher education applicant at the National Transport University, Specialty 051 «Economics»,
Honored Economist of Ukraine,
Head of Department at the Center for Forensic and Special Examinations of the Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine,
Kyiv, Ukraine

Menzul Oksana
Forensic Expert at the Department of the Center for Forensic and Special Examinations of the Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine,
Kyiv, Ukraine

DETERMINING THE COST OF SERVICES IN FORENSIC EXPERTISE

The paper addresses the issue of determining the cost of services provided in the course of forensic examinations. The current regulatory framework governing valuation in Ukraine is analysed and compared with the relevant International and European Valuation Standards.

Keywords: service, goods, valuation methods, cost calculation, pricing.

Стрімкий розвиток науки і техніки, глобалізація економік, пандемія COVID–19, а потім і війна в Україні спонукає як пересічних громадян так і судових експертів відходити від традиційних методів і підходів вирішення експертних завдань.

Цифровізація злочинів та доказів потребує від експертів у різних видах судових експертиз переходити на дослідження цифрових доказів: документів, які завірені ЕЦП, а не звичайним підписом із печатками, спілкування в рамках електронних систем тощо.

Відомо, що судова експертиза є вирішальним інструментом для забезпечення безпеки та цілісності системи правосуддя. В умовах глобалізації та євроінтеграційних процесів особливого значення набуває питання уніфікації методичних підходів та гармонізації національних стандартів судово–експертної діяльності з міжнародними нормами. Це зумовлено необхідністю забезпечення порівнянності результатів експертних досліджень, підвищення рівня довіри до висновків експертів та інтеграції української експертної практики у світовий професійний простір.

Процес визначення вартості об’єктів дослідження регламентується Законом України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» [1] (далі – Закон 2658).

Частиною 4 статті 4 Закону 2658 передбачено «Діяльність судових експертів, пов’язана з оцінкою майна, здійснюється на умовах і в порядку, передбачених Законом України «Про судову експертизу», з урахуванням особливостей, визначених цим Законом щодо методичного регулювання оцінки такого майна. При цьому у дослідницькій частині висновку судового експерта відображаються всі процедури, пов’язані з оцінкою майна, встановлені нормативно–правовими актами з оцінки майна. Інші положення цього Закону не поширюються на судових експертів.»

Статтею 9 Закону 2658 передбачено, що методичне регулювання оцінки майна здійснюється у відповідних нормативно–правових актах з оцінки майна: положеннях (національних стандартах) оцінки майна, що затверджуються Кабінетом Міністрів України, методиках та інших нормативно–правових актах, які розробляються з урахуванням вимог положень (національних стандартів) і затверджуються Кабінетом Міністрів України або Фондом державного майна України.

За Національними стандартом України №1, затверджений постановою КМУ від 10.09.2003 № 1440, статтею 3 передбачено:

«об'єкти оцінки – майно та майнові права, які підлягають оцінці. Об'єкти оцінки класифікують за різними ознаками, зокрема, об'єкти оцінки в матеріальній та нематеріальній формі, у формі цілісного майнового комплексу;

об'єкти оцінки у матеріальній формі – нерухоме майно (нерухомість) та рухоме майно;

об'єкти оцінки у нематеріальній формі – об'єкти оцінки, які не існують у матеріальній формі, але дають змогу отримувати певну економічну вигоду. До об'єктів у нематеріальній формі належать фінансові інтереси (частки (паї, акції), опціони, інші цінні папери та їх похідні, векселі, дебіторська і кредиторська заборгованість тощо), а також інші майнові права;

об'єкти оцінки у формі цілісного майнового комплексу (цілісний майновий комплекс) – об'єкти, сукупність активів яких дає змогу провадити певну господарську діяльність. Цілісними майновими комплексами є підприємства, а також їх структурні підрозділи (цехи, виробництва, дільниці тощо), які можуть бути виділені в установленому порядку в самостійні об'єкти з подальшим складанням відповідного балансу і можуть бути зареєстровані як самостійні суб'єкти господарської діяльності.»

За IVS (International Valuation Standards), оцінюється актив, який має економічну вигоду та може бути предметом права власності чи контролю (можуть бути ідентифіковані).

Отже, відповідно до нормативно–методичної бази України та з урахуванням положень міжнародних стандартів оцінки, до об'єктів дослідження в рамках товарознавчої експертизи можуть бути віднесені товари, сировина, обладнання та інші товари, які є активом з економічною вигодою.

При цьому товару притаманні певні функції, які він має виконувати: функціональна, ергономічна, функція надійності, ремонтопридатності тощо.

Процес ціноутворення об'єктів оцінки передбачає як врахування витрат на виробництво, маркетинг, так і аналіз ринкового середовища. Крім того, є законодавчо прийняті та нормативно обґрунтовані алгоритми визначення вартості товарів за витратним, порівняльним або дохідним підходом.

На відміну від товарів, які відносять до матеріальних об'єктів дослідження, послуги зазвичай не мають матеріальної складової.

Проте все частіше до вартості товарів додають невід'ємні від товару послуги щодо доставки, сервісного обслуговування, тощо.

Експертною практикою судових експертів Експертної служби Служби безпеки України доведено, що вартість товарів, які постачаються за державними замовленнями так і за звичайними господарськими договорами, включає як окрему статтю витрат витрати на доставку, шеф–монтаж, налагодження, сервісне обслуговування. При постачанні складного технологічного обладнання частина вище перелічених послуг мають характер обов'язкових.

Разом з тим, вартість зазначених послуг визначається особливостями товарів, які вони супроводжують при просуванні на ринок .

Розрахунок вартості цих послуг неможливо провести окремо від визначення вартості товарів, оскільки вони не надаються окремо від товару та потребують дотримання умов, які висуває до них товар, що є об'єктом дослідження.

Визначення якості послуг впливає на їх вартість, але не дозволяє застосувати до визначення якості органолептичні, лабораторні та інструментальні методи.

Чинна нормативно–методична база як в Україні так і за її межами не дозволяє застосовувати стандартні методичні підходи до вартості послуг, а отже потребує напрацювання окремих алгоритмів визначення вартості послуг.

Перелік використаних джерел:

1.Закон України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» від 12.07.2001 № 2658–III. URL: https://zakon.rada.gov.ua/laws/show/2658–14/ed20010712#Text

2.Постанова Кабінету Міністрів України «Про затвердження Національного стандарту № 1 «Загальні засади оцінки майна і майнових прав» від 10.09.2003. № 1440. URL: https://zakon.rada.gov.ua/laws/show/1440–2003–%D0%BF#Text

3.Цивільний кодекс України від 16.01.2003 № 435–IV. URL: https://zakon.rada.gov.ua/laws/show/435–15/ed20030116#Text

4.Міжнародні стандарти оцінки (IVS, 2025).

DOI https://doi.org/10.32837/11300.33551

Дереча Андрій
судовий експерт Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України
м. Київ, Україна
ORCID: http://orcid.org/0009–0004–4966–1974,
e–mail: derechaandrej@gmail.com

Абросімов Тарас
судовий експерт Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерств юстиції України
м. Київ, Україна
ORCID: https://orcid.org/0009–0003–1270–9404,
e–mail: taras.abrosimov@gmail.com

СУЧАСНІ ПРОБЛЕМИ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У СУДОВОМУ ДОСЛІДЖЕННІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

У тезах розглянуто роль спеціальних знань у судовому дослідженні комп'ютерних злочинів в умовах цифровізації. Визначено особливості цифрових слідів та електронних доказів, їх динамічність, мінливість і значення для встановлення обставин правопорушень у цифровому середовищі. Визначено проблеми виявлення, фіксації та дослідження цифрової інформації, а також необхідність залучення спеціалістів і судових експертів для забезпечення належного використання доказової інформації у кримінальному провадженні.

Ключові слова: спеціальні знання, комп'ютерні злочини, цифрові сліди, електронні докази, судова комп'ютерно–технічна експертиза, цифровізація.

Derecha Andrii
forensic expert at the Kyiv Branch of the National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute» of the Ministry of Justice of Ukraine
Kyiv, Ukraine

Abrosimov Taras
forensic expert at the Kyiv Branch of the National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute» of the Ministry of Justice of Ukraine
Kyiv, Ukraine

CURRENT PROBLEMS OF USING SPECIAL KNOWLEDGE IN COURT EXAMINATION OF COMPUTER CRIMES UNDER CONDITIONS OF DIGITALIZATION

The theses examine the role of special knowledge in the forensic investigation of computer crimes under the conditions of digitalization. The specific features of digital traces and electronic evidence are identified, including their dynamic nature, variability, and significance for establishing the circumstances of offenses committed in the digital environment. The problems of detecting, recording, and examining digital information are defined, as well as the need to involve specialists and forensic experts to ensure the proper use of evidentiary information in criminal proceedings.

Keywords: special knowledge, computer crimes, digital traces, electronic evidence, forensic computer–technical examination, digitalization.

Настання епохи глобальної цифровізації та всеосяжне впровадження сучасних інформаційно–комунікаційних технологій у різні сфери суспільного життя – економічну, соціальну, управлінську тощо, як в Україні, так і за її межами, зумовили суттєві трансформації злочинної діяльності.

На сьогодні із застосуванням комп'ютерних засобів і систем вчиняються не лише злочини у сфері комп'ютерної інформації, а й правопорушення практично всіх категорій проти життя і здоров'я особи, власності, громадської безпеки тощо. До таких, зокрема, належать: несанкціоноване втручання в роботу електронно–обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, несанкціоновані дії з інформацією, яка оброблюється в електронно–обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї [1].

Встановлення та фіксування змісту веб–сайту (сторінки), інших місць збереження даних в мережі Інтернет, впровадження шкідливого програмного забезпечення, порушення права інтелектуальної власності таких об'єктів інтелектуальної власності (комп'ютерні програми, компіляції даних (бази даних) тощо), шляхом поширення недостовірної інформації, незаконна реклама та інші протиправні дії охоплюють сферу не лише кримінального, а й цивільного та адміністративного судочинства. Правове регулювання відповідних відносин здійснюється, зокрема, положеннями Цивільного кодексу України [2] та Кодексу адміністративного судочинства України [3].

Проблеми виявлення зазначених протиправних посягань мають транснаціональний характер, що зумовлено специфікою функціонування комп'ютерних систем і мереж, а також уніфікованими способами вчинення правопорушень у цифровому середовищі.

Стрімкий розвиток цифрових технологій обумовлює потребу у вдосконаленні методів судово–експертної діяльності, зокрема, щодо дослідження

цифрових доказів, що є необхідною умовою ефективної протидії сучасним формам злочинності. Використання цифрових технологій зумовлює появу нових видів криміналістично значимої інформації, що фіксується на електронних носіях, зокрема, специфічних об'єктів дослідження – цифрових слідів. Водночас слід зазначити, що в законодавстві України термін «цифрові докази» не використовується; натомість нормативно закріплено поняття «електронні докази». Так, відповідно до статті 99 Кодексу адміністративного судочинства України, електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (текстові документи, графічні зображення, плани, фотографії, відео– та звукозаписи тощо), веб–сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [3].

Проблеми використання спеціальних знань під час судового дослідження злочинів (правопорушень), пов'язаних із застосуванням цифрових технологій, що реалізуються через комп'ютерні засоби та системи, набувають особливої актуальності в умовах цифровізації суспільства.

Оскільки будь–які дії з використанням комп'ютерних систем і мереж залишають відображення у вигляді цифрових слідів в оперативній пам'яті комп'ютера, на носіях інформації різних типів, у лініях зв'язку та мережевому обладнанні, під час проведення слідчих (розшукових) дій необхідним є їх виявлення, фіксація та подальше надання експертам для дослідження.

Водночас в умовах функціонування глобальних комп'ютерних мереж отримання криміналістично значущої інформації ускладнюється тим, що вона може зберігатися на віддалених серверах, у тому числі, розташованих за межами держави. У таких випадках фізичне вилучення електронного носія інформації є фактично неможливим, що зумовлює необхідність застосування альтернативних процесуальних механізмів, зокрема, копіювання інформації або забезпечення доступу до неї. Крім того, транснаціональний характер кіберправопорушень проявляється у використанні розподіленої інфраструктури, коли шкідливе програмне забезпечення може функціонувати через сервери управління, розміщені у різних юрисдикціях, що істотно ускладнює їх виявлення та документування.

Цифровий слід – це криміналістично значима комп'ютерна інформація про події або дії, відображена в електронному (цифровому) середовищі на етапах її створення, обробки, зберігання та передачі, яка може бути виявлена, зафіксована й досліджена з метою встановлення обставин, що мають значення для кримінального провадження [4].

Цифрові сліди відзначаються динамічністю, схильністю до швидких змін, можливістю легкого видалення або модифікації, а також здатністю існувати у вигляді великої кількості ідентичних копій. Вони оперативно поширюються в комп'ютерних мережах і можуть бути доступними з будь–якої точки за умови підключення до мережі Інтернет. З урахуванням зазначених особливостей їх виявлення під час проведення огляду чи обшуку є ускладненим, оскільки такі процесуальні дії часто супроводжуються втручанням у роботу інформаційних систем, що може спричиняти зміну або втрату цифрової інформації. У зв'язку з цим навіть незначне зволікання з фіксацією виявлених цифрових слідів може призвести до їх безповоротної втрати.

Відповідно до вимог ст. 104, 107, 168 Кримінального процесуального кодексу України, у протоколі під час кримінального провадження можуть фіксуватися такі процесуальні дії: виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, та спосіб їх ідентифікації; застосовані технічні засоби фіксації процесуальної дії, умови та порядок їх використання; відомості про носії інформації, на які здійснювалося копіювання; характеристики електронних носіїв інформації; відомості про вилучення або копіювання інформації з електронних інформаційних систем чи їх частин; інші обставини, що мають значення для кримінального провадження [1].

Водночас, з огляду на специфіку цифрових слідів, самостійне виконання слідчим дій, пов'язаних з обробленням цифрової інформації без залучення спеціаліста, є ускладненим через недостатній рівень знань у сфері інформаційно–комунікаційних технологій. У той же час, навіть для кваліфікованих фахівців виконання таких дій іноді ускладнюється через недостатній рівень розробленості сучасних методик проведення судових експертиз щодо виявлення, фіксації та дослідження цифрових слідів.

Для ефективної роботи з цифровими слідами судові експерти повинні володіти сучасними інформаційно–комунікаційними технологіями. Водночас існує й інша проблема, що потребує вирішення. Об'єкти дослідження – цифрові сліди – у багатьох випадках надходять на експертне дослідження не на окремих носіях інформації, а безпосередньо містяться в комп'ютерних засобах і системах. У зв'язку з цим їх отримання потребує спеціальних знань у сфері судової комп'ютерно–технічної експертизи, а також, залежно від поставлених експерту питань, може бути призначена комплексна судова експертиза.

Так, на початковому етапі може бути проведена комп'ютерно–технічна експертиза з метою вилучення та фіксації цифрових слідів (наприклад, встановлення наявності програмного забезпечення, наприклад, української ІТ–компанії «СОФТМАКС», визначення її ліцензійності, а також походження масивів бухгалтерської інформації з установлення походження масивів даних (сформовані в межах функціонування програмного продукту або внесені до системи іншим способом). Подальше дослідження отриманих даних може здійснюватися в межах

інших видів судових експертиз, зокрема, економічної, щодо аналізу звітності, представленої у цифровому вигляді.

Судова комп'ютерно–технічна експертиза в Україні проводиться державними судово–експертними установами Міністерства юстиції України, Міністерства внутрішніх справ України, Служби безпеки України, а також судовими експертами, які не є фахівцями державних спеціалізованих установ. Зауважимо, що, зараз відбуваються засідання робочих груп з судових експертиз за участю всіх відомств щодо ухвалення єдиного документу – Методичних рекомендацій. Засідання проводяться з метою вироблення єдиних підходів до визначення об'єктів експертизи за видами (підвидами) судових експертиз, їх основних завдань та орієнтовного переліку питань у науково–методичних рекомендаціях щодо проведення судових експертиз (експертних досліджень).

Умови цифровізації зумовлюють зростання ролі спеціальних знань у судовому дослідженні комп'ютерних злочинів. Особливості цифрових слідів – їх динамічність, мінливість і транснаціональний характер – істотно ускладнюють процес виявлення та дослідження доказової інформації.

Чинне законодавство України частково адаптоване до потреб цифрового середовища, зокрема, передбачає можливість копіювання інформації без вилучення електронних носіїв, однак на практиці існує низка проблем, пов'язаних із обмеженими можливостями слідчих щодо самостійної роботи з цифровими доказами та необхідністю залучення спеціалістів і судових експертів.

Отже, подальший розвиток теоретичних засад і практичних методик використання спеціальних знань у сфері дослідження комп'ютерних злочинів, удосконалення нормативно–правового регулювання та підвищення рівня професійної підготовки фахівців є необхідними умовами підвищення ефективності судово–експертної діяльності в умовах цифровізації.

Перелік використаних джерел:

1. Кримінальний процесуальний кодекс України : Кодекс України; Закон, Кодекс від 13.04.2012 № 4651–VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text

2. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435–IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/435–15#Text

3. Кодекс адміністративного судочинства України : Кодекс України від 06.07.2005 № 2747–IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2747–15#Text

4. Коваленко В. В. Цифрові сліди у криміналістиці: поняття та значення // Вісник кримінального судочинства. 2019. № 2. С. 112–118.

DOI https://doi.org/10.32837/11300.33554

Дикий Олег
кандидат юридичних наук, доцент, доцент кафедри кримінального процесу,
декан факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID ID: https://orcid.org/0000–0000–0000–0000
e–mail: dikiy.oleg@onua.edu.ua

КІБЕРКРИМІНАЛІСТИКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ФАХОВОЇ ПІДГОТОВКИ СУЧАСНОГО ФАХІВЦЯ З БЕЗПЕКИ

Досліджено роль кіберкриміналістики у підготовці сучасних фахівців з безпеки. Розкрито значення цифрових доказів, кіберрозслідувань та криміналістичного аналізу цифрових слідів для формування професійних компетентностей.

Ключові слова: кіберкриміналістика, фахівець з безпеки, цифрові докази, цифрові сліди, кіберзлочинність, кібербезпека, професійна підготовка.

Dykyi Oleg
PhD in Law, Associate Professor, Associate Professor in the Department of Criminal Procedure, Dean of the Faculty of Cybersecurity and Information Technology
at the National University «Odesa Law Academy»,
Odesa, Ukraine

CYBERFORENSICS AS A KEY COMPONENT OF THE PROFESSIONAL TRAINING OF MODERN SECURITY SPECIALISTS

The role of cyber forensics in the training of modern security professionals has been examined. The importance of digital evidence, cyber investigations and the forensic analysis of digital traces for the development of professional competencies has been highlighted.

Key words: cyber forensics, security specialist, digital evidence, digital traces, cybercrime, cybersecurity, professional training.

Стрімка цифровізація суспільних відносин, розвиток інформаційно–комунікаційних технологій та активне впровадження цифрових сервісів у всі сфери життєдіяльності людини зумовлюють появу нових викликів у сфері забезпечення безпеки. Поряд із позитивними наслідками цифрової трансформації спостерігається зростання кількості кіберзлочинів, удосконалення способів несанкціонованого доступу до інформаційних ресурсів, використання шкідливого

програмного забезпечення, цифрового шахрайства, кібершпигунства, атак на критичну інфраструктуру та інших протиправних посягань у кіберпросторі. За таких умов особливого значення набуває підготовка висококваліфікованих фахівців з безпеки, які володіють сучасними знаннями та практичними навичками виявлення, дослідження, фіксації та аналізу цифрових слідів правопорушень. Важливе місце у формуванні таких компетентностей посідає кіберкриміналістика.

Кіберкриміналістика є відносно новим міждисциплінарним напрямом наукового знання, який сформувався на перетині криміналістики, інформаційних технологій, кібербезпеки, цифрової експертизи та кримінального процесу. Її основним призначенням є розроблення теоретичних положень, методів, засобів і технологій виявлення, фіксації, вилучення, дослідження та використання цифрової інформації як джерела доказових відомостей. На відміну від традиційної криміналістики, яка переважно працює з матеріальними слідами злочину, кіберкриміналістика зосереджується на цифрових слідах, що виникають у процесі використання комп'ютерних систем, мобільних пристроїв, мережевих ресурсів, хмарних сервісів та інших інформаційних технологій [1].

Сучасний фахівець з безпеки здійснює свою професійну діяльність у середовищі, де інформація стає одним із найцінніших ресурсів. Будь–яка діяльність організацій, підприємств, державних установ або громадян залишає значний обсяг цифрових даних, які можуть містити відомості про підготовку, вчинення чи приховування правопорушень. У зв'язку з цим виникає необхідність формування у майбутніх фахівців здатності працювати з цифровими доказами, аналізувати електронні документи, журнали подій, мережевий трафік, метадані файлів, інформацію з мобільних пристроїв та інших електронних носіїв. Саме кіберкриміналістика забезпечує методологічну основу для реалізації таких завдань.

Особливістю сучасної злочинності є те, що навіть традиційні кримінальні правопорушення дедалі частіше супроводжуються використанням цифрових технологій. Організовані злочинні групи активно застосовують зашифровані канали зв'язку, криптовалютні транзакції, анонімні мережі та цифрові платформи для координації своєї діяльності. Значна частина доказової інформації у таких провадженнях міститься саме в електронному вигляді. Відповідно, фахівець з безпеки повинен не лише розуміти принципи функціонування інформаційних систем, але й володіти навичками криміналістичного аналізу цифрових даних, встановлення джерел інформації та відтворення механізму вчинення протиправних дій у кіберпросторі.

Важливим аспектом підготовки майбутніх фахівців є формування розуміння природи цифрових слідів. На відміну від традиційних матеріальних слідів, цифрові сліди характеризуються високою мінливістю, можливістю швидкого знищення або модифікації, а також значною залежністю від технічних особливостей конкретних інформаційних систем. Це вимагає спеціальних знань

щодо порядку їх виявлення, документування та збереження. Помилки під час роботи з цифровими доказами можуть призвести до втрати цінної інформації або поставити під сумнів допустимість отриманих доказів у подальшому процесуальному використанні.

Кіберкриміналістика сприяє формуванню у здобувачів освіти системного мислення та здатності комплексно аналізувати інформаційні процеси. Дослідження кіберінцидентів потребує поєднання знань з різних галузей, зокрема програмування, комп'ютерних мереж, операційних систем, цифрової безпеки, криміналістики та права. У процесі навчання здобувачі набувають умінь здійснювати цифрову реконструкцію подій, встановлювати причинно–наслідкові зв'язки між окремими елементами кіберінциденту, виявляти приховані закономірності та прогнозувати можливі загрози безпеці.

Не менш важливим є практичний компонент підготовки. Ефективне опанування кіберкриміналістики неможливе без використання спеціалізованих програмних засобів та лабораторних комплексів. У процесі навчання здобувачі повинні працювати з інструментами цифрової експертизи, програмами аналізу мережевого трафіку, системами моніторингу подій інформаційної безпеки, засобами відновлення видаленої інформації та іншими сучасними технологіями. Практикоорієнтований підхід дозволяє сформувати професійні компетентності, необхідні для ефективного реагування на реальні кіберзагрози.

Особливої актуальності набуває кіберкриміналістична підготовка в умовах воєнного стану та гібридних загроз. Сучасні збройні конфлікти супроводжуються активним використанням кібероперацій, спрямованих на порушення функціонування державних інформаційних ресурсів, об'єктів критичної інфраструктури, фінансових систем та комунікаційних мереж [2]. Відповідно, фахівці з безпеки повинні бути готовими до виявлення наслідків кібератак, проведення цифрових розслідувань, збору доказової інформації та участі у відновленні порушених систем. У таких умовах кіберкриміналістика стає не лише навчальною дисципліною, а й важливим елементом національної безпеки.

Значну роль кіберкриміналістика відіграє у формуванні професійної культури майбутнього фахівця. Робота з цифровими доказами вимагає дотримання принципів законності, об'єктивності, наукової обґрунтованості та професійної етики. Майбутні фахівці повинні усвідомлювати відповідальність за результати своєї діяльності, розуміти правові наслідки помилок під час збору та аналізу цифрової інформації, а також забезпечувати захист персональних даних і конфіденційної інформації.

Важливою перевагою кіберкриміналістики є її універсальний характер. Набуті знання та навички можуть використовуватися не лише у правоохоронній діяльності, але й у сфері корпоративної безпеки, захисту інформаційних систем підприємств, аудиті інформаційної безпеки, реагуванні на кіберінциденти та проведенні внутрішніх розслідувань [3]. Це значно розширює можливості

професійної реалізації випускників та підвищує їх конкурентоспроможність на сучасному ринку праці.

Сучасні освітні програми підготовки фахівців з безпеки повинні передбачати інтеграцію кіберкриміналістики з іншими професійно орієнтованими дисциплінами. Ефективна підготовка можлива лише за умови комплексного поєднання знань з кібербезпеки, криміналістики, цифрової експертизи, інформаційного права, управління ризиками та захисту критичної інфраструктури. Такий міждисциплінарний підхід дозволяє сформувати фахівця нового покоління, здатного ефективно діяти в умовах стрімкого розвитку цифрових технологій та постійної еволюції кіберзагроз.

Таким чином, кіберкриміналістика є одним із ключових елементів фахової підготовки сучасного фахівця з безпеки. Її значення зумовлене зростанням ролі цифрових технологій у суспільстві, поширенням кіберзлочинності та необхідністю забезпечення належного рівня інформаційної безпеки. Формування у майбутніх фахівців знань і практичних навичок у сфері виявлення, дослідження та використання цифрових доказів сприяє підвищенню ефективності протидії сучасним загрозам, зміцненню національної безпеки та забезпеченню захисту інформаційного простору держави. Саме тому кіберкриміналістика повинна розглядатися не як допоміжний напрям підготовки, а як стратегічно важлива складова професійної компетентності сучасного фахівця з безпеки.

Перелік використаних джерел:

1. Shepitko V., Shepitko M. The Formation of Digital Criminalistics as a Strategic Direction for the Development of Science. *XVII Criminalistics and Forensic Expertology: Science, Studies, Practice. Abstracts of the XVII International Congress* (September 16–17, 2021). Bratislava, Slovak Republic, 2021. P. 187–198.

2. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika: XVIII, 2022. Т. 18. С. 31–37.

3. Заєць І.С. Перспективи криміналістики в умовах інформатизації суспільства. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід* : матеріали Міжнар. наук.–практ. круглого столу (Київ, 19 лют. 2020 р.). Київ : НАВС, 2020. С. 77–81.

DOI https://doi.org/10.32837/11300.33557

Євсюков Олександр
кандидат педагогічних наук, доцент,
провідний науковий співробітник Національного наукового центру
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»
Міністерства юстиції України,
м. Харків, Україна
ORCID: https://orcid.org/0000–0002–3554–8848,
e–mail: a.evsyukov1971@gmail.com

ЦИФРОВІ ОБ'ЄКТИ В СУДОВО–ЕКСПЕРТНИХ ДОСЛІДЖЕННЯХ

У тезах розглянута діяльність судового експерта при дослідженні цифрових об'єктів. З урахуванням постійного розвитку цифрових технологій наведено актуальність зазначених досліджень для більш повної міри реалізації ключових принципів об'єктивності та повноти досліджень у судово–експертній діяльності.

Ключові слова: судово–експертні дослідження, аналіз, цифрові об'єкти, цифрові технології, судовий експерт, експертиза.

Yevsiukov Oleksandr
Candidate of Pedagogical Sciences, Associate Professor,
Leading Researcher of the National Scientific Center «Institute of Forensic
Expertise named after Honored Prof. M. S. Bokarius»
of the Ministry of Justice of Ukraine,
Kharkiv, Ukraine

DIGITAL OBJECTS IN FORENSIC RESEARCH

The theses consider the activities of a forensic expert in the study of digital objects. Taking into account the constant development of digital technologies. the relevance of these studies for a more complete implementation of the key principles of objectivity and completeness of research in forensic research is presented.

Key words: forensic research; analysis, digital objects; digital technologies, forensic expert, examination.

Сучасні досягнення розвитку цифрових технологій сьогодні все більше впроваджуються в систему діяльності судових експертів, особливо в контексті досліджуваних матеріалів, що розширює можливості самої судово–експертної діяльності та сприяє підвищенню її ефективності. Зважаючи на це, основні складові сучасної судово–експертної діяльності сьогодні все більше і більше зазнають впливу цифровізації. Це призводить до суттєвого розширення доказової бази шляхом дослідження в ході судочинства сукупності одержуваної інформації, у тому числі отриманої під час оглядів цифрових пристроїв, комп'ютерної техніки,

соціальних мереж, сайтів, групових чатів тощо. Так само в наданих на дослідження матеріалах досліджується цифрова інформація, яка знаходиться в пам'яті мобільних пристроїв зв'язку або хмарних послуг.

Стосовно впливу розвитку цифрових технологій на українське суспільство взагалі та на судову експертну діяльність зокрема, повністю погоджуємось з Наталію Ткаченко, яка у своєму дослідженні зазначає: «Глобальна цифрова трансформація суспільства призвела до кардинальних змін у всіх ключових секторах діяльності юридичних і фізичних осіб та необхідності відповідного реагування з боку державних інституцій на нові умови цифрового середовища. Відбуваються такі процеси й у сфері правосуддя, де оновлюються традиційні підходи до збирання доказів, їх дослідження та оцінювання. За таких умов експертне забезпечення правосуддя в Україні набуває якісно нового змісту та значення, що реалізується шляхом його трансформування у високотехнологічний інструмент, який відіграє надзвичайно важливу роль у встановленні об'єктивних фактів та обставин у кримінальному, адміністративному, цивільному й господарському провадженнях, а також у процесах використання спеціальних знань поза межами судочинства» [1, с. 36].

З початком повномасштабного вторгнення країни агресора в Україну, в мережі Інтернет трапляються випадки поширення екстремістських матеріалів, спонукання як дорослих, так і неповнолітніх до протиправних проявів. У таких матеріалах декларуються ідеї, пов'язані зі спотворенням історичної пам'яті українського народу, руйнуванням традиційних духовних українських цінностей, нав'язуванням сторонніх цінностей, сепаратизмом тощо. Тобто з 2022 року актуальними об'єктами судової експертизи в Україні, які також представляються на дослідження в цифровій формі, є інформаційні матеріали пропагандистського та агітаційного характеру. Все це свідчить про нові способи вчинення злочинів, інформація про які зберігається в електронному вигляді.

Як зазначають у своєму дослідженні Юлія Браїлко, Тетяна Єгорова, Наталія Кисла та Патвакан Восканян: «До актуальних викликів і загроз національній безпеці України належать також загрози в інформаційній сфері. У Стратегії інформаційної безпеки зазначено, що інформаційна безпека є складником національної безпеки України та її суспільства, яким може бути заподіяно шкоду через поширення негативних інформаційних впливів, деструктивну пропаганду, загалом застосування технологій інформаційних операцій тощо» [2, с. 71].

Отже, актуальність наукових досліджень у напрямку цифрових об'єктів в судово–експертних дослідженнях не викликає сумнівів, є пріоритетною. Аналіз результатів зазначених досліджень, на нашу думку, повинен сприяти прогнозуванню вектору розвитку всіх напрямків судово–експертної діяльності задля організації діяльності на випередження.

У наших попередніх дослідженнях ми зазначали про дослідження об'єктів інформаційного матеріалу (відео–, звукозапис, протокол огляду та

прослуховування відеозвукозапису, зафіксований на паперовому або цифровому носії), який містить фактичні дані про певну комунікативну взаємодію (мовленнєву діяльність людини). Звертаємо увагу, що зазначені дослідження здійснюються під час проведення комплексної судової психолого–лінгвістичної експертизи та експертизи відео–, звукозапису щодо встановлення комунікативного впливу за ситуаціями комунікативної взаємодії, зафіксованої у відео–, звукозаписі. Виходячи із функцій комунікативного акту і його знакової природи, предметом комплексного психолого–лінгвістичного дослідження мовлення та дослідження відео–, звукозапису є сукупність фактичних даних щодо особливостей мовленнєвої діяльності людини та наявності (відсутності) комунікативного впливу, які встановлюються шляхом інтеграції знань суміжних галузей наук – лінгвістики, психології та досліджень відео–, звукозапису, і мають значення в юридично релевантній ситуації [3].

Предметом дослідження експерта у галузі відео–, звукозапису є зафіксовані у відео–, звукозаписі фактичні дані про особу мовця, які дозволяють ототожнити цю особу за фізичними параметрами голосу або за лінгвістичними ознаками усного мовлення; фізичні носії інформації та пристрої відео–, звукозапису, які дозволяють отримати інформацію про технічні умови та технологію створення відео–, звукозапису на підставі спеціальних знань. Предметом дослідження експерта–лінгвіста є зафіксовані у відео–, звукозаписі фактичні дані, що належать до мовленнєвих форм (інформування, спонукання, переконання, погроз та ін.), які встановлюються на підставі спеціальних лінгвістичних знань. Предметом дослідження експерта–психолога є зафіксовані у відео–, звукозаписі фактичні дані про особливості комунікативної взаємодії осіб (вербальна і невербальна поведінка, що спрямована на досягнення певних комунікативних і практичних цілей на тлі певних психологічних установок, характеристики комунікативного простору спілкування), які встановлюються на підставі спеціальних психологічних знань [3].

Завданням фахівця у галузі досліджень відео–, звукозапису за зафіксованими ситуаціями комунікативної взаємодії є встановлення технічних умов та технологій отримання відео–, звукозаписів та/або ототожнення осіб. Слід зазначити, що встановлення текстового змісту розмов, що зафіксовані у відео–, звукозаписах, не є окремим експертним завданням, оскільки не потребує застосування спеціальних знань та проводиться спеціалістом при вирішенні питань персоніфікації мовленнєвого матеріалу чи застосування спеціальних методів покращення розбірливості усного мовлення. Для досліджень експерту надаються відповідні протоколи огляду та прослуховування з текстовим змістом розмов. Завданням фахівця–лінгвіста за зафіксованими ситуаціями комунікативної взаємодії є встановлення об’єктивного змісту наданих на дослідження повідомлень, виявлення спонукальних мовленнєвих форм (прямих і непрямих) і встановлення граматичної форми висловлювань (фактичного твердження, оцінного судження та ін.). Завданням фахівця–психолога за

зафіксованими ситуаціями комунікативної взаємодії є визначення наявності (відсутності) у діяльності адресанта вербальних і невербальних засобів комунікації спонукального, маніпулятивного, сугестивного характеру в аспекті їх впливу на зміну поведінки адресата, його емоційного стану, когнітивну, особистісну сфери [3].

Інтеграційним складником окреслених предметів дослідження є поняття комунікативного впливу – реалізованого у ситуації комунікативної взаємодії, зафіксованої у відео–,звукозаписі, й вербалізованого у протоколі огляду та прослуховування (з наведеним змістом розмов), що зумовлює вирішення спільного завдання щодо процесу комунікації певних осіб на основі інтеграції спеціальних знань у галузях психології, лінгвістики та досліджень відео–, звукозапису [3].

Таким чином, експерт сьогодні все частіше проводить аналіз цифрової інформації даних із цифрових пристроїв, із соціальних мереж, здійснює аналіз історії відвідування сайтів тощо. Отримані результати допомагають повною мірою реалізувати ключові принципи судово–експертної діяльності, а саме об’єктивності та повноти досліджень.

Перелік використаних джерел:

1. Ткаченко Н. Тенденції розвитку судово–експертної діяльності в умовах глобальної цифрової трансформації суспільства. Теорія та практика судової експертизи і криміналістики. 2025. Вип. 4 (41). С. 35–51. DOI: 10.32353/khrife.4.2025.03.

2. Браїлко Ю., Єгорова Т., Кисла Н., Восканян П. Методологійні аспекти комплексної судової психолого–лінгвістичної експертизи в реаліях збройної агресії РФ проти України. Теорія та практика судової експертизи і криміналістики. 2025. Вип. 4 (41). С. 69–80. DOI: 10.32353/khrife.4.2025.05.

3. Євсюков О. Сучасний стан і перспективи інтеграції спеціальних знань у галузі психології в комплексні судово–експертні дослідження. Теорія та практика судової експертизи і криміналістики. 2025. Вип. 4 (41). С. 205–230. DOI: 10.32353/khrife.4.2025.12.

DOI https://doi.org/10.32837/11300.33543

Kiose Michael
PhD in Physics and Astronomy,
Junior research associate of the department of physical, chemical, biological research Odesa Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine,
Odesa, Ukraine
ORCID: https://orcid.org/0009–0001–6761–0669
e–mail: mihail20032015@gmail.com

PROSPECTS OF USING ARTIFICIAL INTELLIGENCE IN RESEARCHING TITANIUM, ALUMINUM AND MAGNESIUM ALLOY POWDER AS DUAL–USE GOODS

The abstracts consider the possibility of using artificial intelligence at the stage of analyzing significant amounts of information during the study of titanium, aluminum, and magnesium alloy powders.

Key words: dual–use goods, military goods, metal alloy powders, artificial intelligence.

In the context of confronting the armed aggression of the Russian Federation, as well as the transformation of the defense–industrial complex, control over dual–use goods ceases to be a highly specialized procedure and turns into an important instrument of state policy aimed at supporting the national security of Ukraine. Improper supervision or gaps in the export control system can lead to Ukrainian products getting into the enterprises of the military–industrial complex of the aggressor state or into intermediaries who re–export in circumvention of international sanctions. In such a case, even a small batch of specialized powder can become an element of the production of weapons used against Ukraine.

The definition of dual–use goods is enshrined in numerous international agreements such as the Wassenaar Arrangement, documents and national legislation such as Regulation (EU) No. 2021/821 [1, pp. 179 – 181]. According to the law of Ukraine, these are certain types of products, equipment, materials, software, technologies, as well as services (technical assistance) that are not specifically intended for military use, but can be used not only for civilian, but also for military or terrorist purposes. In particular, they can be used for the development and production of military goods, weapons of mass destruction, their delivery means or nuclear explosive devices. Such goods also include certain types of nuclear materials, chemicals, bacteriological, biological and toxic preparations, the list of which is determined by the Cabinet of Ministers of Ukraine [2, Article 1]. The characteristic properties and list of such goods are given in the Unified List of Dual–Use Goods of Ukraine.

When it comes to titanium, aluminum, and magnesium–based metal alloy powders, their characterization is quite broad and includes different classes of materials

– from pure elemental powders to complex alloys with impurities, modified microstructures, controlled particle morphology, and specified functional properties. These features, along with others, cause the following difficulties when controlling such materials:

1. Titanium, aluminum, and magnesium alloy powders are raw materials, not final products. For example, Ti–6Al–4V powder can be used for medical 3D printing (tools, implants, and prostheses), as well as for the manufacture of aviation parts, missile element structures, M1A2 Abrams tank armor elements, M2A2 Bradley infantry fighting vehicle, M777A1 howitzer elements, and other military goods [3, pp. 11–19]. Aluminum alloy powders, in turn, can be used in the automotive industry, civil aircraft construction, construction [4, pp. 357–365], and for the manufacture of military aircraft parts, missile weapons, and armor for military equipment [5, pp. 983–985]. At the same time, powders for civil and military use:

– are visually indistinguishable;

– often have the same general chemical composition;

– the difference lies in particle size, morphology, and impurity content (oxygen and nitrogen), which cannot be determined without the use of laboratory equipment and specialized knowledge.

2. The powder form of the materials provides ample opportunities for circumventing export control:

– ease of division into small batches, which simplifies transportation;

– the ability to disguise as other powder materials allows transportation under the guise of goods with other trade codes and names.

3. With the development of 3D printing with metals, the need for large–scale production facilities (large factories, press equipment, furnaces) has disappeared, and a sufficiently compact 3D printer has been developed, allowing the use of metal alloy powders locally and covertly for the manufacture of parts and structural elements for military purposes.

According to the unified list of dual–use goods approved by the resolution of the Cabinet of Ministers of Ukraine, the following are subject to control:

1C002.c Metal alloy powders or particulates having all of the following characteristics:

1C002.c.1 Made from any of the following systems:…

1C002.c.1.c Titanium alloys (Ti–Al–X or Ti–X–Al);

1C002.c.1.d Aluminium alloys (Al–Mg–X or Al–X–Mg, Al–Zn–X or Al–X–Zn, Al–Fe–X or Al–X–Fe);

1C002.c.1.e Magnesium alloys (Mg–Al–X or Mg–X–Al) «X» denotes one or more alloying elements contained in the alloy…

1C002.c.2. are manufactured in a controlled environment by any of the following processes: 1C002.c.2.a to 1C002.c.2.h a) «Vacuum spraying»; b) «Gas spraying»; c)

«Centrifugal spraying»; d) «Rapid drop quenching»; e) «Melt spinning» and «milling»; f) «Melt extraction» and «milling»; g) «Mechanical alloying»; h) «Plasma spraying».

Each of the production methods is characterized by technological features that directly affect the physical and chemical properties of the resulting powders. In particular, process conditions such as atmosphere, pressure, cooling rate, and mechanical processing determine the size and shape of the particles, their surface structure, degree of purity, and phase and chemical composition.

Vacuum spraying. The metal melt is sprayed in a vacuum, which reduces the reaction with gases and minimizes oxidation, has the following distinctive features:

– low content of impurities (O, N, H) in the finished powder;
– particles have a spherical shape;
– fewer oxide inclusions compared to atmospheric spraying.

Gas atomization. Atomization of molten metal by a jet of high–velocity inert gas (Ar, He) in a chamber where the droplets cool and crystallize into spherical particles has the following distinctive features:

– spherical particles with a smooth surface;
– narrow fractional distribution;
– usually low impurity content [6, pp. 1855–1857].

Centrifugal spraying. A metal rod or wire is melted at the end and rotates at high speed. Centrifugal forces eject the melt in the form of drops, which, when cooled, form a powder, which has the following distinctive features:

– spherical or elongated particles;
– particle surface without significant defects;
– relatively large particle size (often larger than with gas spraying);
– low impurity content.

Rapid quenching of the droplet (plasma atomization). The metal is melted and fed into a plasma stream, where it is broken into very small droplets, having the following distinctive features:

– often extremely small particle size;
– spherical particles with a smooth surface.

Melt extraction and grinding. A mechanical method in which a titanium alloy is hydrogenated, becomes brittle, mechanically ground, dehydrogenated, and a powder is obtained, having the following distinctive features:

– particles of complex shape;
– high surface roughness of particles;
– significant size distribution;
– usually a high content of impurities associated with mechanical processes.

Mechanical alloying. A solid–phase powder metallurgy process in which metal and alloy powders are repeatedly compressed, ground, and recombined by intense mechanical action in special mills, has the following distinguishing features:

– particles are nanostructured and heterogeneous;
– a mixture of phases/solid solutions may be present;

– particles are non–spherical, often broken in shape.

Plasma spraying. A metal wire or rod melts in a plasma jet and is sprayed into particles, which have the following distinctive features:

– spherical particles with high fluidity;

– low impurity content due to the presence of a protective atmosphere;

– variable fractional composition due to the possibility of its regulation by changing the plasma parameters [7, pp. 43 – 47].

The considered physical and chemical features are due to the specifics of the methods of manufacturing titanium, aluminum and magnesium alloy powders, as well as the given items of the Unified List of Dual–Use Goods, which determine a significant amount of research information that needs to be processed, analyzed and compared. Therefore, it is considered promising to use artificial intelligence at the stage of analyzing the results obtained when studying the chemical composition and morphological features of metal powder particles. Artificial intelligence can also be used when comparing the results obtained with the provisions of the Unified List of Dual–Use Goods. This approach will significantly reduce the time required for conducting research.

References:

1. Грицишен Д. О., Абрамова І. В., Вакун О. В. Система вимог Європейського Союзу до експортного контролю за товарами військового призначення та подвійного використання. Економіка, управління та адміністрування. 2025, Вип. 2 (112). С. 177 – 186. DOI: https://doi.org/10.26642/ema–2025–2(112)–177–186.

2. Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» (із змінами, внесеними згідно із Законами останній № 4577–IX від 21.08.2025) https://zakon.rada.gov.ua/laws/show/549–15#Text

3. Gooch W. Potential Applications of Titanium Alloys in Armor Systems / Conference Paper: Titanium 2011. International Titanium Association. San Diego, California, October 2011. P. 21.

4. Davis J.R. Aluminum and Aluminum Alloys. Academic Society: ASM International®. 2001. P. 351 – 416.

5. Gooch W. A., Burkins M. S., Squillacioti R. J. Ballistic testing of commercial aluminum alloys and alternate processing techniques to increase the Availability of aluminum armor. 23rd International symposium on ballistics tarragona. Spain. 2007. P. 981 – 988.

6. Pei Sun, Zhigang Zak Fang, Ying Zhang, Yang Xia. Review of the Methods for Production of Spherical Ti and Ti Alloy Powder/ The Minerals, Metals & Materials Society. 2017. P. 1853 – 1860.

7. Коржик В.М., Строгонов Д.В., Бурлаченко О.М., Войтенко О.М., Куницький Д.В. Розвиток плазмово–дугових технологій отримання сферичних гранул для адитивного виробництва і гранульної металургії. Автоматичне зварювання. 2023. № 11. С. 37 – 52.

DOI https://doi.org/10.32837/11300.33560

Лущик Ігор
старший науковий співробітник лабораторії теоретичних досліджень, міжнародної, редакційно–видавничої та науково–методичної діяльності Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України,
м. Харків, Україна,
ORCID: https://orcid.org/0000–0001–9766–4628,
e–mail: fizedu@ukr.net

Тяпкін Анатолій
Завідувач відділу лабораторії теоретичних досліджень, міжнародної, редакційно–видавничої та науково–методичної діяльності Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України,
м. Харків, Україна,
ORCID: https://orcid.org/0000-0003-0773-8959,
e–mail: tyapkin@ukr.net

ШЛЯХИ ВЗАЄМОДІЇ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ І СУДОВОЇ ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ

У тезах розглянуто перспективи впровадження сучасних високотехнологічних інструментів у практику експертів–лінгвістів і зворотний процес впливу напрацювань судової лінгвістики на вдосконалювання навчання моделей штучного інтелекту.

Ключові слова: великі мовні моделі; судова лінгвістика; аналіз.

Lushchyk Ihor
Senior Researcher at R&D and Publishing, International Cooperation Laboratory National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute» of the Ministry of Justice of Ukraine,
Kharkiv, Ukraine

Tiapkin Anatolii
Head of the Department of the Laboratory of Theoretical Research, International, Editorial and Publishing, Scientific and Methodological Activities of the National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute» of the Ministry of Justice of Ukraine,
Kharkiv, Ukraine

WAYS IN WHICH LARGE LANGUAGE MODELS INTERACT WITH FORENSIC LINGUISTIC EXPERTISE

This abstract examines the prospects for integrating modern high–tech tools into the practice of linguistic experts and the reciprocal influence of developments in forensic linguistics on the refinement of artificial intelligence model training.

Keywords: large language models; forensic linguistics; analysis.

Технологічна трансформація викликів і можливостей судової лінгвістичної експертизи, що відбувається просто зараз, пов’язана зі швидким розвитком і дедалі частішим використанням результатів діяльності генеративного штучного інтелекту (далі – ШІ) у вигляді великих мовних моделей (англ. Large Language Models, LLM), таких як ChatGPT, Claude, Gemini та ін. Судова лінгвістична експертиза та навчання LLM мають глибокий двосторонній зв’язок, заснований на потребах в аналізуванні мовних аномалій, автоматизації виявлення дезінформації та ідентифікації штучно згенерованого контенту. Методологічні підходи судового лінгвістичного аналізу можуть допомогти удосконалювати архітектуру LLM, а сучасні LLM – стати інструментами для підвищення результативності експертних висновків.

Як складний тип ШІ, спеціально розроблений для розуміння та взаємодії з людською мовою, LLM на відміну від інших моделей ШІ використовують передові архітектури та механізми самоконтролю, що дають змогу охопити складні контекстуальні зв’язки в тексті. На величезних наборах даних із книг, статей, дописів у мережах та інших джерел вони навчаються глибоко розуміти синтаксис, семантику та нюанси певної мови.

Методи лінгвістичної експертизи можна використовувати на етапі фільтрації навчальних даних для очищення датасетів від мови ворожнечі, закликів до насильства та маніпулятивного контенту перед етапом попереднього навчання моделей. Особливо це стосується семантико–текстуальної експертизи, завданнями якої є визначення змісту понять, лексичного значення слів (словосполучень), використаних у наданих на дослідження текстах або усних повідомленнях (за їх текстовими відтвореннями), їх стилістичного забарвлення, смислового навантаження, характеру інформації, які вони містять (чи можна таку інформацію розглядати як образливу, чи містить вона загрозу конкретній особі або групі осіб та ін.) [1]. Методики судової лінгвістичної експертизи дають змогу аналізувати контекст повідомлень, виявляти маніпуляції та приховані інтенції автора, що у навчанні LLM може бути використано для опанування ними здібності передбачати токени з урахуванням певного (небажаного) контексту.

Судово–експертні критерії оцінювання погроз, шантажу або наклепу можуть допомогти оцінити токсичність навчальних матеріалів для LLM, якщо їх інтегрувати на етапі навчання з підкріпленням шляхом виставлення обмежень

безпеки. Логіко–лінгвістичний аналіз текстових зв'язків дає змогу розробникам LLM знаходити логічні аномалії у відповідях моделей і їх коригувати. В експертному дослідженні публічного тексту існують дві презумпції, що забезпечують принципову можливість співвіднести текст як мовленнєву дію з диспозицією юридичного припису [2]: 1) осмислене конструювання тексту (для відхилення припущення про випадковість нав'язаних пресупозицій, логічних акцентів, причиново–наслідкових зв'язків та ін.); 2) осмислене й адекватне сприйняття тексту з урахуванням його дискурсивної належності (для відхилення аномальних інтерпретацій і викривлених смислів, породжуваних психічною своєрідністю інтерпретатора, нестандартністю його загальних і спеціальних знань і комунікативних очікувань).

З іншого боку, LLM можуть суттєво допомогти під час проведення судових лінгвістичних експертиз. Наприклад, у судовій авторознавчій експертизі вони можуть диференціювати людське і машинне мовлення, адже тексти, згенеровані різними моделями ШІ, мають специфічні статистичні закономірності (низьку варіативність токенів). До того ж LLM можуть стати неоціненним інструментом в аналізуванні значних обсягів даних, оскільки вони здатні майже миттєво обробляти гігабайти текстових логів із соціальних мереж або месенджерів і виокремлювати потенційні кримінальні загрози (наприклад, ознаки радикалізації, шахрайства або образливі висловлювання). Як зазначає В. Колонюк [3], злочинці можуть використовувати так звані діпфейки як результати «глибокого навчання», під час якого LLM навчаються не лише генерувати необхідні повідомлення, а й розуміти правила фільтрування небажаного контенту і створювати за запитом необхідні тексти, що можуть обходити знову–таки комп'ютерні моделі перевірки. Тому надзвичайно актуальним є питання постійного вдосконалювання семантичного пошуку прихованих значень за допомогою тонко налаштованих LLM для виявлення завуальованого контексту, жаргонізмів, закодованих закликів до протиправних дій або мови ворожнечі.

Ключові сценарії використання LLM як допоміжного інструмента судового експерта у семантико–текстуальній експертизі можуть бути реалізовані у вигляді, по–перше, експрес–скринінгу та кластеризації на початковому етапі експертного аналізу. Оскільки експерту часто доводиться аналізувати значні обсяги даних із листувань у месенджерах, чатах, блогах та ін. публікацій, то LLM можуть групувати тексти за тематичними векторами, відсіювати інформаційний шум (спам, побутові розмови) та виокремлювати фрагменти, що можуть потенційно містити ознаки правопорушення (наприклад, мову ворожнечі, заклики до насильства або фінансове шахрайство) [4].

По–друге, завдяки широкій базі попереднього навчання LLM здатна під час контекстуального аналізування та декодування мовлення підказати експерту приховані конотації, розкрити значення сленгу та проаналізувати контекстне навантаження слів, що у загальновживаних словниках мають нейтральне значення

[5], оскільки зловмисники можуть використовувати завуальовані заклики, жаргон, неофразеологізми або криптолекти (закодовані слова для позначення наркотиків, зброї тощо).

По–третє, під час перевірки тексту на відповідність юридичним дефініціям (наприклад, визначення, чи є вислів «образою» або «наклепом») моделі здійснюють семантичний (а не лише ключовий) пошук, знаходячи синонімічні конструкції та мовленнєві акти погроз або приниження гідності, спираючись на закладені в промпт лінгвістичні маркери.

По–четверте, LLM дають змогу автоматизувати певні рутинні операції експерта, на що він часто витрачає багато часу (наприклад, добирати цитати, структурувати тексти, виокремлювати суб’єкти й об’єкти висловлювання, визначати дієслова дії та структурувати твердження у зручні аналітичні таблиці).

На жаль, у процесі взаємодії між LLM і судовими експертами в Україні існують певні процесуальні та технічні обмеження, адже експертна практика суворо детермінована чинним законодавством і методологією. Результати роботи таких моделей можуть бути лише проміжними даними, а будь–яку лінгвістичну інтерпретацію, яку вносять до висновку, має виконувати винятково атестований судовий експерт. Окрім того, що експерт несе повну юридичну відповідальність за свій висновок (на відміну від LLM), остання може мати так звані галюцинації у вигляді вигадування фактів або спотворювання цитат, тому експерт зобов’язаний відповідально верифікувати кожне посилання на першоджерело.

З іншого боку, процесуальне законодавство (ст. 222 Кримінального процесуального кодексу України [6]) категорично забороняє розголошення даних із матеріалів кримінальних проваджень (зокрема, завантаження у публічні хмарні моделі). Тому для судової лінгвістичної експертизи мають використовуватися винятково локальні розгорнуті моделі (наприклад, сімейства Llama або Mistral) без передачі даних третім сторонам. У разі використання LLM експерт обов’язково має це чітко атрибувати у наданих висновках – на якому етапі та з якою метою це було здійснено (наприклад, для аналізу масивів даних) і зазначити назву та версію використаного програмного забезпечення.

У роботі M. Chernyshev et al. [7] системно досліджено найсучасніші взаємозв’язки між генеративним ШІ та цифровою криміналістикою. Ці дослідники дійшли висновків, що незважаючи на суттєве покращення продуктивності LLM у різних судово–експертних завданнях, залишаються невирішеними протиріччя між імовірнісною природою результатів LLM і нормативно детермінованими вимогами до висновків експертів, а також занепокоєння щодо їх прозорості, відтворюваності та юридичної прийнятності як доказів у судових провадженнях. Також автори наголошують на необхідності міждисциплінарного співробітництва та розробленні єдиних міжнародних підходів щодо співпраці людини і ШІ у межах судових лінгвістичних експертиз.

Додаткового опрацювання потребують також проблеми у сфері еталонів окремих мов (лінгвістична експертиза спирається на зафіксовані лінгвістичні

норми та чинні словники, а LLM формують власне уявлення про норми на базі статистичних розподілів, що можуть бути хибними) і у питаннях визначення авторства (експертиза визначає унікальний ідіолект конкретної особи, натомість LLM може імітувати стилістику будь–якого автора, ускладнюючи роботу експертів).

Перелік використаних джерел:

1.Науково–методичні основи судово–лінгвістичної експертизи писемного мовлення : метод. рек. / Юсупов В. В., Атаманчук В. М., Саковський А. А., Шутенко С. В., Доценко О. Л., Меркулова О. В. Київ : Нац. акад. внутр. справ, 2025. 80 с. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/48e0c483–78fa–452a–a7b7–d0564106383c/content

2.Ажнюк Л. В. Лінгвістична експертиза як юридичний інструмент. Магістеріум. 2017. Вип. 66. Мовознавчі студії. С. 8–15. URL: http://lingvoexpert.org.ua/files/Lesia_Azhniuk_Linhvistychna_ekspertyza.pdf

3.Колонюк В. В. Сучасні можливості використання судових експертиз при досудовому розслідуванні злочинів проти інформаційної безпеки України. Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. 2025. № 74. С. 68–72. URL: https://vestnik–pravo.mgu.od.ua/archive/juspradenc74/15.pdf

4.Thakker A. Large Language Models in Digital Forensics / Medium. Oct 2, 2025. URL: https://medium.com/@aasthathakker/large–language–models–in–digital–forensics–475cb8115b7f

5.Yin Zh., Wang Z., Xu W., Zhuang J., Mozumder P., Smith A., Zhang W. Digital Forensics in the Age of Large Language Models. arXiv:2504.02963v1 [cs.CR]. 03.04.2025. URL: https://arxiv.org/html/2504.02963v1

6.Кримінальний процесуальний кодекс України від 13.04.2012 № 4651–VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text

7.Chernyshev M., Baig Z., Syed N., Doss R., Shore M. Large language models in digital forensics: capabilities, challenges and future directions. Forensic Science International: Digital Investigation. 2026. Vol. 56. 302043. DOI: 10.1016/j.fsidi.2025.302043

DOI https://doi.org/10.32837/11300.33564

Міняйло Анатолій
кандидат сільськогосподарських наук, доцент,
судовий експерт Українського науково–дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України,
м. Київ, Україна
ORCID: https://orcid.org/0000–0003–0959–0855,
e–mail: ma.anatoliy@gmail.com

Дмитренко Людмила
судовий експерт Українського науково–дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України,
м. Київ, Україна
ORCID: https://orcid.org/0009–0002–8555–6851,
e–mail: Dmitrenko_Liudmyla@ukr.net

Міняйло Надія
доктор філософії в галузі знань
«Природничі науки» заступник завідувача відділу аспірантури Національного університету біоресурсів і природокористування України
м. Київ, Україна
ORCID: https://orcid.org/0000–0002–5191–6057,
e–mail: nadia_m@it.nubip.edu.ua

ІНЖЕНЕРНО–ЕКОЛОГІЧНА ЕКСПЕРТИЗА – ВАЖЛИВА ЛАНКА ПРОТИДІЇ ЕКОЛОГІЧНИМ ПРАВОПОРУШЕННЯМ

Інженерну–екологічну експертизу призначають і проводять з метою встановлення не лише безпосереднього антропогенного впливу (забруднення території, виснаження чи забруднення поверхневих або підземних вод, заподіяння шкоди тваринному та рослинному світу тощо), а і його специфічних обставин, наслідків, зокрема й прогнозованих на близьке чи більш віддалене майбутнє, тощо.

Особливістю інженерно–екологічної експертизи є те, що об’єктами дослідження зазвичай є конкретні об’єднання великої кількості різнорідних компонентів, які взаємодіють між собою і з навколишнім середовищем. Різноманітність компонентів за їх походженням (геологічним, біологічним, антропогенним) і за природою їх взаємодії (фізичні, хімічні, біологічні процеси; механічне пересування і змішування, забруднення небезпечними речовинами) створюють неповторний комплекс ознак антропогенно–змінених об’єктів навколишнього середовища на локальній ділянці, де відбулася екологічна подія. Предметом дослідження є дані щодо екологічних ризиків та збитків довкіллю.

Методи дослідження – аналітичні розрахунки на базі загальноприйнятих методик досліджень в галузі екології.

Ключові слова: екологія, екологічні збитки, порушення законодавства, підприємства, інженерно–екологічна експертиза.

Miniailo Anatolii
Ph.D., Associate Professor, Forensic Expert,
Ukrainian Research Institute of Special
Equipment and Forensic Expertise of the SSU,
Kyiv, Ukraine

Dmitrenko Liudmyla
Forensic Expert,
Ukrainian Research Institute of Special
Equipment and Forensic Expertise of the SSU,
Kyiv, Ukraine

Miniailo Nadia
Doctor of Philosophy in Natural Sciences,
Deputy Head of the postgraduate Department,
National University of Life and Environmental Sciences of Ukraine
Kyiv, Ukraine

ENGINEERING ENVIRONMENTAL EXPERTISE – AN IMPORTANT LINK IN COMBATING ENVIRONMENTAL OFFENSE

An engineering environmental examination is assigned and conducted to establish not only the direct anthropogenic impact (pollution of the territory, depletion or contamination of surface or groundwater, harm to fauna and flora, etc.), but also its specific circumstances, consequences, including those predicted for the near or more distant future, etc.

A feature of engineering environmental expertise is that the objects of research are usually specific associations of a large number of heterogeneous components that interact with each other and with the environment. The diversity of components by their origin (geological, biological, anthropogenic) and by the nature of their interaction (physical, chemical, biological processes; mechanical movement and mixing, contamination with hazardous substances) create a unique complex of features of anthropogenically modified environmental objects in the local area where the environmental event occurred.

The subject of the study is data on environmental risks and environmental damage. Research methods – analytical calculations based on generally accepted research methods in the field of ecology.

Keywords: ecology, environmental damage, violation of legislation, enterprises, engineering and environmental expertise

З початком науково–технічного прогресу суспільства та розвитком різноманітних галузей промисловості, пов’язаним з інтенсивним видобуванням корисних копалин, використанням лісів, земель, водойм, флори та фауни, людина все більше займає природні комплекси для задоволення власних потреб. Чим далі суспільство просувається у власному розвитку, тим більше чинить негативний вплив на довкілля. Такі дії призводять не лише до зменшення ресурсів, але й до забруднення і засмічення навколишнього природного середовища продуктами життєдіяльності, що чинить згубний вплив на довкілля не лише в реальному часі, а й на декілька поколінь наперед. При цьому, для задоволення своїх власних матеріальних потреб, суспільство все частіше переступає закон.

Проблема протидії екологічним правопорушенням завжди стояла гостро, адже мала комплексний та інтегративний характер, що зумовлює деструктивний вплив цих посягань на довкілля шкідливими наслідками для життя й здоров’я людей, майна, безпеки виробництва, системи господарювання в державі. Для вирішення цих проблем розроблена та застосовується така галузь як екологічне право.

Екологічне право є системою правових норм, якими регулюються та охороняються суспільні відносини в галузі охорони навколишнього природного середовища та забезпечення екологічної безпеки. Принципами екологічного права є виражені в його нормах основоположні ідеї, засади, риси, відповідно до яких здійснюється регулювання екологічних відносин. Характерною особливістю екологічного права як комплексної галузі є включення до неї визнаних на сьогодні інших галузей права – земельного, гірничого, водного, лісового, фауністичного і атмосфероохоронного, кожна з яких має власну внутрішню структуру, свій предмет і метод правового регулювання та фактично є його підгалузями.

Акти екологічного права (накази й інструкції міністерств та інших органів центральної виконавчої влади та акти місцевих органів державної виконавчої влади й місцевого самоврядування, постанови Кабінету Міністрів України, укази Президента) мають різну юридичну силу, але діють за принципом піраміди, вершиною якої є Конституція України. Відносини в галузі екологічної експертизи регулюються Законом України «Про екологічну експертизу», Законом України «Про охорону навколишнього природного середовища» та іншими актами законодавства України [1].

Для того, щоб не допустити на території України повної і незворотної екологічної катастрофи, в державі функціонує система охорони довкілля і раціонального використання природних ресурсів. В цій системі одне з

найважливіших місць посідає детальний екологічний аналіз намічуваної та діючої господарської діяльності, який складається з багатьох соціально–економіко–екологічних стандартних процедур. Серед них, – екологічна експертиза є найбільш визнаною і поширеною як у нас в країні, так і в міжнародній практиці. Ця сфера діяльності постійно вивчається, досліджується, розвивається та вдосконалюється залежно від викликів, які стоять перед суспільством. Одним з різновидів екологічної експертизи є судова екологічна експертиза.

Загалом, судова експертиза – це дослідження експертом на основі спеціальних знань матеріальних об’єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів досудового розслідування чи суду [2].

На сьогодні, в зв’язку з військовими діями на території України, екологічна ситуація в державі стала значно гіршою – внаслідок постійних обстрілів знищуються цілі біогеоценози, токсичні речовини потрапляють в атмосферне повітря, ґрунт та воду. Наслідки такого впливу на довкілля будуть відчуватися багато десятиліть, потребуючи величезних зусиль та матеріальних ресурсів для відновлення балансу екологічних компонентів які забезпечують стійкість рівноваги екосистеми.

Для притягнення до відповідальності винних в протиправних діях в сфері екології, в тому числі веденні повномасштабної війни на території України, а також з метою отримання відшкодування за заподіяну шкоду довкіллю, важливе значення має інженерно–екологічна експертиза, яка використовується як джерело доказів у кримінальному, цивільному, господарському, адміністративному судовому процесі, у справах про адміністративні правопорушення, а також у виконавчому провадженні, в тому числі в міжнародних судових установах.

Проаналізувавши кількість злочинів в сфері екологічного законодавства можна дійти висновку, що з часом екологічна ситуація тільки погіршується, а кількість екологічних злочинів зростає. Серед порушень екологічного законодавства: незаконне заволодіння землями водного фонду (незаконний видобуток піску у гирлі р. Десна, що призвело до тяжких наслідків у вигляді зміни берегової лінії, деформації ґрунтів, знищення ґрунтів та рослинності), незаконне лісокористування (підробка документації по заниженню обсягу деревини для санітарної рубки, незаконна порубка лісу), незаконне надрокористування (незаконне видобування граніту шляхом проведення масових вибухів, незаконний видобуток вапняку, незаконний видобуток піску), незаконне поводження з відходами (скид на земельні ділянки не призначені для цього небезпечних медичних відходів, залишків гудрону, що призвело до забруднення землі обмінним амонієм, залізом, сульфатами та вуглеводнями), кримінальні правопорушення проти дикої природи (порушення правил боротьби із шкідниками і хворобами рослин внаслідок чого настала масова загибель птахів, в т. ч. червонокнижних), порушення правил охорони вод і забруднення моря (скид

пальмової олії в акваторію морського порту), забруднення атмосферного повітря (забруднення атмосферного повітря шкідливими для життя людей та довкілля відходами промислового виробництва) [3].

Тож, Україну чекає нелегкий шлях відновлення у всіх сферах функціонування держави, в тому числі в сфері збереження та відновлення навколишнього природного середовища. Важливою ланкою в цьому процесі залишається інженерно–екологічна експертиза, адже ефективне використання спеціальних знань експертів в галузі екології має значну роль в кримінальному судочинстві при розгляді злочинів спрямованих проти довкілля.

Звісно, використання спеціальних знань експертів в галузі дослідження обставин та організаційно–технічних причин і наслідків впливу техногенних джерел на об’єкти довкілля дадуть можливість повноцінно оцінити ситуацію та максимально визначити шкоду завдану довкіллю, проте умови сьогодення потребують створення нових і вдосконалення існуючих методик дослідження наслідків порушень екологічного законодавства.

Перелік використаних джерел:

1. Тетарчук І. В., Дяків Т. Є. Екологічне право України, навчальний посібник для підготовки до іспитів, «Центр учбової літератури», Київ – 2021, с.228
2. Бордюгов Л. Г. Судово–екологічна експертиза – основна форма використання спеціальних знань під час розслідування злочинів проти довкілля. Криміналістичний вісник. – 2008. – № 2 (10). – С. 67–71.
3. Результати роботи Спеціалізованої екологічної прокуратури за 2021 рік. URL: https://C:/Users/Lena/Downloads/111SEP._ZVIT _24.01.2022_noviy%20(1).pdf

DOI https://doi.org/10.32837/11300.33566

Пірог Олександр
кандидат технічних наук, головний судовий експерт
Українського науково–дослідного інституту спеціальної техніки та
судових експертиз СБУ, м. Київ, Україна,
доцент кафедри комп'ютерної інженерії та кібербезпеки
Державного університету «Житомирська політехніка»,
м. Житомир, Україна
ORCID: https://orcid.org/0009–0001–6111–9676
e–mail:pirogov@ztu.edu.ua

ОСОБЛИВОСТІ ВИЛУЧЕННЯ ВОЛАТИЛЬНИХ ДАНИХ З ІОТ–ПРИСТРОЇВ

У тезах розглянуто особливості вилучення волатильних даних з IoT–пристроїв під час проведення цифрових розслідувань та огляду місця події. Проаналізовано основні категорії волатильних цифрових артефактів, що можуть мати доказове значення для слідства, а також сучасні проблеми їх виявлення, фіксації та збереження. Особливу увагу приділено енергозалежним даним сучасних edge IoT–пристроїв, які виконують локальну обробку та тимчасове зберігання інформації.

Ключові слова: IoT, цифрова криміналістика, волатильні дані, огляд місця події, цифрові докази.

Piroh Oleksandr
Candidate of Technical Sciences, Chief Forensic Expert
Ukrainian Scientific Research Institute of Special Equipment and Forensic
Expertise of the Security Service of Ukraine, Kyiv, Ukraine,
Associate Professor of the Department of Computer Engineering and
Cybersecurity Zhytomyr Polytechnic State University,
Zhytomyr, Ukraine

FEATURES OF VOLATILE DATA ACQUISITION FROM IOT DEVICES

The abstract examines the peculiarities of volatile data acquisition from IoT devices during digital investigations and crime scene examination. The main categories of volatile digital artifacts with evidential value are analyzed, along with current challenges related to their identification, preservation, and acquisition. Particular attention is paid to volatile data generated by modern edge IoT devices performing local processing and temporary storage of information.

Key words: IoT, digital forensics, volatile data, crime scene examination, digital evidence.

Стрімкий розвиток технологій Інтернету речей (Internet of Things, IoT) призвів до широкого впровадження IoT–пристроїв у системах відеоспостереження, «розумних» будинках, промислових мережах, транспортній інфраструктурі, телекомунікаціях та інших сферах. У сучасних кримінальних провадженнях такі пристрої дедалі частіше виступають джерелами цифрових доказів, здатних містити відомості про дії користувачів, мережеву взаємодію, функціонування програмного забезпечення та події безпеки [1, 2].

Особливістю сучасних IoT–пристроїв є значний обсяг енергозалежних (волатильних) даних, що існують лише під час функціонування пристрою та можуть бути безповоротно втрачені після його вимкнення або перезавантаження. У сучасних IoT–системах значна частина обробки даних здійснюється локально без постійної передачі інформації до хмарних сервісів, унаслідок чого критично важливі цифрові артефакти можуть зберігатися виключно в оперативній пам’яті або тимчасових буферах пристрою [3].

У сучасній науковій літературі проблематика цифрової криміналістики IoT–середовищ розглядається як один із найбільш складних напрямів цифрових розслідувань. Дослідники звертають увагу на гетерогенність IoT–платформ, обмежені апаратні ресурси пристроїв, складність забезпечення цілісності доказів та високу швидкість втрати енергозалежних даних [1, 2]. Окрему увагу приділено питанням готовності IoT–середовищ до проведення цифрових розслідувань, а також використанню штучного інтелекту для виявлення аномалій і цифрових артефактів [4; 5].

У роботах останніх років значна увага приділяється впливу периферійних обчислень (edge computing) на цифрову криміналістику IoT–пристроїв. Зокрема, зазначається, що локальна аналітика, тимчасова буферизація даних та виконання алгоритмів машинного навчання безпосередньо на пристрої формують нові категорії цифрових доказів, які можуть бути втрачені ще до початку слідчих дій [3; 6].

Сучасні дослідження також демонструють важливість оперативного вилучення даних з працюючих систем, оскільки традиційні підходи, орієнтовані переважно на аналіз постійних носіїв інформації, не забезпечують отримання повної картини функціонування IoT–пристрою під час інциденту [7]. Водночас проблеми допустимості цифрових доказів, забезпечення ланцюга збереження доказів та підтвердження їх цілісності залишаються актуальними для практики цифрової криміналістики [8].

Під час огляду місця події на IoT–пристроях можуть бути виявлені різноманітні волатильні цифрові артефакти, здатні містити доказову інформацію для кримінального провадження. До таких артефактів належать активні мережеві

з'єднання, відомості про запущені процеси, вміст оперативної пам'яті, тимчасові журнали подій, службові файли, кеші аналітичних модулів та інші runtime–дані.

Особливу цінність для слідства можуть становити мережеві артефакти, які дозволяють встановити взаємодію пристрою із зовнішніми вузлами. Під час дослідження працюючого IoT–пристрою можуть бути виявлені активні TCP/UDP–з'єднання, таблиці ARP, DNS–cache, VPN–сесії, інформація про віддалене керування та ознаки взаємодії із сервером управління шкідливим програмним забезпеченням (ШПЗ). Такі відомості можуть бути використані для встановлення джерел компрометації, способу несанкціонованого доступу або зв'язку пристрою з іншими елементами інфраструктури.

Для сучасних IP–камер та IoT–пристроїв характерною є наявність тимчасових буферів даних, файлів метаданих та кешів локальної аналітики. У оперативній пам'яті можуть зберігатися результати виявлення руху, розпізнавання об'єктів, параметри роботи аналітичних модулів, фрагменти відеопотоку, журнали подій та службові дані систем відеоаналітики [9]. У деяких випадках такі артефакти можуть містити інформацію, яка відсутня у постійній пам'яті пристрою або не передавалася до хмарних сервісів.

Крім того, у пам'яті IoT–пристроїв можуть зберігатися токени сесій, криптографічні ключі, тимчасові файли автентифікації та параметри активних користувацьких сесій. Такі дані можуть мати важливе значення для встановлення факту несанкціонованого доступу, використання віддаленого адміністрування або функціонування ШПЗ [7].

Важливою особливістю IoT–пристроїв є висока швидкість втрати енергозалежних даних. У процесі нормального функціонування відбувається постійний перезапис буферів пам'яті, журналів подій та тимчасових файлів. Унаслідок цього значна частина цифрових артефактів може бути втрачена ще до прибуття слідчо–оперативної групи на місце події [10].

Практика цифрових розслідувань свідчить, що традиційне відключення живлення IoT–пристрою нерідко призводить до повної втрати важливої доказової інформації. Особливо це стосується сучасних IoT–систем, де значна частина аналітичних даних існує виключно в оперативній пам'яті пристрою. У зв'язку з цим особливого значення набувають методи оперативного вилучення даних з працюючих систем, які дозволяють мінімізувати втрату волатильних цифрових артефактів.

Додаткову складність становить ризик спрацювання механізмів протидії цифровій криміналістиці (anti–forensic mechanisms). У деяких випадках різка втрата мережевого з'єднання, перезавантаження або зміна конфігурації пристрою можуть активувати автоматичне очищення пам'яті, завершення процесів або механізми віддаленого видалення даних. Тому під час огляду місця події важливе значення має контрольоване обмеження мережевої взаємодії без повного вимкнення пристрою.

Під час вилучення волатильних даних особливу увагу необхідно приділяти забезпеченню цілісності цифрових доказів та документуванню дій спеціаліста. Усі дії повинні супроводжуватися фіксацією часу, стану пристрою, активних мережевих підключень, параметрів системи та використаних інструментів. Після вилучення даних необхідно здійснювати їх хешування із застосуванням сучасних криптографічних алгоритмів.

Таким чином, сучасні IoT–пристрої є важливими джерелами волатильних цифрових доказів, здатних містити критично важливу інформацію для розслідування. Значна частина таких артефактів існує лише під час функціонування пристрою та може бути безповоротно втрачена внаслідок неправильного поводження з ним під час огляду місця події. Ефективне вилучення енергозалежних даних потребує використання методів оперативного дослідження працюючих систем, врахування особливостей периферійних обчислень та мінімізації впливу на поточний стан IoT–пристрою. Подальший розвиток цифрової криміналістики IoT–середовищ повинен бути спрямований на вдосконалення методів виявлення, збереження та аналізу волатильних цифрових артефактів, а також забезпечення допустимості отриманих цифрових доказів у кримінальному провадженні.

Перелік використаних джерел:

1.Ahmed A.A., Farhan K., Jabbar W.A., Al–Othmani A., Abdulrahman A.G. IoT forensics: Current perspectives and future directions. Sensors. 2024. Vol. 24(16). P. 5210.

2.Al–Shaer M. The Internet of Things (IoT) forensic investigation process: Challenges and open issues. Journal of Information Security and Cybercrimes Research. 2023. Vol. 6(1). P. 1–15.

3.Castelo Gómez J.M., Ruiz–Villafranca S. Integrating the edge computing paradigm into the development of IoT forensic methodologies. International Journal of Information Security. 2024. Vol. 23. P. 1093–1116.

4.Friedl S., Pernul G. IoT forensics readiness – Influencing factors. Forensic Science International: Digital Investigation. 2024. Vol. 49. P. 301768.

5.Rizvi S., Scanlon M., McGibney J., Sheppard J. Pushing network forensic readiness to the edge: A resource constrained artificial intelligence based methodology. 2024 Cyber Research Conference – Ireland. IEEE. 2024. P. 1–8.

6.Williams M., Emeteveke I., Adeyeye O.J., Emehin O. Enhancing data forensics through edge computing in IoT environments. International Journal of Research Publication and Reviews. 2025.

7.Mujtaba H.A., Mumtaz G., Ahmad M.H., Rehman M. Forensic strategies for revealing memory artifacts in IoT devices. Journal of Computing & Biomedical Informatics. 2024. Vol. 7(2).

8.Nath S., Summers K., Baek J., Ahn G.J. Digital evidence chain of custody: Navigating new realities of digital forensics. Proceedings of the IEEE International

Conference on Trust, Privacy and Security in Intelligent Systems and Applications. 2024. P. 11–20.

9.Salem Y., Kassem A., Abdul Salam M., Alhaidari F. Forensically analyzing IoT smart camera using MAoIDFF–IoT framework. Journal of Network and Computer Applications. 2024. Vol. 229. P. 103912.

10.Oyeyemi K., Chrysikos A., Salekzamankhani S. Digital forensic readiness in IoT–enabled organisations and forensic investigation analysis in real–time. International Journal of Electrical, Electronics and Data Communication. 2024. Vol. 12(9). P. 21–28.

DOI https://doi.org/10.32837/11300.33567

Радецький Сергій
аспірант кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009-0003-7920-4187
e–mail: rad.177@gmail.com

ОСОБЛИВОСТІ ОГЛЯДУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ, РОЗМІЩЕНИХ У ВІДКРИТОМУ ДОСТУПІ

Розкрито значення огляду електронних документів у кримінальному провадженні, запропоновано їх класифікацію залежно від місця зберігання та охарактеризовано особливості дослідження документів, розміщених на фізичних носіях інформації, у відкритому доступі в мережі Інтернет і хмарних сервісах. Визначено організаційні, процесуальні й тактичні вимоги до проведення такого огляду, зокрема щодо залучення спеціаліста, фіксації метаданих, створення цифрових образів носіїв, забезпечення незмінності, автентичності та можливості подальшої перевірки отриманої доказової інформації.

Ключові слова: огляд, електронний документ, цифрові докази, фізичний носій інформації, інтернет-публікація, хмарне сховище.

Radetskyi Serhii
postgraduate student of the Department of Criminalistics, Forensic Examinations and Polygraphology
National University «Odesa Law Academy», Odesa, Ukraine

SPECIFIC FEATURES OF THE EXAMINATION OF ELECTRONIC DOCUMENTS AVAILABLE IN OPEN ACCESS

The article examines the significance of the examination of electronic documents in criminal proceedings, proposes their classification according to the place of storage, and outlines the specific features of examining documents stored on physical data carriers, publicly available on the Internet, and held in cloud services. The organisational, procedural, and tactical requirements for conducting such an examination are identified, particularly those concerning the involvement of a specialist, the recording of metadata, the creation of forensic images of data carriers, and the preservation of the integrity and authenticity of evidential information, as well as the possibility of its subsequent verification.

Keywords: examination, electronic document, digital evidence, physical data carrier, online publication, cloud storage.

Огляд належить до числа найбільш результативних, а в окремих випадках і незамінних слідчих (розшукових) дій, за допомогою яких на початковому етапі досудового розслідування виявляються, фіксуються та досліджуються відомості про обставини вчинення кримінального правопорушення. Саме завдяки огляду уповноважена особа отримує можливість безпосередньо сприймати обстановку події, встановлювати наявні сліди, локалізацію предметів, характер пошкоджень, просторові взаємозв'язки між об'єктами та інші фактичні дані, що мають значення для подальшого доказування. У багатьох випадках саме результати своєчасно проведеного огляду визначають подальший напрям розслідування, дозволяють висунути первинні версії та уникнути втрати важливої доказової інформації.

Огляд найчастіше є першою невідкладною слідчою (розшуковою) дією, яка проводиться у межах кримінального провадження невдовзі після отримання повідомлення про подію. Характерною ознакою огляду є його пізнавальна спрямованість, адже він дає змогу отримати первинні дані шляхом особистого спостереження та використання криміналістичних методів фіксації.

З огляду на специфіку об'єктів, які підлягають дослідженню під час досудового розслідування, доцільно окремо розрізняти огляд документів, огляд комп'ютерної та іншої електронної техніки, а також огляд електронних документів, розміщених як на електронних носіях інформації, так й у відкритому доступі.

З розвитком інформаційних технологій люди дедалі частіше зберігають робочі матеріали в електронному вигляді. Це значно підвищує значення огляду електронних документів, однак водночас ускладнює тактику цієї слідчої дії. Електронний документ у кримінальному провадженні доцільно розуміти як інформацію, зафіксовану в електронній формі на відповідному носії або в інформаційній системі, яка може бути відтворена у доступному для сприйняття вигляді та використана для встановлення обставин, що мають значення для провадження. До таких документів можуть належати текстові файли, фотографії, відеозаписи, аудіофайли, електронне листування, повідомлення у месенджерах, інтернет-публікації, файли у хмарних сховищах та інші цифрові матеріали.

Особливість електронних документів полягає в тому, що їх доказове значення залежить не лише від змісту, а й від можливості перевірити походження, цілісність, час створення, автора, історію редагування, місце зберігання та спосіб отримання. Тому поводження з такими об'єктами має ґрунтуватися на кількох базових правилах: недопущення зміни вихідних даних, використання лише службового обладнання та ліцензійного програмного забезпечення, залучення компетентного спеціаліста, фіксація кожної дії з електронним об'єктом, забезпечення можливості повторної перевірки отриманого результату іншою уповноваженою особою .

У межах досудового розслідування кримінальних правопорушень електронні документи доцільно поділяти на три основні групи: документи,

розміщені на фізичних носіях інформації; документи у відкритому доступі в мережі Інтернет; документи, що зберігаються у хмарних сервісах.

До фізичних носіїв інформації належать жорсткі диски, SSD-накопичувачі, USB-флеш-накопичувачі, CD, DVD, Blu-ray-диски, SD і microSD-карти, пам'ять мобільних телефонів, планшетів, фото- та відеокамер, а також пам'ять окремих периферійних пристроїв. Особливе значення мають мобільні пристрої, оскільки за їх допомогою часто створюються аудіозаписи, фото- і відеоматеріали, ведеться службове листування, зберігаються контакти джерел інформації та дані про переміщення особи.

Електронні документи на фізичних носіях можуть бути отримані під час огляду місця події, обшуку, тимчасового доступу до речей і документів або добровільного надання. У багатьох випадках для повноцінного дослідження доцільним є вилучення самого носія. Водночас, якщо вилучення може паралізувати роботу установи чи організації, більш виправданим є створення побайтової копії носія, тобто його цифрового образу, із залученням спеціаліста. Такий спосіб дозволяє зберегти доказову інформацію і водночас не перешкоджати законній діяльності установи.

Огляд електронних документів, розміщених у відкритому доступі в мережі Інтернет, має власну специфіку [1]. Йдеться насамперед про інтернет-публікації, відеозаписи, фотоматеріали, пости у соціальних мережах, коментарі, повідомлення на сайтах редакцій або інформаційних порталах. Такі матеріали можуть підтверджувати тематику професійної діяльності потерпілого, наявність конфліктів, погроз, агресивних реакцій аудиторії або зацікавленість певних осіб у припиненні його роботи.

Огляд інтернет-публікації доцільно проводити у службовому приміщенні з використанням службового комп'ютера, стабільного доступу до мережі Інтернет, ліцензійного програмного забезпечення та, за необхідності, за участю спеціаліста. У протоколі потрібно зазначити технічні характеристики комп'ютера, серійний номер, назву й версію операційної системи, назву та версію браузера, адресу веб-сторінки, дату і час доступу до неї. Веб-сторінку слід переглядати у стандартному масштабі, без додатків чи надбудов, які можуть змінювати її відображення.

У протоколі огляду інтернет-публікації необхідно зафіксувати назву веб-сайту, URL-адресу, заголовок матеріалу, дату публікації, ім'я чи псевдонім автора, жанр або рубрику, основний зміст, згаданих фізичних і юридичних осіб, додані фото-, відео- чи аудіофайли, а також посилання на них. Окремо варто досліджувати коментарі до публікації, оскільки в них можуть міститися погрози, заклики до насильства, образи або інші прояви агресії щодо журналіста. Водночас рекламні блоки та сторонні мультимедійні елементи, які не пов'язані зі змістом матеріалу, не потребують детального опису [2].

Для фіксації веб-сторінки її доцільно роздрукувати та долучити до протоколу як додаток із зазначенням моделі та серійного номера принтера. Фото- , відео- та аудіофайли, які є частиною публікації, слід зберегти на службовий носій

і також долучити до матеріалів провадження. Додатково може застосовуватися збереження сторінки у форматі HTML або інший технічно надійний спосіб фіксації її змісту.

Окремої уваги потребують електронні документи, що зберігаються у хмарних сервісах. Такі сервіси активно використовуються для збереження чернеток, фото-, відео- та аудіоматеріалів, робочих планів, записів, таблиць, спільних документів та інших матеріалів. Їх перевага полягає у можливості доступу з будь-якого пристрою, однак для слідства це створює додаткові труднощі, пов’язані з авторизацією, захистом персональних даних, юрисдикцією провайдера та ризиком дистанційного видалення інформації .

Доступ до хмарного сховища може бути отриманий шляхом добровільного надання логіна і пароля потерпілим, його родичами або іншими уповноваженими особами; шляхом тимчасового доступу до електронних інформаційних систем відповідного сервісу; через міжнародну правову допомогу, якщо провайдер перебуває за межами України; або шляхом зняття інформації з електронних інформаційних систем у порядку, передбаченому КПК України. У разі самостійного доступу слідчого чи прокурора до хмарного сервісу з використанням авторизаційних даних особи потрібно діяти особливо обережно. Логін і пароль не варто зазначати у протоколі, щоб не допустити розголошення персональних даних і несанкціонованого доступу до акаунта.

Під час огляду документів у хмарному сховищі в протоколі слід зазначити назву сервісу, його веб-адресу, дату й час доступу, каталог розміщення документа, назву файлу, його формат, дату створення, дату останнього редагування, доступну історію змін, відомості про автора або користувачів, які мали доступ до документа, а також постійне посилання на файл, якщо воно існує. Текстові документи та зображення доцільно роздруковувати й долучати до протоколу, а аудіо-, фото- та відеофайли зберігати на службовий носій із належним описом технічних параметрів.

Отже, комп’ютерна техніка, мобільні пристрої, фізичні носії інформації, інтернет-публікації та хмарні сервіси є надзвичайно важливими джерелами інформації у межах розслідування різних видів кримінальних проваджень. Їх огляд потребує спеціальних знань, технічної обережності, чіткої процесуальної фіксації та дотримання принципу незмінності цифрових даних. Залежно від місця розміщення електронного документа – на фізичному носії, у відкритому доступі в мережі Інтернет або в хмарному сховищі – тактика його огляду має відрізнятися, однак у всіх випадках головним завданням залишається збереження автентичності інформації та забезпечення можливості її подальшого використання у кримінальному провадженні.

Перелік використаних джерел:

1. Коваленко А. В. Огляд комп'ютерних даних: сутність і процесуальний порядок проведення. *Вісник Харківського національного університету внутрішніх справ.* 2023. № 3 (102). Ч. 2. С. 187–197.

2. Коваленко А. В. Особливості проведення огляду вебресурсів як різновиду огляду комп'ютерних даних. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали V Міжнар. наук.-практ. конф. (м. Київ, 21 грудня 2023 р.). Київ : КНДІСЕ, 2023. С. 199–202.

DOI https://doi.org/10.32837/11300.33572

Стаурська Олександра
доктор філософії в галузі права, доцент кафедри криміналістики, судових експертиз та поліграфології, Національного університету «Одеська юридична академія» м.Одеса, Україна
ORCID ID: https://orcid.org/0000–0003–2269–3699
e–mail: staurskaya.sasha@onua.edu.ua

АВТОМАТИЗАЦІЯ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ У КРИМІНАЛІСТИЦІ: ВІД КЛАСИЧНИХ МЕТОДИК ДО ІНТЕЛЕКТУАЛЬНИХ АЛГОРИТМІВ

Досліджено трансформацію експертної діяльності у криміналістиці під впливом автоматизованих систем, цифрових технологій та алгоритмів штучного інтелекту. Акцентовано увагу на тому, що класичні криміналістичні методики не втрачають свого значення, однак поступово доповнюються інструментами комп'ютерного аналізу, машинного навчання, цифрового моделювання та автоматизованого порівняння об'єктів. Обґрунтовано, що автоматизація експертних досліджень сприяє підвищенню швидкості, точності й відтворюваності експертних висновків, але водночас породжує нові методологічні, етичні та процесуальні виклики. Підкреслено необхідність збереження провідної ролі експерта як суб'єкта критичної оцінки результатів, отриманих за допомогою інтелектуальних алгоритмів.

Ключові слова: криміналістика, судова експертиза, автоматизація, штучний інтелект, експертне дослідження, цифрові технології, алгоритми.

Staurska Oleksandra
Doctor of Philosophy in Law, Associate Professor of the Department of Criminalistics, Forensic Examinations and Polygraphology, National University «Odesa Law Academy» Odesa, Ukraine

«AUTOMATION OF EXPERT RESEARCH IN CRIMINALISTICS: FROM CLASSICAL METHODS TO INTELLIGENT ALGORITHMS»

The article examine the transformation of expert activity in criminalistics under the influence of automated systems, digital technologies and artificial intelligence algorithms. It is emphasized that classical forensic methods do not lose their significance, but are increasingly supplemented by computer analysis, machine learning, digital modelling and automated comparison of forensic objects. The paper substantiates that automation of expert research contributes to increasing the speed, accuracy and

reproducibility of expert conclusions, while also generating new methodological, ethical and procedural challenges. The need to preserve the leading role of the forensic expert as the subject of critical assessment of results obtained through intelligent algorithms is emphasized.ve not only a criminal but also a sociocultural impact on society.

Keywords: criminalistics, forensic examination, automation, artificial intelligence, expert research, digital technologies, algorithms.

У сучасних умовах цифровізації кримінального провадження судово–експертна діяльність дедалі активніше змінює свою методологічну основуn [1, с.42]. Якщо раніше експертне дослідження переважно спиралося на індивідуальний професійний досвід експерта, візуальне порівняння, описові методики та ручну обробку матеріалів, то сьогодні значна частина експертних завдань виконується із застосуванням автоматизованих інформаційних систем, спеціалізованого програмного забезпечення, електронних баз даних, алгоритмів розпізнавання образів і технологій штучного інтелекту. Така трансформація не є простим технічним оновленням інструментарію. Вона фактично змінює спосіб мислення експерта, логіку побудови дослідження та критерії оцінки отриманого результату.

Автоматизація експертних досліджень у криміналістиці може бути визначена як процес упровадження технічних, програмних та алгоритмічних засобів, що забезпечують часткове або комплексне виконання операцій із виявлення, фіксації, аналізу, порівняння, класифікації та інтерпретації криміналістично значущих об’єктів [2, с. 117]. Йдеться не лише про використання комп’ютера як допоміжного засобу, а про формування нової моделі експертної діяльності, у якій цифровий інструмент стає активним елементом пізнання.

Класичні криміналістичні методики традиційно ґрунтуються на принципах науковості, повноти, об’єктивності, порівняльності та відтворюваності. Саме ці принципи дозволяють забезпечити доказову цінність експертного висновку. Однак розвиток злочинності, збільшення обсягів цифрової інформації, ускладнення способів приховування слідів та поява нових видів об’єктів дослідження зумовлюють необхідність модернізації експертного інструментарію. У таких умовах традиційний підхід, заснований виключно на ручній роботі експерта, часто виявляється недостатнім через часові обмеження, великий масив даних та потребу у високій точності аналізу.

Одним із найбільш поширених напрямів автоматизації є використання автоматизованих систем у дактилоскопічній, балістичній, трасологічній, почеркознавчій, портретній, фоноскопічній та молекулярно–генетичній експертизі [3, с. 89]. Так, сучасні науковці звертають увагу на те, що цифрові алгоритми особливо ефективні під час автоматизованого порівняння папілярних візерунків, аналізу слідів на кулях і гільзах, дослідження рукописних текстів, біометричної ідентифікації особи за зовнішністю та встановлення генетичних збігів у ДНК–профілюванні [4, с. 54; 5, с. 201]. У фоноскопічній експертизі

інтелектуальні алгоритми використовуються для аналізу голосу, тембру, інтонаційних характеристик та виявлення ознак монтажу аудіозаписів, що суттєво розширює можливості доказування у кримінальному провадженні [6, с. 73]. Їх призначення полягає у прискоренні пошуку збігів, систематизації об'єктів, попередньому групуванні ознак та формуванні ймовірних варіантів ідентифікації. Наприклад, у дактилоскопічних дослідженнях автоматизовані системи дають змогу порівнювати сліди пальців із великими масивами наявних обліків, тоді як у балістиці програмні комплекси аналізують мікрорельєф слідів на кулях і гільзах. Проте остаточне рішення у таких випадках не повинно автоматично переноситися на програму, оскільки експерт має перевірити релевантність збігів, оцінити якість сліду, умови його утворення та можливість альтернативного пояснення.

Особливої актуальності набуває застосування штучного інтелекту у сфері судової експертизи [4, с. 56]. Інтелектуальні алгоритми можуть використовуватися для розпізнавання зображень, аналізу відеозаписів, ідентифікації голосу, виявлення цифрових маніпуляцій, класифікації документів, прогнозування зв'язків між об'єктами та пошуку закономірностей у великих наборах даних. Машинне навчання дає змогу алгоритмам удосконалювати результати обробки інформації на основі навчальних вибірок, що відкриває значні перспективи для криміналістики. Водночас саме ця особливість породжує проблему прозорості алгоритму, адже не кожна модель дозволяє чітко пояснити, чому вона дійшла певного результату.

У кримінальному процесі така ситуація має принципове значення. Експертний висновок не може бути перетворений на некритичне відтворення результату, сформованого «чорною скринькою». Для суду, сторони обвинувачення, сторони захисту та інших учасників провадження важливо розуміти не лише підсумок дослідження, а й шлях, яким експерт до нього дійшов. Саме тому автоматизовані системи та інтелектуальні алгоритми мають розглядатися як допоміжні інструменти, а не як повноцінна заміна експерта.

Методологічно доцільно розрізняти кілька рівнів автоматизації експертних досліджень. Перший рівень охоплює технічну автоматизацію, пов'язану з оцифруванням матеріалів, електронним документообігом, створенням цифрових копій, використанням баз даних та програм для вимірювання параметрів об'єктів. Другий рівень передбачає аналітичну автоматизацію, за якої програмні засоби виконують порівняння, класифікацію, фільтрацію та статистичну обробку інформації. Третій рівень становить інтелектуальна автоматизація, коли застосовуються алгоритми машинного навчання, нейронні мережі, системи розпізнавання образів та прогнозні моделі. Кожен із цих рівнів має різний ступінь впливу на експертне рішення і, відповідно, потребує різного рівня процесуального контролю.

Важливою перевагою автоматизації є підвищення відтворюваності результатів [5, с. 203]. Якщо класичне дослідження іноді залежить від суб'єктивної

оцінки окремого експерта, то алгоритмічні інструменти дозволяють стандартизувати певні етапи аналізу. Це особливо важливо у випадках, коли об'єкти мають значну кількість параметрів або коли необхідно порівняти сотні чи тисячі зразків. Автоматизована система здатна швидко обробити та структурувати масив даних, виокремити найбільш релевантні ознаки й зменшити ризик технічної помилки.

Водночас автоматизація не усуває ризику помилок повністю. Алгоритм може працювати некоректно через неякісні вхідні дані, нерепрезентативну навчальну вибірку, технічні обмеження програмного забезпечення або помилки в налаштуванні системи. Крім того, у криміналістиці особливе значення мають контекст, умови утворення слідів, механізм події та взаємозв'язок між окремими доказами. Такі аспекти не завжди можуть бути повною мірою враховані автоматизованою системою. Тому експерт має не лише використовувати технологію, а й розуміти межі її застосування.

Окремої уваги потребує питання валідації інтелектуальних алгоритмів [6, с. 71]. Для використання у судово–експертній діяльності програмний інструмент має бути перевіреним, науково обґрунтованим, стабільним і придатним до повторної перевірки. Необхідно встановити, на яких даних навчалася модель, якою є її похибка, у яких умовах вона демонструє найкращі результати, а в яких може давати хибні висновки. Без такої перевірки використання алгоритмів у кримінальному провадженні може поставити під сумнів допустимість і достовірність доказів.

Не менш важливим є етичний аспект автоматизації. Використання штучного інтелекту в експертних дослідженнях пов'язане з ризиком алгоритмічної упередженості, порушенням права на захист, непрозорістю джерел даних та надмірною довірою до технічного результату. У цьому контексті особливого значення набуває принцип «людина в контурі прийняття рішення», відповідно до якого остаточну оцінку має здійснювати компетентний експерт, а не автоматизована система.

Практичне значення автоматизації експертних досліджень полягає у можливості переходу від фрагментарного аналізу окремих слідів до комплексного дослідження цифрового та матеріального середовища злочину [7, с. 134]. Наприклад, у розслідуванні складних злочинів алгоритми можуть одночасно аналізувати відеозаписи, геолокаційні дані, електронне листування, фінансові транзакції, цифрові сліди та результати традиційних експертиз. Такий підхід дозволяє формувати цілісну криміналістичну картину події та виявляти зв'язки, які залишалися б непомітними при застосуванні лише класичних методик.

Перспективним є також поєднання автоматизації з концепцією криміналістичної профілактики. Накопичення та аналіз великих масивів експертної інформації можуть використовуватися не лише для розслідування вже вчинених кримінальних правопорушень, а й для виявлення типових способів злочинної діяльності, прогнозування ризиків і попередження нових злочинів.

Проте такий напрям потребує особливо обережного підходу, адже прогнозні алгоритми не повинні перетворюватися на інструмент необґрунтованого обмеження прав людини.

Таким чином, автоматизація експертних досліджень у криміналістиці є закономірним етапом розвитку судово–експертної діяльності. Вона не заперечує класичних методик, а розширює їх можливості, створюючи умови для швидшого, точнішого та комплекснішого аналізу доказової інформації. Водночас ефективність такої автоматизації залежить від наукової обґрунтованості алгоритмів, прозорості їх застосування, належної валідації, процесуальної регламентації та професійної підготовки експертів.

На завершення варто підкреслити, що майбутнє криміналістичної експертизи полягає не у заміні експерта машиною, а у формуванні нової моделі взаємодії людини й технології. Класичні криміналістичні методики забезпечують наукову та процесуальну основу експертного дослідження, тоді як інтелектуальні алгоритми розширюють аналітичні можливості експерта. Саме баланс між традиційною криміналістичною школою та інноваційними цифровими інструментами має стати ключовою умовою розвитку сучасної судової експертизи.

Перелік використаних джерел:

1. Шепітько В. Ю., Шепітько М. В. Цифрова криміналістика та перспективи розвитку судової експертизи в Україні. Вісник Національної академії правових наук України. 2023. № 2. С. 39–48.

2. Коваленко В. В. Інформаційні технології у криміналістичній діяльності: монографія. Київ : Юрінком Інтер, 2022. 248 с.

3. Клименко Н. І. Сучасні автоматизовані системи судово–експертних досліджень. Криміналістичний вісник. 2024. № 1. С. 84–92.

4. Біленчук П. Д., Удовенко Ж. В. Штучний інтелект у системі криміналістичного забезпечення правосуддя. Юридична Україна. 2024. № 5. С. 52–60.

5. Лисенко Д. О. Автоматизація криміналістичних досліджень у контексті цифрової трансформації. Право і суспільство. 2023. № 4. С. 198–205.

6. Сегай М. Я., Стринжа В. К. Судова експертиза: сучасні технології та проблеми валідації методик. Харків : Право, 2021. 312 с.

7. Журавель В. А. Інтелектуальні алгоритми в криміналістиці: перспективи використання та процесуальні ризики. Актуальні проблеми держави і права. 2025. № 98. С. 129–138.

DOI https://doi.org/10.32837/11300.33575

Хамула Дмитро
кандидат культурології, старший науковий співробітник лабораторії психологічних, мистецтвознавчих та інших видів досліджень Одеського науково–дослідного інституту судових експертиз Міністерства юстиції України,
м. Одеса, Україна
ORCID: http://orcid.org/0000–0002–3146–1390,
e–mail: 0957487542dh@gmail.com

ДО ПИТАННЯ АТРИБУЦІЇ КАХЕЛЬНОЇ КАМІНО–ПЕЧІ З ГРИФОНАМИ В БУДИНКУ М. ПІДГОРСЬКОГО В КИЄВІ

У тезах розглянуто попереднє повідомлення про іконографічну атрибуцію відомої каміно–печі, збережену в інтер'єрах будинку М. Підгорського за адресою Ярославів Вал, 1 у Києві, яку традиційно прийнято вважати такою, що виготовлена на київській кахельній фабриці І. Андржеєвського. Автор подає своє бачення з приводу цієї атрибуції.

Ключові слова: судова мистецтвознавча експертиза, майоліка, пічні кахлі, Андржеєвський, Цельм і Бем, атрибуція, пічне мистецтво, фурнологія.

Khamula Dmytro
PhD in Cultural Studies,
Senior Research Fellow at the Laboratory of psychological, Art History and other types of Studies, Odesa Research Institute of Forensic expertise of the Ministry of Justice of Ukraine,
Odesa, Ukraine

ON THE QUESTION OF THE ATTRIBUTION OF THE GRIFFIN–TILED FIREPLACE STOVE FROM M. PIDHORSKYI'S HOUSE IN KYIV

The theses consider a preliminary report on the iconographic attribution of the well–known fireplace stove preserved in the interiors of M. Pidhorskyi's house located at Yaroslaviv Val Street in Kyiv, which has traditionally been regarded as a product of I. Andrzejewski's Kyiv tile factory. The author presents his own perspective regarding this attribution.

Key words: forensic art expertise, majolica, stove tiles, Andrzejewski, Celm & Boehm, attribution, stove art, furnology.

Дослідження проводиться в рамках НДР «Розробки методики проведення мистецтвознавчої експертизи антикварних теракотових, кахельних, фаянсових, майолікових печей та камінів щодо приналежності їх до культурних цінностей, які

мають історичне, художнє, етнографічне та наукове значення», що знаходиться в розробці співробітника та керівника НДР ОНДІСЕ (керівник Д.В. Хамула).

Увагу дослідників давно привертають кахельні печі з будинку М. Підгорського (1897 р. інж. М. Добачевський). Особливо ж розкішна т.зв. каміно–піч із грифонами. Піч прикрашена багатим рельєфним декором та майоліковою поліхромією. Вона має масивну цокольну і топкову частину. Топкова частина прикрашена фланкуючими по боках складно профільованими колонами–пілонами та жіночими маскаронами, розташованими у верхньому регістрі кутів. Конструктивно дана каміно–піч складається з кількох ярусів. Нижній ярус над топкою має камінну поличку. Нижня частина напіччя по боках фланкована низькими лізенами у вигляді декоративних фігурок грифонів. По центру, та по боках від грифонів розміщуються кахлі з картушевим орнаментом (Рис. 1–3). По центру напіччя наявна розетка–мушля, навколо якої розташовані панелі з симетричними рослинними мотивами, облямовані темними рамками. Вище розташований антаблемент, прикрашений рослинним декором та складно–профільований карниз з пояском орнаменту іоніків та пояском із листя аканфу. Традиційно цю піч, як і решту інших печей цього будинку приписують фабрикації І. Андржеєвського. Проте, чи так це, є інтригою, адже клейм на кахлях ніхто не бачив.

Більш менш достеменно підтверджується атрибуція розкішної каталожної печі моделі №11 [2, іл. 20] І. Андржеєвського з будинків М. Підгорського, Городецького та в особняку 1903 р. І. Філіпова в Житомирі. Тож треба вивчати каталоги, робити детальний іконографічний аналіз. Отже декілька слів треба сказати про знаменитий київський керамічний завод.

Кахельний та майоліковий завод І. Андржеєвського (Andrzejowski) відомий з початку 1880 рр. Тут виготовляли пічні кахлі, майоліку, теракоту, фасадну плитку, тощо [2, с. 160; 6, с. 27–28]. Завод мав великі потужності: з 1887 по 1894 р. виробництво кахлів зросло з 95 тис./рік до 150 тис./рік [1, с. 337]. Продукцію заводу було відзначено медалями та дипломами на виставках у різних містах. Перелік цих нагород відомий, наприклад, з фірмових бланків [3, рис. 7–8, с. 190].

Порівняльний мистецтвознавчий та стилістичний аналіз показав, що дана модель каміно–печі зустрічається серед північних виробників кахельних печей. Так, наприклад, коли ми звертаємось до виробництва заводу Цельм і Бем («Zelm & Boehm», Riga, Гончарний та ізразцевий завод Цельм І., Товариство ізразцевих заводів Цельм і Бем в м. Рига, ми стикаємося з такою самою моделлю каміно–печі. Так, серед світлин з Ювілейної Виставки до 700–річчя Риги в 1901 р. можна побачити вітрину фабрики, де ми взнаємо ту саму каміно–піч, яка в повній комплектації повинна мати над карнизом аттик з рядку пальмет (Рис. 4).

Першу фабрику, з якої починається знаменита фірма Цельм і Бем, у було засновано у 1859 р. І.К. Цельмом в Ризі. Станом на 1893 р. на фабриці вироблялося до 100,000 тис. кахлів [1, 337]. На підприємстві працювали також син засновника

Йоганн Цельм та його зять Пауль Йоганн Фрідріх Бем (1850–1926). З 1877 р. він стає співвласником фірми J.C. Zelm. З 1892 р. фабрика виготовляла майолікові печі та вази. З 1892 р. фірма діяла під назвою «Zelm & Boehm», а з 1910 р. «Paul Boehm».

Серед аналогій до київської каміно–печі виділяється ціла низка майолікових печей чудової збереженості. Так, в м. Кéльці в одній кам'яниці зберіглася аналогійна піч із грифонами в монохромній колористиці [6] (Рис. 5). За колористикою найбільш ближча до київської каміно–піч в м. Валмієра в Латвії (Рис. 6). Серед колекції із 20 печей та камінів палацу в Діклі (маєток був власністю родини фон дер Паленів, останнім володарем якого до 1919 р. був барон Пауль Вольф), яку зібрав нинішній його власник Е. Медніс, які були туди перенесені з середмістя Риги, є повністю аналогійний київському експонат. Відомо, що частину з них виготовлено латвійською пічною компанією « Zelm & Boehm», ще частину на порцеляновій мануфактурі Мейсена в Німеччині, деякі в Санкт–Петербурзі.

Дві поліхромні каміно–печі збереглися в Крустпілському замку. З 1996 р. тут розташований Екабпілський історичний музей [7] (Рис. 8–9). Аналогійна каміно–піч знаходиться в маєтку Медемів в Бергхові (з 1920 р. Калнамуйжа), зведений з 1906–1912 рр.

Піч цієї ж моделі зберіглася в 3–зірковому готелі «Guesthouse Airava», що розміщено у колишній купальні Е. Рацене в Юрмалі в Латвії [5] (Рис. 11–12). На сайті німецької фірми з побудови печей «Masuch GmbH – Kamin– und Ofenbau» виставлена піч цієї ж моделі у світло коричневому кольорі «Спеціальна пропозиція: антикварна коричнева кахельна піч». Фабрикація тут нажаль не зазначена [8] (Рис. 13). Найбільш відомою у світі аналогією є каміно–піч (єдина із бюстом) в маєтку Тернбладів («American Swedish Institute») в Міннеаполісі [4] (Рис. 14). Фабрикацію ж цієї печі відносять до шведської порцелянової фабрики «Рьорстранд».

Отже, проведений попередній іконографічний аналіз майолікової каміно–печі з грифонами в колишньому будинку М. Підгорського, як визначної пам'ятки декоративно–прикладного і монументального мистецтва, сподіваємось, дасть орієнтири для подальшого поглиблення щодо наукової атрибуції аналогійних об'єктів на теренах України, де виготовлялися та куди завозилися з інших країн високохудожні печі та каміни протягом XIX та початку XX ст. Подібні дослідження, окрім суто мистецтвознавчої складової, розкриваюсь важливі аспекти зовнішніх торгівельних зв'язків минулого нашої країни.

Перелік використаних джерел:

1. Орлов П.А., Будагов С.Г. Указатель фабрик и заводов Европейской России: Материалы для фабрично–заводской статистики. Спб.: тип. В. Киршбаума, 1894. 850 с.

2. Смолій Ю. Кахельний і майоліковий завод Йосафата Андржейовського в Києві: власники, виробництво, каталоги. Студії мистецтвознавчі. Архітектура. Образотворче та декоративно–житкове мистецтво; НАН України; ІМФЕ ім. М.Т. Рильського. К.: ІМФЕ, 2012. С. 158–173.

3. Шулешко І. «Фабрика кахлів» Іосафата Андржейовського. Хронопис. Вісник Українського державного науково–дослідного проектного інституту «УкрНДШпроектреставрація». №7–8, 2013. К.: Софія. С. 181–193.

4. Darby Johnson. What is a Kakelugn? Learn. Blog. Turnblad Mansion & Collections. URL: https://asimn.org/turnblad–mansion–collections/what–is–a–kakelugn/

5. Guesthouse Airava. URL: https://www.booking.com/hotel/lv/guesthouse–airava.en–gb.html?lang=en–gb&soz=1&lang_changed=1

6. Kielce: piec kaflowy z gryfami. kamienicewpolsce. https://www.kamienicewpolsce.pl/2015/08/kielce–piec–kaflowy–z–gryfami.html?m=1

7. Krustpils pils top par nozīmīgu tūrisma magnētu. Publicēts: 11.12.2020. URL: https://www.cfla.gov.lv/lv/jaunums/krustpils–pils–top–par–nozimigu–turisma–magnetu

8. Sonderangebot antiker brauner Kachelofen. masuch–kamine. URL: https://www.masuch–kamine.de/kacheloefen/antike–kacheloefen/sonderangebot–antiker–brauner–kachelofen/ 2

Рис. 1. 2. 3. Каміно–піч у будинку М. Підгірського. Київ, вул. Ярославів вал, 1.

Рис. 4. Світлина вітрини виробів заводу «Zelm & Boehm» на виставці в Ризі, 1901 р. Рис. 5. Каміно–піч в Ке́льцях (Польща). Рис. 6. Каміно–піч в м. Валмієра (Латвія). Рис. 7. Каміно–піч в палаці Діклі (Латвія.).

Рис. 8. 9. Дві каміно–печі в Крустпілському замку (Латвія). Рис. 10. Каміно–піч в маєтку Медем. Бергхов (Калнамуйжа).

Рис. 11. 12. Каміно–піч в купальні Е. Рацене. Юрмала (Латвія). Рис. 13. Каміно–піч з сайту «Masuch GmbH – Kamin– und Ofenbau». Рис. 14. Шведський какелунг в American Swedish Institute. Мініалосіс. Мінесота. США.

DOI https://doi.org/10.32837/11300.33578

Чабанець Тетяна
кандидат наук з державного управління, судовий експерт (не є фахівцем державної спеціалізованої установи), патентний повірений
м. Київ, Україна
ORCID ID: https://orcid.org/0000–0002–3146–2051
e–mail: t.chabanets@gmail.com

Макарець Альбіна
провідний судовий експерт Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України
м. Київ, Україна
ORCID ID: https://orcid.org/0009–0007–1296–0796
e–mail: kyiv@nncise.org.ua

НАТУРНЕ ДОСЛІДЖЕННЯ У СУДОВО–ТОВАРОЗНАВЧІЙ ЕКСПЕРТИЗІ ЯК ОСНОВА ІДЕНТИФІКАЦІЇ, ДЕФЕКТОСКОПІЇ ТА ПАРАМЕТРИЧНОГО ПІДБОРУ АНАЛОГІВ

У тезах систематизовано покроковий алгоритм проведення натурного огляду з урахуванням положень профільних НДР і методичних матеріалів судово–експертних установ України. Окрему увагу приділено значенню фіксації ідентифікаційних та дефектних ознак для подальшого визначення ринкової вартості товару.

Ключові слова: ідентифікація, дефектоскопія, інструментальне вимірювання, фіксація.

Chabanets Tetiana
Candidate of Sciences in Public Administration, forensic expert (not affiliated with a state specialized forensic institution), patent attorney
Hora village, Boryspil District,
Kyiv, Ukraine

Makarets Albina
Leading Forensic Expert of the Kyiv Branch of the National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute» of the Ministry of Justice of Ukraine,
Kyiv, Ukraine

IN–SITU EXAMINATION IN FORENSIC COMMODITY EXPERTISE AS A BASIS FOR IDENTIFICATION, DEFECT DETECTION AND PARAMETRIC SELECTION OF ANALOGUES

The paper systematizes a step–by–step algorithm for conducting an in–situ examination, taking into account the provisions of specialized research works and methodological materials of forensic expert institutions of Ukraine. Particular attention is paid to the importance of recording identification and defect–related features for the subsequent determination of the market value of goods.

Keywords: identification, defect examination, instrumental measurement, recording.

Проведення судово–товарознавчої експертизи передбачає поєднання процесуальних вимог із товарознавчим, матеріалознавчим та оціночним аналізом об’єкта. Фізичний огляд об’єкта (натурне дослідження) є центральною стадією експертизи. Помилки, допущені на цьому етапі, можуть нівелювати всі подальші математичні розрахунки вартості чи зносу та призвести до втрати висновком статусу належного доказу в суді.

Перш ніж перейти до безпосереднього огляду об’єкта, експерт має сформувати належні процесуальні, інформаційні та технічні умови дослідження. Саме підготовчий етап визначає межі подальшої ідентифікації, перелік необхідних інструментів і джерела порівняльної інформації.

Процесуальний підготовчий етап. Натурне дослідження не починається в момент дотику до товару. Йому передує етап верифікації та забезпечення умов, регламентований профільними НДР (зокрема, методикою [1] та посібником [2]):

Аналітичне проектування: Вивчення ухвали суду, постанови слідчого або заяви, зіставлення специфікацій, контрактних умов (Інкотермс) та кодів закупівель за Єдиним закупівельним словником (ДК 021:2015) [3]. На цьому етапі, як зазначено у Методрекомендаціях [4], експерт формує інформаційну модель ринку досліджуваного об’єкта, що дозволяє усунути цінові викривлення на ринку, на якому ціни на товари або активи змінюються дуже швидко, різко та непередбачувано впродовж короткого проміжку часу.

Світлові та мікрокліматичні умови огляду: Огляд має проводитися за стабільного, бажано природного або еквівалентного штучного освітлення (не менше 300 лк). Недостатнє освітлення ускладнює виявлення прихованих вад, наприклад на текстилі, а також мікротріщин на склі й кришталі.

Після уточнення завдання експертизи та вихідних документальних даних ключового значення набуває технічна готовність робочого місця експерта. Якість натурного дослідження прямо залежить від того, чи забезпечено належні умови освітлення, вимірювання, фотофіксації та безпечного доступу до конструктивних елементів об’єкта.

Мінімальний інструментальний паспорт робочого місця експерта–товарознавця передбачений вимогами Інструкції [5].

Судовий експерт здійснює дослідження не лише шляхом візуального огляду, а й із застосуванням повірених засобів вимірювальної техніки (ЗВТ) та спеціального обладнання, які становлять технічну базу його атестованого робочого місця та можуть включати:

Засоби фіксації: Засіб для фіксації зображень (цифрова камера високої роздільної здатності для точної передачі кольору й текстури) та криміналістичні масштабні лінійки (для верифікації метричних параметрів вад на фото).

Оптичні прилади та освітлення: Набір луп (3 набори: текстильна вимірювальна – для аналізу волокон; ручна з підсвічуванням – для дефектоскопії; годинникова панкратична – для маркувальних клейм та ювелірних виробів) і ліхтар із регулюванням світлового потоку (для створення косо падаючого світла, що виявляє мікрорельєфні подряпини).

Вимірювальні прилади (ЗВТ): Рулетки різної довжини (для великогабаритних об’єктів), штангенциркуль (ноніусний або цифровий з точністю до 0,01–0,05 мм), товщиномір (для листового металу, скла, стінок тари) та терези (високоточні аналітичні або технічні, залежно від групи товарів).

Допоміжний інструментарій: Пінцет (для безконтактної роботи з дрібними деталями чи волокнами) та універсальний набір інструментів (для демонтажу захисних кожухів побутової техніки або огляду внутрішніх кріплень меблів).

Наявність належного інструментарію сама по собі не гарантує повноти дослідження. Методологічно важливим є дотримання послідовності огляду – від зовнішніх ознак і пакування до маркування, конструктивних параметрів, експлуатаційного стану та дефектів.

Чотиришаровий алгоритм дослідження. Товарознавча ідентифікація та дефектоскопія потребують послідовного огляду об’єкта – від пакування й зовнішніх ознак до конструктивних параметрів, фактичного стану та дефектів.

Етап І. Верифікація пакування та умов середовища

Відповідно до методики [6] огляд доцільно починати з тари. Експерт фіксує тип пакування, сліди деформації, розривів, підмокання чи температурного впливу. Це дає змогу попередньо розмежувати виробничі пошкодження та дефекти, спричинені неналежним транспортуванням або зберіганням.

Етап ІІ. Маркувальний аудит та товарознавча ідентифікація

На цьому етапі натурні дані зіставляються з документальними. Фіксація маркування, зовнішніх ознак, артикулу, модифікації, комплектності й технічних параметрів є основою для правильної ідентифікації товару та подальшого підбору об’єктів–аналогів. Зокрема, деталізація серійних номерів зброї [7], IMEI чи ревізій плат телекомунікаційних засобів [8] впливає на точність подальшого економічного дослідження. Опис має здійснюватися із застосуванням спеціалізованої галузевої термінології.

Етап ІІІ. Органолептичний та інструментальний аналіз

Фактичний якісний стан об’єкта визначається шляхом візуального аналізу поверхонь, тактильної оцінки матеріалів, виявлення сторонніх запахів, вимірювання лінійних розмірів, зазорів і перевірки геометрії виробів. Наприклад, для меблевих виробів може оцінюватися щільність та еластичність оббивки за посібником [2].

Етап IV. Товарознавча дефектоскопія

Кожен дефект описується за трьома ознаками: локалізація, метричні параметри та причинно–наслідковий характер. Експерт розмежовує виробничі дефекти, зокрема технологічні вади ювелірних виробів [9], і невиробничі пошкодження, пов’язані із заливтям, пожежею, аварійним режимом роботи чи грубою експлуатацією. Для дефектів одягу може застосовуватися класифікатор [10]. Отримані дані фіксуються в дефектній відомості та використовуються для розрахунку втрати якості за методикою [6].

Зафіксовані під час натурного дослідження ідентифікаційні, конструктивні та дефектні ознаки мають не лише описове, а й оціночне значення: саме вони визначають можливість коректного зіставлення товару з ринковими аналогами або параметрично подібними об’єктами.

Параметрична подібність як засіб забезпечення точності оцінки

При визначенні ринкової вартості експерт не завжди має можливість підібрати повністю ідентичний аналог, особливо щодо специфічного чи унікального обладнання. У таких випадках відповідно до загальних підходів оцінки машин та обладнання [11] застосовується перехід до параметрично подібних об’єктів, зокрема методу рівноефективного функціонального аналога.

Коректність такого підбору залежить від повноти натурного огляду: експерт має зафіксувати основні ціноутворюючі параметри об’єкта, виявити відмінності між ним і аналогом та обґрунтувати необхідні комерційні, функціональні чи параметричні коригування.

Неточна або неповна фіксація цих параметрів може призвести до помилкового вибору аналога, викривлення ринкової вартості та зниження доказової стійкості експертного висновку. Тому параметричні й дефектні ознаки мають бути підтверджені фотофіксацією та відповідними відомостями.

Криміналістичні стандарти фіксації: фото і відомості

Результати огляду мають бути неупереджено задокументовані.

Правило чотирьох планів фотофіксації

Орієнтуюче фото: Фіксація загального плану приміщення чи майданчика, де знаходиться об’єкт, з прив’язкою до нерухомих орієнтирів.

Оглядове фото: Об’єкт зйомки крупним планом (повний вигляд виробу з кількох ракурсів для однозначної візуальної ідентифікації моделі та стану).

Вузлове фото: Фіксація маркувальних ярликів, шильд, маркувальних написів, панелей керування чи замків (головне джерело параметричних даних).

Детальне фото: макрофіксація кожного візуально ідентифікованого дефекту з розміщенням масштабної лінійки в одній площині з об'єктом зйомки.

Таким чином, натурне дослідження формує доказову й розрахункову основу судово–товарознавчої експертизи. Його результати визначають якість ідентифікації об'єкта, обґрунтованість дефектоскопії, коректність підбору аналогів і стійкість експертного висновку до перевірки.

Висновок

Натурне дослідження у практиці судового експерта–товарознавця є не формальним візуальним оглядом, а комплексною процедурою ідентифікації, інструментального вимірювання, дефектоскопії та документальної фіксації стану об'єкта. Дотримання послідовності огляду – від пакування та зовнішніх ознак до маркування, конструктивних параметрів і дефектів – забезпечує повноту вихідних даних для подальшого визначення ринкової вартості. Належна параметрична ідентифікація, обґрунтований підбір аналогів і масштабна фотофіксація підвищують методологічну обґрунтованість, об'єктивність і доказову стійкість експертного висновку.

Перелік використаних джерел:

1.Методика товарознавчого дослідження електропобутових товарів: звіт про НДР (заключний) / Одеський НДІ судових експертиз; керівник НДР Н.П. Сапун. Одеса, 2010. № держреєстрації 0109U007824.

2.Судово–товарознавча експертиза меблевих виробів: звіт про НДР (заключний) / Київський НДІ судових експертиз; керівник НДР О.О. Желавська; відп. викон. О.В. Павленко. Київ, 2003. № держреєстрації 0102U003878.

3.ДК 021:2015. Єдиний закупівельний словник: Національний класифікатор України : затв. наказом Міністерства економічного розвитку і торгівлі України від 23.12.2015 № 1749.

4.Методичні рекомендації з визначення вартості машин, обладнання, сировини та споживчих товарів з урахуванням ретроспективності оцінки при проведенні судово–товарознавчих експертиз: звіт про НДР (остаточний) / Дніпропетровський НДІ судових експертиз; наук. керівник О.Ю. Холодова. Дніпро, 2019. № держреєстрації 0118U000659.

5.Інструкція про особливості здійснення судово–експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах: затв. наказом Міністерства юстиції України від 12.12.2011 № 3505/5.

6.Розрахунок втрати якості непродовольчих товарів у зв'язку з їх зносом та наявністю дефектів, який використовується в проведенні товарознавчих досліджень : методичні рекомендації / О.О. Желавська. Київ: Київський НДІСЕ, 2003. 45 с.

7.Судово–товарознавча експертиза з оцінки зброї асортименту спеціалізованої роздрібної торгівельної мережі: звіт про НДР (заключний) / МЮУ,

ХНДІСЕ; наук. кер. А.І. Лозовий; викон.: О.О. Михальський, О.С. Донцова, В.Г. Нікітюк та ін. Харків: ХНДІСЕ, 2013. 111 с. № ДР 0112U001392.

8.Методичні рекомендації з питань призначення та проведення судових товарознавчих експертиз аудіовізуальної продукції та програмного забезпечення: звіт про НДР (заключний) / МЮУ, ХНДІСЕ; наук. кер. А.І. Лозовий; викон.: О.О. Михальський, В.М. Губарева, О.С. Донцова та ін. Харків: ХНДІСЕ, 2011. 64 с. № ДР 0111U002336.

9.Розробка методичного посібника «Судово–товарознавча експертиза ювелірних виробів»: звіт про НДР (заключний) / МЮУ, КНДІСЕ; наук. кер. В.О. Сорокіна; викон.: О.О. Желавська, О. В. Павленко та ін. Київ: КНДІСЕ, 2014. 424 с. № ДР 0113U000620.

10.Словник термінів і визначень судової товарознавчої експертизи: словник / уклад.: К.І. Рудакова, С.О. Коробова, О.О. Желавська, О.В. Ярославцева. Сімферополь: КримНДІСЕ, 2003. 128 с.

11.Загальний підхід до експертної оцінки машин та обладнання при проведенні судово–товарознавчих експертиз / М.Є. Башкатова, В.П. Верестун, В.М. Скороход; ред. С.В. Тарасютіна. Слов’янськ: Донецький НДІ судових експертиз, 2019.

DOI https://doi.org/10.32837/11300.33583

Черемнова Антоніна
кандидат юридичних наук, доцент,
вчений секретар Одеського науково–дослідного інституту
судових експертиз Міністерства юстиції України,
професор кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–0221–6337
e–mail:cheremnova2506@gmail.com

СУДОВА ЕКСПЕРТИЗА В СИСТЕМІ ДОКАЗУВАННЯ: РОЛЬ, ФУНКЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Досліджено роль судової експертизи у системі доказування, її основні функції та значення для встановлення об'єктивної істини. Проаналізовано сучасні тенденції розвитку експертної діяльності, цифровізацію та використання новітніх технологій.

Ключові слова: судова експертиза, доказування, експертний висновок, спеціальні знання, цифрова криміналістика, докази.

Cheremnova Antonina
Candidate of Law, Associate Professor,
Scientific Secretary of the Odesa Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine,
Professor of the Department of Criminalistics, Forensic Examinations and Polygraphology, National University «Odesa Law Academy»,
Odesa, Ukraine

FORENSIC EXPERTISE IN THE EVIDENTIARY SYSTEM: ROLE, FUNCTIONS AND PROSPECTS FOR DEVELOPMENT

This study examines the role of forensic expertise within the system of evidence, its main functions, and its significance in establishing the objective truth. It analyses current trends in the development of expert practice, digitalization, and the use of cutting–edge technologies.

Key words: forensic examination, evidence, expert opinion, specialist knowledge, digital forensics, evidence.

Судова експертиза в сучасному кримінальному, цивільному, господарському та адміністративному судочинстві є одним із ключових елементів системи доказування, оскільки саме вона забезпечує використання спеціальних знань для встановлення фактичних обставин справи. В умовах розвитку науки,

техніки, цифрових технологій та ускладнення механізмів вчинення правопорушень значення судової експертизи постійно зростає. Сьогодні експертні дослідження охоплюють не лише традиційні напрями, пов'язані з криміналістичними, медичними чи економічними дослідженнями, а й новітні сфери, зокрема цифрову криміналістику, телекомунікаційні дослідження, психологічні та лінгвістичні експертизи, дослідження криптовалютних операцій, кіберзлочинності та електронних доказів. У зв'язку з цим судова експертиза перетворюється на важливий інструмент забезпечення об'єктивності та достовірності доказової діяльності.

Система доказування в юридичному процесі передбачає збирання, перевірку, оцінку та використання доказів для встановлення істини у провадженні. У цій системі судова експертиза виконує особливу функцію, оскільки її результати формуються на основі спеціальних знань, методик та науково обґрунтованих досліджень. Висновок експерта не є звичайним джерелом інформації, а являє собою результат професійного аналізу об'єктів, явищ чи процесів із використанням спеціальних методів. Саме тому експертний висновок має підвищену доказову цінність у тих випадках, коли встановлення певних фактів неможливе без застосування наукових знань.

Роль судової експертизи у системі доказування визначається насамперед її здатністю встановлювати фактичні дані, які неможливо отримати іншими процесуальними засобами. Наприклад, лише судово–медична експертиза може об'єктивно встановити причину смерті, характер тілесних ушкоджень чи механізм їх утворення. Судово–балістична експертиза дозволяє ідентифікувати зброю, з якої було здійснено постріл, а комп'ютерно–технічна експертиза забезпечує дослідження електронних носіїв інформації та відновлення цифрових даних. Таким чином, експертна діяльність забезпечує можливість трансформації спеціальних знань у процесуально допустимі докази.

Особливе значення судова експертиза має під час розслідування складних та багатоепізодних кримінальних правопорушень. Організована злочинність, корупційні правопорушення, кіберзлочини, терористичні акти та злочини, пов'язані з незаконним обігом зброї чи наркотичних засобів, характеризуються високим рівнем конспірації та використанням сучасних технологій. У таких умовах традиційні слідчі (розшукові) дії часто не забезпечують отримання достатнього обсягу доказової інформації, що підвищує роль експертних досліджень. Наприклад, під час розслідування кіберзлочинів саме результати комп'ютерно–технічної експертизи дозволяють встановити IP–адреси, цифрові сліди користувачів, шляхи передачі інформації та факти несанкціонованого втручання у комп'ютерні системи.

Судова експертиза також виконує важливу гарантійну функцію у забезпеченні прав і свобод учасників процесу. Об'єктивний експертний висновок може підтвердити або спростувати версії сторін, виключити помилки слідства та

запобігти незаконному притягненню особи до відповідальності. Особливо це стосується випадків, коли показання свідків є суперечливими, а матеріальні докази потребують спеціального дослідження. Наприклад, молекулярно–генетичні експертизи ДНК нерідко стають вирішальними для встановлення невинуватості особи або підтвердження її причетності до вчинення злочину.

Функції судової експертизи в системі доказування є багатогранними. Однією з основних є пізнавальна функція, яка полягає у встановленні нових фактів та обставин шляхом дослідження об'єктів експертизи. Саме завдяки цій функції експерт здатний надати інформацію, яка не може бути безпосередньо сприйнята слідчим чи судом. Наприклад, експерт може встановити давність документа, механізм виникнення пошкоджень або факт втручання у цифрову систему.

Не менш важливою є доказова функція судової експертизи. Висновок експерта виступає самостійним джерелом доказів і використовується під час оцінки обставин провадження. При цьому суд не пов'язаний висновком експерта, однак у разі незгоди з ним зобов'язаний мотивувати своє рішення. Такий підхід забезпечує баланс між принципом вільної оцінки доказів і необхідністю врахування науково обґрунтованих результатів досліджень.

Ідентифікаційна функція судової експертизи полягає у встановленні тотожності об'єктів або осіб за певними ознаками. Найбільш поширеним прикладом є дактилоскопічні, трасологічні, балістичні та генетичні експертизи. Саме вони дозволяють встановити особу злочинця, ідентифікувати транспортний засіб, зброю чи інші об'єкти, пов'язані з подією правопорушення [1]. У сучасних умовах значного розвитку набуває також біометрична ідентифікація, яка базується на аналізі рис обличчя, голосу або поведінкових характеристик людини.

Діагностична функція експертизи спрямована на визначення механізму події, причин та умов виникнення певних явищ. Наприклад, пожежно–технічна експертиза дозволяє встановити причину займання, а автотехнічна експертиза визначає механізм дорожньо–транспортної пригоди та технічну можливість уникнення зіткнення. Завдяки цьому забезпечується не лише встановлення фактичних обставин, а й формування об'єктивної картини події.

Прогностична функція судової експертизи полягає у можливості прогнозування певних наслідків або поведінкових характеристик на основі дослідження наявних даних. Особливе значення вона має у психологічних та психіатричних експертизах, де оцінюється психічний стан особи, її здатність усвідомлювати свої дії та прогнозується можливість небезпечної поведінки.

Сучасний розвиток судової експертизи нерозривно пов'язаний із цифровізацією суспільства. Зростання кількості електронних доказів зумовлює необхідність удосконалення методик їх дослідження. Сьогодні значна частина доказової інформації міститься у смартфонах, комп'ютерах, хмарних сервісах, месенджерах та соціальних мережах. Це вимагає від експертів не лише технічної підготовки, а й постійного оновлення знань у сфері інформаційних технологій. Перспективним напрямом є розвиток цифрової криміналістики, яка охоплює

дослідження електронних слідів, криптовалютних транзакцій, блокчейн–технологій та штучного інтелекту.

Водночас розвиток судової експертизи супроводжується низкою проблем. Однією з основних є перевантаження експертних установ та значні строки проведення експертиз. У складних провадженнях експертні дослідження можуть тривати місяцями, що негативно впливає на ефективність досудового розслідування та судового розгляду. Крім того, існує проблема недостатнього матеріально–технічного забезпечення експертних установ, особливо в умовах воєнного стану та економічних труднощів.

Окремої уваги потребує питання незалежності експерта. Судова експертиза повинна ґрунтуватися виключно на принципах наукової об'єктивності та неупередженості. Однак у практичній діяльності інколи виникають ризики тиску на експертів або спроб використання експертних висновків у маніпулятивних цілях. Саме тому важливим напрямом розвитку є посилення гарантій незалежності експертної діяльності, удосконалення механізмів професійної атестації та підвищення відповідальності за надання завідомо неправдивого висновку.

Перспективи розвитку судової експертизи пов'язані також із міжнародною інтеграцією та гармонізацією експертних стандартів. Україна поступово адаптує систему судово–експертної діяльності до європейських стандартів, що передбачає впровадження сучасних методик, міжнародної сертифікації лабораторій та уніфікації процедур досліджень. Важливого значення набуває співпраця з міжнародними організаціями та використання досвіду іноземних експертних установ [2].

Одним із найбільш перспективних напрямів є використання технологій штучного інтелекту у судово–експертній діяльності. Алгоритми машинного навчання вже сьогодні застосовуються для аналізу великих масивів даних, розпізнавання облич, автоматизованого аналізу документів та дослідження цифрових слідів. У майбутньому такі технології можуть суттєво підвищити швидкість та точність експертних досліджень. Водночас використання штучного інтелекту породжує нові виклики, пов'язані з достовірністю алгоритмів, захистом персональних даних та процесуальною допустимістю результатів автоматизованого аналізу.

Не менш важливим напрямом є розвиток комплексних та міждисциплінарних експертиз. Сучасні правопорушення часто потребують одночасного застосування знань із різних галузей науки. Наприклад, розслідування економічних злочинів може вимагати проведення комплексної економічної, комп'ютерно–технічної та почеркознавчої експертизи. Такий підхід дозволяє забезпечити всебічне дослідження обставин провадження та підвищити ефективність доказування.

Таким чином, судова експертиза є невід'ємним елементом сучасної системи доказування та одним із найбільш ефективних засобів встановлення об'єктивної

істини у конкретному провадженні. Її роль постійно зростає у зв'язку з розвитком науки, техніки та ускладненням форм злочинної діяльності. Судова експертиза виконує пізнавальну, доказову, ідентифікаційну, діагностичну та прогностичну функції, забезпечуючи використання спеціальних знань у процесуальній діяльності. Подальший розвиток судово–експертної діяльності пов'язаний із цифровізацією, впровадженням технологій штучного інтелекту, міжнародною інтеграцією та удосконаленням нормативно–правового регулювання. Водночас важливими залишаються питання забезпечення незалежності експертів, підвищення якості експертних досліджень та скорочення строків їх проведення. Саме комплексне вирішення цих завдань дозволить підвищити ефективність судової експертизи та зміцнити її значення у системі доказування.

Перелік використаних джерел:

1. Бабенко А.М., Матвєєвський О.В., Федоров І.В. Судові експертизи у кримінальному провадженні: навчальний посібник // Одеській державний університет внутрішніх справ. Одеса: ОДУВС, 2026. 241 с.

2. Клюєв О. Перспективи розвитку судової експертології в Україні з урахуванням міжнародного досвіду. Теорія та практика судової експертизи і криміналістики. 2022. Вип. 4 (29). С. 5–11.

DOI https://doi.org/10.32837/11300.33584

Чернов Олександр
доктор філософії у галузі права, доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0009–0002–6038–9479
e–mail:sanjehan.14@gmail.com

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ПОЧЕРКОЗНАВЧОЇ ЕКСПЕРТИЗИ ПІДПИСІВ У ЦИФРОВИХ КОПІЯХ ДОКУМЕНТІВ

Досліджено особливості проведення почеркознавчої експертизи підписів у цифрових копіях документів, проблеми втрати ідентифікаційних ознак та ризики цифрового редагування. Проаналізовано сучасні підходи до оцінки автентичності підписів і можливості цифрових технологій у експертній практиці.

Ключові слова: судова експертиза, почеркознавство, підпис, електронний документ, підроблення, цифрова криміналістика, ідентифікація.

Chernov Oleksandr
Doctor of Philosophy in Law, Associate Professor of the Department of Criminalistics, Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

FEATURES OF CONDUCTING HANDWRITING ANALYSIS OF SIGNATURES IN DIGITAL COPIES OF DOCUMENTS

This study examines the specific features of handwriting analysis of signatures in digital copies of documents, the issues surrounding the loss of identifying characteristics, and the risks associated with digital editing. It analyses contemporary approaches to assessing the authenticity of signatures and the potential of digital technologies in forensic practice.

Key words: forensic examination, handwriting analysis, signature, electronic document, forgery, digital forensics, identification.

Почеркознавча експертиза традиційно належить до найбільш поширених видів криміналістичних досліджень документів, оскільки підпис виступає одним із ключових реквізитів, що підтверджує волевиявлення особи, засвідчує юридичну значущість документа та забезпечує його доказове значення. У сучасних умовах цифровізації документообігу, широкого використання електронних засобів комунікації та дистанційного обміну документацією суттєво зросла кількість

випадків, коли об'єктом дослідження стають не оригінали документів, а їх цифрові копії у вигляді сканованих зображень, фотокопій, PDF–файлів або інших електронних форматів. Така тенденція формує нові виклики для судової почеркознавчої експертизи, оскільки класичні методики дослідження підписів історично були орієнтовані саме на аналіз оригіналів документів, де можливо дослідити не лише графічну будову підпису, а й динамічні, натискні, трасологічні та інші характеристики письмово–рухового акту.

Особливість проведення почеркознавчої експертизи підписів у цифрових копіях документів полягає насамперед у суттєвому обмеженні обсягу доступної криміналістично значущої інформації. На відміну від оригіналу документа, цифрова копія не дозволяє експерту безпосередньо оцінити характер натиску письмового приладу, послідовність накладення штрихів, мікрорельєф поверхні паперу, наявність тремтіння ліній, продавлювання чи інших ознак, які мають істотне значення для встановлення способу виконання підпису [1]. У таких умовах експерт вимушений зосереджуватись переважно на морфологічних та загально–графічних характеристиках підпису, що значно ускладнює процес ідентифікації виконавця та підвищує ризик помилкових висновків.

Дослідження цифрових копій документів має комплексний характер, оскільки поєднує елементи почеркознавчого, технічного та комп'ютерно–технічного аналізу. Перед експертом постає завдання не лише встановити можливого виконавця підпису, а й оцінити якість цифрового зображення, спосіб його отримання, можливі ознаки редагування або монтажу, а також технічні параметри файлу. У багатьох випадках саме попереднє технічне дослідження дозволяє встановити, чи є цифрова копія придатною для подальшого почеркознавчого аналізу.

Однією з ключових проблем є втрата індивідуалізуючих ознак підпису в процесі сканування або фотографування документа. Під час цифрового копіювання відбувається спрощення структури штрихів, зниження роздільної здатності, поява артефактів компресії, спотворення контурів та зміна контрастності зображення. Особливо негативний вплив мають повторне копіювання, пересилання документів через месенджери, використання автоматичних фільтрів обробки зображення та конвертація файлів між різними форматами. У результаті окремі ознаки підпису можуть бути частково або повністю втрачені, що обмежує можливість проведення повноцінного порівняльного дослідження.

Суттєвого значення набуває оцінка якості цифрової копії документа. Для проведення якісного почеркознавчого дослідження необхідно, щоб зображення містило достатню кількість графічної інформації, забезпечувало чіткість відображення штрихів та не мало значних технічних дефектів. Експерт повинен враховувати роздільну здатність файлу, ступінь контрастності, рівень цифрового шуму, геометричні спотворення, наявність тіней або відблисків. Особливо складними є випадки дослідження фотографій документів, зроблених мобільними

телефонами під кутом або в умовах недостатнього освітлення, оскільки такі фактори можуть істотно деформувати форму підпису.

Важливою особливістю є необхідність встановлення автентичності цифрової копії документа. Сучасні програмні засоби дозволяють легко здійснювати вставлення, копіювання, редагування або модифікацію підписів у графічних редакторах. У зв'язку з цим експерт повинен перевіряти наявність ознак комп'ютерного монтажу, дублювання окремих фрагментів, накладення графічних шарів, неприродних меж штрихів або невідповідностей у структурі зображення. Такі ознаки можуть свідчити про штучне створення підпису або його перенесення з іншого документа.

Окрему проблему становить дослідження так званих факсимільних або вставлених підписів, які можуть бути відсканованими зразками справжнього підпису та повторно використаними у різних документах. У цифрових копіях такі підписи зовні можуть виглядати як справжні рукописні виконання, однак при детальному аналізі виявляються ознаки тотожності окремих елементів, ідентичного розташування штрихів та відсутності природної варіативності рухів. Для справжнього підпису характерна певна мінливість графічних ознак навіть у межах виконання однією особою, тоді як вставлені підписи мають надмірно однакову структуру.

Особливе значення у проведенні таких експертиз має питання достатності та якості порівняльних зразків. У випадку дослідження цифрових копій експерту необхідно отримати максимально можливу кількість вільних, умовно–вільних та експериментальних зразків підпису особи. При цьому бажано, щоб порівняльні матеріали також були виконані у формах, максимально наближених до досліджуваного об'єкта. Недостатність порівняльних матеріалів значно знижує достовірність висновків, особливо якщо спірний підпис містить малу кількість індивідуальних ознак або виконаний у спрощеній формі.

У сучасній експертній практиці дедалі ширше використовуються цифрові технології аналізу зображень, що дозволяють частково компенсувати обмеження дослідження копій документів. Застосування спеціалізованого програмного забезпечення дає можливість збільшувати окремі фрагменти підпису, покращувати контрастність, аналізувати структуру штрихів, виявляти ознаки монтажу та проводити комп'ютерне порівняння графічних елементів. Водночас такі технології мають допоміжний характер і не можуть повністю замінити традиційний експертний аналіз.

Складність дослідження підписів у цифрових копіях документів обумовлює необхідність обережного формулювання експертних висновків. У багатьох випадках експерт не має можливості дійти категоричного висновку через недостатність інформативних ознак або неналежну якість зображення. Тому поширеними є ймовірнісні висновки або висновки про неможливість вирішення поставленого питання. Подібна практика відповідає принципу наукової

обґрунтованості експертного дослідження та спрямована на недопущення необґрунтованих категоричних тверджень.

Особливості оцінки висновків такої експертизи проявляються і в процесуальному аспекті. Суд та сторони кримінального або цивільного провадження повинні враховувати обмеженість дослідження цифрових копій порівняно з аналізом оригіналів документів. Висновок експерта у таких випадках підлягає оцінці у сукупності з іншими доказами, зокрема показаннями осіб, технічними даними електронного документообігу, результатами комп'ютерно–технічних експертиз та інформацією про походження документа.

У практиці розслідування кримінальних правопорушень значна кількість випадків пов'язана саме з використанням цифрових копій документів у шахрайських схемах, фінансових махінаціях, підробленні договорів, банківських документів, довіреностей та інших юридично значущих актів [2]. Злочинці активно використовують можливості сучасних графічних редакторів для створення реалістичних копій підписів, що ускладнює виявлення фальсифікацій. Це обумовлює необхідність постійного вдосконалення методик експертного дослідження та підготовки фахівців, здатних працювати з цифровими об'єктами.

Перспективним напрямом розвитку є інтеграція можливостей штучного інтелекту та автоматизованих систем аналізу підписів. Використання алгоритмів машинного навчання дозволяє виявляти приховані закономірності у структурі штрихів, оцінювати ступінь подібності між підписами та автоматично фіксувати нетипові ознаки. Водночас застосування таких технологій потребує належного нормативного регулювання, стандартизації методик та перевірки їх наукової достовірності.

Не менш важливим є питання нормативного забезпечення проведення експертиз цифрових копій документів. Сучасне законодавство та методичні рекомендації потребують адаптації до умов активного використання електронного документообігу. Необхідним є визначення чітких критеріїв придатності цифрових копій для експертного дослідження, встановлення стандартів якості електронних зображень та врегулювання процесу фіксації цифрових доказів.

Отже, проведення почеркознавчої експертизи підписів у цифрових копіях документів характеризується комплексом специфічних особливостей, пов'язаних із обмеженістю доступної графічної інформації, ризиками цифрової модифікації зображень та необхідністю використання спеціалізованих технічних засобів аналізу. Дослідження таких об'єктів вимагає від експерта поєднання знань у сфері почеркознавства, технічної експертизи документів та цифрової криміналістики. Попри наявні труднощі, розвиток сучасних технологій аналізу зображень та удосконалення методичних підходів створюють передумови для підвищення ефективності й достовірності таких експертних досліджень у майбутньому.

Перелік використаних джерел:

1. Юзишина Т. В. Проблематика проведення судово–почеркознавчої експертизи при ідентифікаційному дослідженні почерку та підписів в електронних документах. Експерт: парадигми юридичних наук і державного управління. 2023. № 1 (25). С. 56–61.

2. Судово–почеркознавча експертиза у кримінальних провадженнях про корупційні правопорушення: метод. рекомендації / В. В. Юсупов, Є. Ю. Свобода, О. М. Шрамко, Ю. О. Пілюков, А. А. Саковський. Київ : Нац. акад. внутр. справ, 2023. 46 с.

DOI https://doi.org/10.32837/11300.33587

Юсупов Володимир
доктор юридичних наук, професор, завідувач відділу Київського науково–дослідного інституту судових експертиз Міністерства юстиції України, м. Київ, Україна,
ORCID: https://orcid.org/0000–0001–5216–4144,
e–mail:yusupov1vv@gmail.com

Кісіль Наталія
кандидат сільськогосподарських наук, старший науковий співробітник, доцент кафедри інтелектуальної власності та приватного права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», провідний науковий співробітник Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України; м. Київ, Україна,
ORCID: https://orcid.org/0000–0003–1097–360X,
e–mail: kisil_n@ukr.net

ІНТЕГРАЦІЯ МЕТОДІВ КРИМІНАЛІСТИКИ У ПРАКТИКУ ПРОВЕДЕННЯ СУДОВИХ ЕКСПЕРТИЗ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У тезах розглянуто особливості застосування криміналістичних методів для фіксації та дослідження цифрових доказів, а також перспективи інтеграції методів криміналістики у практику проведення судових експертиз у сфері інтелектуальної власності.

Ключові слова: судова експертиза, інтелектуальна власність, криміналістика.

Yusupov Volodymyr
Doctor of Law, Professor, Head of Department, Kyiv Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine, Kyiv, Ukraine

Kisil Nataliia
Candidate of Sciences in Agriculture, Senior Researcher, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv Branch of NSC «Hon. Prof. M. S. Bokarius FSI», Kyiv, Ukraine

INTEGRATION OF CRIMINALISTICS METHODS INTO THE PRACTICE OF CONDUCTING FORENSIC EXPERT EXAMINATIONS OF INTELLECTUAL PROPERTY OBJECTS

The theses examine the specific features of the application of forensic methods for the identification and examination of digital evidence, as well as the prospects for integrating forensic methods into the practice of conducting forensic examinations in the field of intellectual property.

Keywords: forensic examination, intellectual property, forensic science.

Сучасний розвиток технологій забезпечує можливість оперативного доступу до новітніх наукових, технічних і технологічних розробок, а також створює умови для масового копіювання та використання різних об’єктів права інтелектуальної власності, зокрема об’єктів авторського і суміжного права, торговельних марок, винаходів, промислових зразків та інших результатів інтелектуальної творчої діяльності. Специфіка Інтернету полягає в надзвичайно високій швидкості обміну інформацією, а також у можливості її оперативної зміни або видалення.

У зв’язку з цим виникає потреба у запровадженні ефективних засобів фіксації випадків незаконного використання об’єктів інтелектуальної власності та встановлення фактів порушення прав на них. Під час виявлення, фіксації та доказування порушень прав інтелектуальної власності особливого значення може набувати інтеграція методів криміналістики у практику проведення судових експертиз.

За понад двадцятирічний період існування напряму судової експертизи у сфері інтелектуальної власності накопичено значний досвід вирішення різноманітних експертних задач. Між тим, на нашу думку, перспективним напрямом подальшого розвитку судової експертизи є більш широке впровадження криміналістичних підходів для дослідження різних об’єктів інтелектуальної творчої діяльності, що сприятиме підвищенню ефективності процесу доказування та забезпеченню достовірності експертних висновків.

Значна частина порушень прав інтелектуальної власності нині вчиняється у мережі Інтернет через різноманітні інтернет–ресурси, зокрема, вебсайти, маркетплейси, онлайн–платформи зі стоковими фото–, відео– та іншим медіа–контентом, у соціальних мережах під час пропонування до продажу, рекламування, реалізації та іншого введення у цивільний оборот товарів і послуг, у яких використовуються охоронювані об’єкти права інтелектуальної власності. Це зумовлює необхідність дослідження закономірностей і механізмів утворення цифрових слідів, а також розроблення методів їх виявлення та фіксації під час розслідування кримінальних правопорушень і судового розгляду справ, пов’язаних із порушенням прав інтелектуальної власності.

До спеціальних знань експерта у сфері інтелектуальної власності не відноситься дослідження змісту веб–сторінки, її внутрішньої структури, аналізу вихідного коду, та інших технічних відомостей. У зв'язку з цим встановлення факту розміщення на відповідному вебсайті певної інформації або об'єктів, а також відсутності модифікацій чи іншого втручання виходить за межі його компетенції. Тому вирішення зазначених питань потребує проведення комплексного експертного дослідження із залученням спеціальних знань у відповідних галузях.

Так, під час доведення факту порушення прав інтелектуальної власності в мережі Інтернет або способу передачі цієї інформації, може виникати необхідність проведення комплексної експертизи або комплексу експертиз із залученням експертів за спеціальністю 10.17 «Дослідження електронних комунікацій» або 10.9 «Дослідження комп'ютерної техніки та програмних продуктів» та експертів за відповідною спеціальністю у сфері інтелектуальної власності, які встановлюють факт використання об'єкту інтелектуальної власності на певному інтернет–ресурсі. За необхідності дослідження інформації, що розміщена на веб–сайті, може проводитися комп'ютерно–технічне дослідження (спеціальність 10.9), а за умови дослідження способів передачі цієї інформації – експертиза електронних комунікацій (спеціальність 10.17), у межах якої можуть встановлюватися, зокрема, протоколи та сервери, що використовуються, а також технічні механізми передачі цих даних.

Особливості проведення комплексних експертиз електронних комунікацій, комп'ютерних програм та об'єктів інтелектуальної власності розглянуто у роботі «Розробка методичних рекомендацій щодо проведення комплексних експертиз, пов'язаних з об'єктами інтелектуальної власності» [1], що проведено колективом авторів Національного наукового центру «ІСЕ ім. Засл. проф. М. С. Бокаріуса» та Львівського науково–дослідного інституту судових експертиз. При цьому слід відмітити, що активний розвиток цифрової криміналістики сприятиме удосконаленню підходів до проведення таких судових експертиз.

Методи криміналістики дають можливість за слідами та іншими відображеннями ідентифікувати об'єкт, що залишив певні сліди, та встановити зв'язок людини, предмета або об'єкта з розслідуваною подією.

Об'єкти права інтелектуальної власності за своєю природою є нематеріальними об'єктами (нематеріальними активами). Водночас для набуття ними правової охорони необхідним є їх вираження в об'єктивній формі або фіксація на певному матеріальному носії. Так, правова охорона об'єкта авторського права виникає з моменту створення твору та його вираження в об'єктивній формі (у рукописі, видінні, малюнку, електронному файлі тощо). Права на торговельну марку виникають з моменту її державної реєстрації з фіксацією відповідного позначення у державному реєстрі. Охорона винаходу (корисної моделі) також виникає з моменту державної реєстрації, при цьому обсяг правової охорони, що надається, визначається формулою винаходу (корисної

моделі), а тлумачення формули здійснюється в межах опису винаходу (корисної моделі) та відповідних креслень. При цьому під час проведення судових експертиз дослідженню підлягають властивості та ознаки безпосередньо об'єктів права інтелектуальної власності: твору, торговельної марки, винаходу (корисної моделі) та інших об'єктів, які за своєю природою є нематеріальними об'єктами.

Окремі експертні завдання, що вирішуються під час розгляду справ, пов'язаних із порушеннями прав інтелектуальної власності, можуть потребувати застосування методів криміналістичної ідентифікації. До завдань криміналістичної ідентифікації в академічних підручниках [2, с. 62] відносять встановлення факту наявності або відсутності тотожності конкретного індивідуально визначеного матеріального об'єкта (людини, предмета, тварини).

У судовій експертизі у сфері інтелектуальної власності питання щодо наявності тотожності або схожості вирішуються, зокрема, під час дослідження торговельних марок. Типовим є питання такого змісту: «Чи є позначення «Х», нанесене на етикетку товару «…» тотожним або схожим настільки, що його можна сплутати із знаком для товарів і послуг за Свідоцтвом України № 000 від 00.00.2000?». Між тим під час вирішення подібних питань, як правило, не здійснюється криміналістична ідентифікація у класичному її розумінні, а переважно вирішуються діагностичні задачі. У цьому випадку фокус спрямований не стільки на установлення тотожності досліджуваних об'єктів, скільки на визначення імовірності сплутування споживачами певних учасників цивільного обороту, їх товарів та послуг при застосуванні схожих позначень.

Водночас вирішення окремих експертних завдань потребує застосування методів криміналістичної ідентифікації. Наприклад, під час експертизи сортів рослин з метою встановлення факту використання певного сорту рослин, можуть здійснюватися молекулярно–генетичні дослідження, спрямовані на визначення збігу ознак досліджуваних зразків за ДНК–маркерами.

Таким чином, перспективним напрямом удосконалення підходів до проведення судових експертиз, пов'язаних з об'єктами інтелектуальної власності, є подальша інтеграція методів криміналістики у судово–експертну практику. У цьому контексті важливого значення набуває застосування методів криміналістичної ідентифікації, а також напрацювань цифрової криміналістики, комп'ютерно–технічної експертизи та експертизи електронних комунікацій, що забезпечують ефективну фіксацію, збереження та дослідження цифрових доказів порушення прав інтелектуальної власності.

Перелік використаних джерел:

1.Розробка методичних рекомендацій щодо проведення комплексних експертиз, пов'язаних з об'єктами інтелектуальної власності : звіт НДР (закл.) / МЮ України, ННЦ «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса»;

кер. Н.В. Кісіль; викон.: Т.М. Чабанець, О.С. Пукліч [та ін.], № ДР 0226U002441. 2025. 152 с.

2.Криміналістика: підручник / В.М. Шевчук, В.А. Журавель, В.Ю. Шепитько та інш.; за ред. В. М. Шевчука ; Нац. юрид. ун–т ім. Ярослава Мудрого. Харків : Право, 2024. 1008 с.

Секція 4
КРИМІНАЛЬНО–ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ВИКЛИКИ ЦИФРОВІЗАЦІЇ: ВІД КІБЕРТЕРОРИЗМУ ДО АВТОНОМНИХ СИСТЕМ ОЗБРОЄННЯ

DOI https://doi.org/10.32837/11300.33600

Артюх Надія
здобувачка вищої освіти 4 курсу
Криворізького навчально–наукового інституту
Національного університету «Одеська юридична академія»,
м. Кривий Ріг, Україна
ORCID: https://orcid.org/0009–0004–4897–5337
E–mail:nadik20044@gmail.com

Козаченко Віталій
кандидат юридичних наук,
старший викладач кафедри кримінально–правових дисциплін
Криворізького навчально–наукового інституту
Національного університету «Одеська юридична академія»,
м. Кривий Ріг, Україна
ORCID: https://orcid.org/0009–0003–9802–2020
e–mail: vitalii.kozachenko92@gmail.com

КІБЕРБУЛІНГ У СИСТЕМІ ДЕТЕРМІНАНТ ДЕВІАНТНОЇ ПОВЕДІНКИ МОЛОДІ

У тезах досліджено кібербулінг як одну з ключових детермінант девіантної поведінки молоді в умовах цифрового суспільства. Проаналізовано кримінологічні ознаки, соціально–психологічні наслідки онлайн–насильства та напрями його профілактики.

Ключові слова: кібербулінг, девіантна поведінка, молодь, онлайн–насильство, кримінологія.

Artiukh Nadiia
Fourth–year undergraduate student
of the Kryvyi Rih Educational and Scientific Institute of the
National University «Odesa Law Academy»,
Kryvyi Rih, Ukraine

Kozachenko Vitalii
PhD in Law, Senior Lecturer
of the Department of Criminal Law Disciplines,

Kryvyi Rih Educational and Scientific Institute of the
National University «Odesa Law Academy»,
Kryvyi Rih, Ukraine

CYBERBULLYING IN THE SYSTEM OF DETERMINANTS OF YOUTH DEVIANT BEHAVIOR

The theses examine cyberbullying as one of the key determinants of deviant behavior among young people in the digital society. The criminological characteristics, socio–psychological consequences of online violence, and directions for its prevention are analyzed.

Keywords: cyberbullying, deviant behavior, youth, online violence, criminology.

Сучасний етап розвитку інформаційного суспільства характеризується інтенсивним поширенням цифрових технологій та активною інтеграцією мережі Інтернет у всі сфери суспільного життя. Особливо помітним цей процес є серед молоді, для якої віртуальний простір став не лише засобом комунікації, але й важливим середовищем соціалізації, самовираження та формування особистості. Разом із позитивними аспектами цифровізації суспільства дедалі більшого поширення набувають негативні явища, пов'язані із використанням інформаційно–комунікаційних технологій. Одним із найбільш небезпечних серед них є кібербулінг, який сьогодні визнається серйозною соціальною, психологічною та кримінологічною проблемою.

У сучасній кримінологічній науці кібербулінг розглядається як форма агресивної та девіантної поведінки, що реалізується у цифровому середовищі шляхом систематичного психологічного впливу на особу через електронні засоби комунікації. До найбільш поширених форм кібербулінгу належать образи, приниження, погрози, переслідування, поширення недостовірної або компрометуючої інформації, публічне висміювання, створення фейкових акаунтів, а також навмисне виключення особи із віртуальних спільнот [1, с. 205]. Особливу небезпеку цього явища зумовлює його латентний характер, можливість анонімного вчинення та практично необмежена аудиторія спостерігачів.

На відміну від традиційного булінгу, кібербулінг не обмежується конкретним місцем або часом. Якщо фізичне чи психологічне цькування у реальному середовищі часто припиняється після завершення навчального процесу або особистого контакту, то цифрове переслідування може тривати безперервно, створюючи для потерпілої особи стан постійної психологічної напруги. Саме ця безперервність впливу значною мірою посилює деструктивні наслідки кібербулінгу для психоемоційного стану молоді [2].

У кримінологічному аспекті кібербулінг доцільно розглядати як одну із детермінант девіантної поведінки молоді. Поняття детермінації у кримінології охоплює систему причин, умов та факторів, що впливають на формування

протиправної або асоціальної поведінки особи. В умовах сучасного цифрового суспільства кібербулінг стає специфічним криміногенним фактором, який здатний впливати як на жертву, так і на самого агресора, формуючи у них стійкі деструктивні поведінкові установки.

Жертви кібербулінгу часто зазнають серйозних психологічних наслідків, серед яких депресивні стани, тривожність, емоційна нестабільність, зниження самооцінки та розвиток соціальної ізоляції. У багатьох випадках систематичний психологічний тиск у цифровому середовищі призводить до втрати довіри до соціального оточення, відчуття безпорадності та формування девіантних форм реагування на стресові ситуації [3]. Особливо небезпечним є те, що молодь через недостатній рівень психологічної зрілості часто не здатна самостійно протистояти тривалому онлайн–переслідуванню.

Численні дослідження підтверджують існування взаємозв'язку між кібербулінгом та аутоагресивною поведінкою молоді. Особи, які регулярно стають об'єктами онлайн–цькування, значно частіше демонструють схильність до самоушкодження, суїцидальних думок, розладів харчової поведінки та вживання психоактивних речовин [2]. У цьому контексті кібербулінг можна розглядати як фактор психологічної віктимізації, який створює сприятливі умови для подальшої соціальної дезадаптації особистості.

Водночас негативний вплив кібербулінгу проявляється не лише щодо потерпілих осіб, але й щодо самих агресорів. Постійне вчинення актів цифрового насильства формує у молоді толерантність до жорстокості, знижує рівень емпатії та поступово руйнує морально–етичні обмеження щодо допустимості агресивної поведінки. Анонімність інтернет–середовища створює ілюзію безкарності, що сприяє закріпленню девіантних моделей поведінки.

Окремої уваги заслуговує проблема групового кібербулінгу, коли онлайн–переслідування здійснюється не однією особою, а колективом користувачів соціальних мереж або месенджерів. У таких випадках психологічний вплив на потерпілу особу значно посилюється через масовий характер приниження та суспільного осуду. Крім того, групова форма кібербулінгу сприяє поширенню колективної агресії та закріпленню девіантних моделей комунікації серед молоді.

Серед основних соціально–психологічних детермінант поширення кібербулінгу доцільно виділити недостатній рівень сімейного контролю, дефіцит емоційної підтримки, проблеми у міжособистісному спілкуванні, низький рівень цифрової культури та популяризацію агресивного контенту у соціальних мережах. Важливим фактором також є вплив сучасної медіакультури, у якій прояви агресії нерідко сприймаються як допустима форма самоствердження або спосіб привернення уваги.

Суттєве значення має і проблема правової необізнаності молоді щодо відповідальності за вчинення кібербулінгу. В Україні правові засади протидії булінгу та кібербулінгу визначаються, зокрема, положеннями Закону України

«Про освіту», відповідно до якого булінг визнається однією з форм насильства в освітньому середовищі [4], а також ст. 173–4 Кодексу України про адміністративні правопорушення, що передбачає адміністративну відповідальність за вчинення булінгу учасників освітнього процесу [5]. Значна частина підлітків та молодих осіб не усвідомлює, що окремі прояви онлайн–переслідування можуть утворювати склад адміністративного правопорушення. Відсутність належного рівня правової культури у поєднанні з відчуттям анонімності формує сприятливі умови для подальшого поширення цифрового насильства.

Крім того, важливим кримінологічним аспектом є латентність кібербулінгу. Більшість випадків онлайн–цькування залишаються поза увагою правоохоронних органів, педагогів та батьків. Потерпілі часто не повідомляють про факти переслідування через страх осуду, недовіру до механізмів захисту чи їх незнання, або переконання у неефективності реагування. У результаті формується ситуація прихованої віктимізації, що сприяє подальшому розвитку девіантних проявів у молодіжному середовищі.

Важливим напрямом кримінологічного дослідження є аналіз взаємозв’язку між кібербулінгом та іншими формами девіантної поведінки молоді. Зокрема, сучасні наукові дослідження вказують на існування кореляції між участю у кібербулінгу та схильністю до агресивної поведінки, інтернет–залежності, порушення соціальних норм та вчинення інших правопорушень [2]. Це свідчить про те, що кібербулінг не є ізольованим явищем, а виступає складовою ширшого комплексу криміногенних факторів сучасного цифрового суспільства.

У зв’язку з цим особливого значення набуває проблема профілактики кібербулінгу серед молоді. Ефективна система запобігання повинна поєднувати правові, психологічні, соціальні та освітні механізми впливу. Насамперед необхідним є підвищення рівня цифрової грамотності молоді та формування навичок безпечної поведінки у мережі Інтернет. Освітні заклади повинні проводити системну інформаційно–просвітницьку роботу щодо ризиків онлайн–насильства та способів протидії йому.

Не менш важливим є удосконалення правового механізму реагування на випадки кібербулінгу. Доцільним видається розширення форм співпраці між закладами освіти, правоохоронними органами, психологічними службами та адміністраціями цифрових платформ. Важливого значення також набуває створення спеціалізованих програм психологічної підтримки потерпілих осіб та впровадження механізмів раннього виявлення молоді, схильної до агресивної поведінки у цифровому середовищі.

Перспективним напрямом подальших кримінологічних досліджень є вивчення впливу соціальних мереж на трансформацію девіантної поведінки молоді, а також аналіз новітніх форм цифрової агресії, пов’язаних із використанням штучного інтелекту, анонімних платформ та технологій маніпулятивного впливу. Актуальним залишається також питання розроблення ефективних міжнародних механізмів співпраці у сфері протидії кібербулінгу,

оскільки цифрове середовище не має територіальних меж і потребує комплексного міждержавного реагування.

Таким чином, кібербулінг є одним із найбільш небезпечних криміногенних факторів сучасного цифрового суспільства, який впливає на формування девіантної поведінки молоді та потребує комплексної системи кримінологічної профілактики. Ефективна протидія цьому явищу можлива лише за умови поєднання правових, психологічних, освітніх та соціальних механізмів впливу.

Перелік використаних джерел:

1. Шкарупа В., Воробйова А. Кібербулінг як форма здійснення психологічного насильства. Психологічні та педагогічні проблеми професійної освіти та патріотичного виховання персоналу системи МВС України : матеріали Всеукр. наук.–практ. конф. (м. Вінниця, 24 берез. 2023 р.). – Вінниця : ХНУВС, 2023. – С. 204–206. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/3ba6e5ba–76ec–4db3–826b–28c5994e07ad/content

2. Kowalski R. M., Giumetti G. W., Schroeder A. N., Lattanner M. R. Bullying in the Digital Age: A Critical Review and Meta–Analysis of Cyberbullying Research Among Youth. Psychological Bulletin. 2014. Vol. 140(4). P. 1073–1137. URL: https://www.researchgate.net/publication/260151324_Bullying_in_the_Digital_Age_A_Critical_Review_and_Meta–Analysis_of_Cyberbullying_Research_Among_Youth

3. Hinduja S., Patchin J. W. Cyberbullying: Identification, Prevention, and Response. Cyberbullying Research Center. 2022. 9 p. URL: https://cyberbullying.org/Cyberbullying–Identification–Prevention–Response–2022.pdf

4. Про освіту : Закон України від 05 вересня 2017 р. № 2145–VIII. URL: https://zakon.rada.gov.ua/laws/show/2145–19

5. Кодекс України про адміністративні правопорушення : Закон України від 07 грудня 1984 р. № 8073–X. URL: https://zakon.rada.gov.ua/laws/show/80731–10

DOI https://doi.org/10.32837/11300.33595

Бершавська Анастасія
аспірант кафедри оперативно–розшукової та поліцейської діяльності
Національного університету «Одеська юридична академія»,
м.Одеса, Україна
ORCID: https://orcid.org/00009–0007–7331–3138
e–mail: samoilenko_elena@ukr.net

ОРГАНІЗАЦІЙНО–ТАКТИЧНІ ОСОБЛИВОСТІ ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ ІЗ ПОСОБНИЦТВОМ ДЕРЖАВІ–АГРЕСОРУ

У тезах досліджено сучасні організаційно–тактичні особливості протидії злочинам, пов'язаним із пособництвом державі–агресору, в умовах воєнного стану. Обґрунтовано необхідність використання сучасних технологій кримінального аналізу, цифрової криміналістики, кіберрозвідки та систем прогнозування ризиків для виявлення прихованих зв'язків між суб'єктами злочинної діяльності. Досліджено особливості моделей поведінки осіб, які здійснюють пособництво державі–агресору,

Ключові слова: пособництво державі–агресору, оперативно–розшукова діяльність, національна безпека.

Bershavska Anastasiia
Postgraduate Student of the Department of
Operational–Investigative and Police Activity,
National University «Odesa Law Academy»
Odesa, Ukraine

ORGANIZATIONAL AND TACTICAL FEATURES OF COUNTERING CRIMES RELATED TO AIDING THE AGGRESSOR

The theses examine modern organizational and tactical features of countering crimes related to aiding the aggressor state under martial law. The role of information and analytical support, interagency cooperation, and operational–investigative activity in detecting and documenting collaboration and agent–related activities is analyzed. The necessity of using modern criminal analysis technologies, digital forensics, cyber intelligence, and risk forecasting systems to identify hidden criminal connections is substantiated. The study explores behavioral models of persons involved in aiding the aggressor state, as well as the role of operational units of penitentiary institutions in countering hybrid threats, radicalization, and criminal influence under conditions of armed aggression. Directions for improving information–analytical systems and integrating operational units into the national security framework are proposed.

Keywords: aiding the aggressor state, operational–investigative activity, national security.

Повномасштабна збройна агресія Російської Федерації проти України актуалізувала проблему виявлення, документування та припинення злочинів, пов'язаних із пособництвом державі–агресору. Такі кримінальні правопорушення становлять підвищену суспільну небезпеку, оскільки посягають не лише на основи національної безпеки, але й створюють умови для дестабілізації діяльності державних інституцій, інформаційного впливу на населення, підтримки окупаційних адміністрацій та забезпечення функціонування ворожих агентурних мереж.

Сучасні форми пособництва державі–агресору характеризуються високим рівнем латентності, використанням цифрових технологій, дистанційних засобів комунікації, криптовалютних розрахунків, а також активним застосуванням механізмів конспірації. У зв'язку з цим протидія зазначеним злочинам потребує комплексного організаційно–тактичного підходу, який поєднує можливості оперативно–розшукової діяльності, кримінального аналізу, інформаційно–аналітичного забезпечення та міжвідомчої взаємодії.

Важливого значення набуває розуміння криміналістично значущої інформації про злочини, пов'язані з пособництвом державі–агресору. У криміналістиці така інформація традиційно визначається як сукупність відомостей процесуального та непроцесуального характеру про подію злочину, його учасників, спосіб вчинення, механізм слідоутворення та інші обставини, що мають значення для доказування. Аналіз механізму вчинення злочинів цієї категорії дозволяє встановити закономірності між способом дій правопорушника, цифровими слідами, характером комунікації із представниками держави–агресора, використаними технічними засобами та особою злочинця.

Аналіз матеріалів слідчо–судової практики свідчить, що особи, які вчиняють пособництво державі–агресору, використовують декілька моделей злочинної поведінки.

Перша модель характеризується відкритим та демонстративним характером діяльності. Особи не приховують факту співпраці з державою–агресором, публічно підтримують окупаційні адміністрації, поширюють пропагандистські матеріали або беруть участь у діяльності незаконних органів влади. У таких випадках основне значення мають заходи оперативного реагування, документування публічної діяльності, фіксація цифрових слідів та організація розшуку підозрюваних.

Друга модель передбачає повне приховування злочинної діяльності. Комунікація здійснюється через захищені канали зв'язку, а передача інформації чи матеріальних ресурсів – із використанням конспіративних методів. У цьому випадку ключову роль відіграють негласні слідчі (розшукові) дії, кіберрозвідка, аналіз цифрових слідів, радіоелектронна розвідка та кримінальний аналіз.

Третя модель полягає у приховуванні причетності до окремих епізодів злочинної діяльності при зовнішньо легальній поведінці. Особливого значення тут набуває встановлення часових і просторових зв'язків між учасниками події, аналіз фінансових операцій, телефонних контактів, маршрутів переміщення та поведінкових характеристик особи.

Організаційно–тактична протидія таким злочинам неможлива без ефективної міжвідомчої взаємодії між оперативними підрозділами СБУ, НПУ, ДБР, ДКВС України та іншими суб'єктами сектору безпеки й оборони. Ефективне документування злочинів, пов'язаних із пособництвом державі–агресору, потребує інтеграції оперативно–розшукової інформації з можливостями інших правоохоронних органів, насамперед у сфері кіберрозвідки, контррозвідувального забезпечення та кримінального аналізу.

Суттєвого значення набуває інформаційно–аналітичне забезпечення протидії злочинам цієї категорії. Сучасні інформаційні системи повинні забезпечувати накопичення, систематизацію та аналіз відомостей щодо осіб, схильних до підтримки держави–агресора, їхніх соціальних зв'язків, каналів комунікації, фінансових операцій, контактів із представниками кримінального середовища та осіб, які перебувають на тимчасово окупованих територіях.

Сучасна злочинна діяльність дедалі більше переходить у цифровий простір. Використання месенджерів із наскрізним шифруванням, криптовалют, VPN–сервісів та анонімних платформ суттєво ускладнює документування злочинної діяльності. У зв'язку з цим важливими напрямами оперативно–розшукової діяльності стають Mobile Device Forensics, Blockchain Forensics, радіоелектронна розвідка та цифрова криміналістика.

Таким чином, ефективна протидія злочинам, пов'язаним із пособництвом державі–агресору, потребує комплексного організаційно–тактичного забезпечення, що включає: міжвідомчу взаємодію, інтеграцію інформаційно–аналітичних систем, використання сучасних цифрових технологій, удосконалення кримінального аналізу та впровадження сучасних методів оперативно–розшукової діяльності. Лише поєднання технологічних можливостей та належної координації правоохоронних органів дозволить ефективно протидіяти сучасним формам колаборційної та агентурної діяльності в умовах воєнного стану.

DOI https://doi.org/10.32837/11300.33594

Горбачова Ірина
кандидат юридичних наук, доцент, професор кафедри кримінального права Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–6589–3143
e–mail: irynagorbachova15@gmail.com

ІНФОРМАЦІЙНІ ВКИДИ ТА ЦИФРОВА ДЕЗІНФОРМАЦІЯ ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ

У тезах досліджується проблема поширення дезінформації та фейкових повідомлень в умовах цифровізації суспільства й воєнного стану, а також їх вплив на інформаційну безпеку держави, громадський порядок і суспільну стабільність. Аналізується роль дезінформації як елементу гібридної війни та інструменту дискредитації держави як на внутрішньодержавному, так і на міжнародному рівні. Визначається, що в умовах інформаційної війни фейки можуть виступати інструментом сприяння агресії, дестабілізації держави та вчинення кримінально протиправних посягань проти основ національної безпеки України.

Ключові слова: дезінформація, агресія, національна безпека, свобода висловлювань, мова ворожнечі.

Gorbachova Iryna
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminal Law,
National University «Odesa Law Academy»,
Odesa, Ukraine

INFORMATION INJECTIONS AND DIGITAL DISINFORMATION AS AN ELEMENT OF HYBRID WARFARE

This abstract analyzes the problem of the spread of disinformation and fake news in the context of a digital society and martial law, as well as their influence on the information and national security of the state, public order, and social stability. It examines the role of disinformation as an element of hybrid warfare and a tool for discrediting the state at both the domestic and international levels. It is determined that in the context of information warfare, fake news can serve as a tool to facilitate aggression, destabilize the state, and commit criminal acts against the security of Ukraine.

Keywords: disinformation, aggression, national security, freedom of expressing opinions, hate speech.

Поширення фейкової інформації та маніпулятивних інформаційних вкидів за допомогою сучасних цифрових технологій становить серйозну загрозу як для окремої особи (її честі, гідності), так і для суспільства та держави в цілому. Небезпечність таких явищ обумовлена насамперед масштабністю, швидкістю розповсюдження та складністю контролю за поширенням дезінформації в цифровому просторі. Цифрові технології, соціальні мережі, месенджери, можливості штучного інтелекту дозволяють миттєво охоплювати широку аудиторію споживачів, формуючи викривлене уявлення щодо фактів, подій, процесів. Як наслідок поширення фейків та дезінформація дестабілізується суспільство, формуються панічні настрої, підривається довіра до органів державної влади, органів місцевого самоврядування, провокується соціальна напруга та конфлікти, що здатне вплинути на політичні процеси та результати демократичних процедур.

В умовах воєнного стану та збройної агресії фейки та дезінформація використовуються як елемент інформаційно–психологічних операцій, спрямованих на деморалізацію населення, дестабілізацію суспільства, дискредитацію Сил Оборони, нагнітання панічних настроїв та невдоволення ситуацією в державі. При цьому негативний вплив дезінформації посилюється високою швидкістю її поширення, в той час як спростування неправдивих відомостей зазвичай відбувається значно повільніше та не завжди здатне усунути вже сформований деструктивний інформаційний вплив. Це створює загрозу інформаційній безпеці держави, стабільності суспільства, реалізації прав людини та нормальному функціонуванню демократичних інститутів.

Дезінформація являє собою умисне поширення недостовірних, викривлених або маніпулятивно поданих відомостей з метою введення суспільства чи окремої аудиторії в оману, впливу на громадську думку, отримання політичних, економічних чи інших переваг або заподіяння шкоди суспільним інтересам. У сучасному цифровому середовищі дезінформація нерідко реалізується у формі так званих «фейків» та інформаційних «вкидів», які зовні імітують об’єктивні журналістські матеріали, новини чи аналітичний контент, створюючи у користувача враження достовірності та офіційності джерела. Водночас такі повідомлення можуть містити повністю вигадані факти, перекручену інформацію, маніпулятивні інтерпретації або навмисно вирвані з контексту відомості. Найбільш поширеними сферами поширення дезінформації є питання охорони здоров’я та медицини, пандемій і біологічних загроз (тваринні та пташині грипи, коронавірус, хантавірус); діяльності органів державної влади та під час виборчих процесів. В умовах збройної агресії такі сфери розширено за рахунок інформаційних «вкидів» щодо міжнародної підтримки та фінансування, воєнно–політичної ситуації та безпеки і обороноздатності держави. Наприклад, теми – коронавірус, медицина, влада, вибори, фінансування та ін. [1], «мальчікі в трусіках», розправи з МОК, «все пропало» [2], «трудові мігранти» та ін.

Фейкові новини є інструментом інформаційного впливу, який підриває суспільну довіру не тільки до «героїв» такої дезінформації, але й до медіа та демократичних інститутів, призводить до «інформаційного хаосу», коли суспільство перестає відрізняти правдиву інформацію від «вкидів», маніпуляції та пропаганди.

В умовах інформаційної війни дезінформація використовується не як випадкове поширення неправдивих відомостей (для рейтингів), а як цілеспрямований інструмент впливу на суспільну свідомість. Дезінформація виступає формою інформаційної зброї, метою якої є підрив довіри до законних державних інституцій, деморалізація населення, дестабілізація внутрішньої ситуації та вплив на міжнародну підтримку держави. В такий спосіб дезінформація стає елементом гібридної агресії. Наразі, поширення фейкових повідомлень про військові поразки, масові втрати або «зраду» спрямоване на пригнічення волі до спротиву.

Фейкові повідомлення та інформаційні вкиди, що поширюються державою–агресором, можуть бути спрямовані не лише на дестабілізацію внутрішньої ситуації в державі, а й на її дискредитацію на міжнародному рівні. Така дезінформація часто реалізується шляхом поширення неправдивих відомостей щодо нібито вчинення воєнних злочинів, маніпулювання гуманітарною проблематикою, поширення фейків про незаконний обіг чи продаж гуманітарної та військової допомоги, а також формування у міжнародної спільноти образу держави як «нестабільної», «корумпованої» або «недемократичної». Подібний інформаційний вплив здатний негативно позначатися на міжнародному авторитеті держави, підривати рівень довіри з боку іноземних партнерів, впливати на обсяги зовнішньої підтримки, міжнародне співробітництво та перебіг дипломатичних процесів. У сучасних умовах інформаційний простір фактично перетворюється на окремий напрям ведення гібридної війни, у межах якого дезінформація використовується як інструмент політичного та психологічного впливу.

На внутрішньодержавному рівні поширення дезінформації також створює суттєві загрози національній безпеці. Інформаційні маніпуляції можуть впливати на процес ухвалення рішень органами державної влади, провокувати суспільну напругу, дестабілізувати громадський порядок, ускладнювати діяльність правоохоронних органів та створювати передумови для виникнення панічних настроїв, протестної активності чи масових заворушень. Особливо небезпечним є поширення фейкової інформації в умовах воєнного стану, коли інформаційна стабільність безпосередньо пов’язана із забезпеченням обороноздатності та суспільної безпеки держави.

Поширення дезінформації в умовах воєнного стану не може розглядатися виключно як прояв свободи слова чи реалізація права на висловлення власної позиції, оскільки така діяльність здатна створювати реальні загрози національній безпеці, громадському порядку, обороноздатності держави та життю людей.

Особливо небезпечним є умисне поширення фейкової інформації особами, які мають значний вплив на формування громадської думки, зокрема журналістами, блогерами, політичними діячами, адміністраторами великих інформаційних ресурсів та іншими публічними суб'єктами. Суспільна небезпечність таких дій обумовлюється не лише самим фактом поширення неправдивих відомостей, а й масштабом аудиторії, рівнем довіри до відповідної особи та потенційними наслідками інформаційного впливу.

У зв'язку з цим особи, які свідомо здійснюють поширення дезінформації, особливо в інтересах держави–агресора або з усвідомленням можливих суспільно небезпечних наслідків, повинні нести відповідальність, зокрема і кримінальну. Такий підхід обумовлений необхідністю забезпечення належного захисту інформаційної безпеки держави та недопущення використання свободи інформаційної діяльності як інструменту інформаційної війни чи прихованого деструктивного впливу на суспільство.

Свобода вираження поглядів, гарантована ст. 10 ЄКПЛ та ст. 34 Конституції України, є однією з основ демократичного суспільства. Крім того, ЄСПЛ наголошував, що ця свобода охоплює «інформацію», що може «обурювати, шокувати або турбувати». Втім свобода слова не має абсолютного характеру (обмеження передбачені законом, переслідують легітимну мету, є необхідними у демократичному суспільстві). Свобода вираження не охоплює умисне поширення неправдивих відомостей, якщо воно: створює загрозу національній безпеці, спричиняє паніку серед населення, підриває обороноздатність та розпалює ворожнечу або насильство.

Найбільш типовою формою реагування на фейки є цивільний позов про захист честі, гідності та ділової репутації, спростування недостовірної інформації та відшкодування моральної шкоди. Втім в умовах ведення інформаційної війни як складової збройної агресії з використанням журналістів, блогерів, політичних діячів, питання відповідальності таких осіб переходить в площину регулювання кримінального законодавства у випадках, коли дезінформація підбурює до насильницьких дії проти держави – ст.ст. 109, 110, 111–2 – 113 КК, розпалює ворожнечу – ст. 161 КК, створює загрозу громадській безпеці – ст. 258–2 КК, сприяє агресії або воєнним злочинам країни–окупанта – ст.ст.436, 436–2 КК, спричиняє масові заворушення – ст.ст. 294, 295 КК.

Перелік використаних джерел:

1. Колотвін П. Фейки та маніпуляції накрили одеський медіапростір перед місцевими виборами. URL: https://imi.org.ua/monitorings/fejky–ta–manipulyatsiyi–nakryly–odeskyj–media–prostir–pered–mistsevymy–vyboramy–i35123, Соколовська І. Найрезонансніші псевдоновини, у які всі повірили: як шукати правду у ЗМІ. URL: https://dyvys.info/2019/11/19/najrezonansnishi–psevdonovyny–u–yaki–vsi–poviryly–yak–shukaty–pravdu–u–zmi/, Котубей–Герцька О. Про що цього року брехала Росія: фейки, дезінформація та вкиди про

російсько–українську війну і як їм протидіяти. URL: https://suspilne.media/culture/636550–pro–so–cogo–roku–brehala–rosia–fejki–dezinformacia–ta–vkidi–pro–rosijsko–ukrainsku–vijnu–i–ak–im–protidiati/

2. Фейкові новини. BBC News Україна. URL: https://www.bbc.com/ukrainian/topics/c6vzyzw21qnt, Фейкові новини. Детектор медіа. URL:https://detector.media/tag/29528/, Фактчек. Гвара Медіа. URL: https://gwaramedia.com/factcheck/

DOI https://doi.org/10.32837/11300.33561

Єрофеєва Ольга
аспірантка кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID https://orcid.org/0009–0008–9506–3114
e–mail: olga_yeroveyewa@ukr.net

МОТИВИ ЗЛОЧИННОГО ПОСЯГАННЯ У КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЯХ, ПОВ'ЯЗАНИХ ІЗ ЗАВОЛОДІННЯМ СПАДКОВИМ МАЙНОМ

У тезах розглянуто мотиви злочинного посягання, проаналізовано сутність та види корисливих мотивів, які спонукають правопорушників до незаконного привласнення спадщини та усунення законних спадкоємців.

Ключові слова: спадкове майно, корисливий мотив, шахрайство, спадкування, криміналістичні методи.

Yerofeieva Olha
postgraduate student of the Department of Criminalistics, Forensic Examinations, and Polygraphology, National University «Odesa Law Academy,» Odesa, Ukraine

MOTIVES OF CRIMINAL ENCOURAGEMENT IN CRIMINAL OFFENSES RELATED TO THE CONFISCATION OF INHERITABLE PROPERTY

The theses consider the motives of criminal encroachment, analyze the essence and types of selfish motives that encourage offenders to illegally appropriate inheritance and eliminate legitimate heirs.

Key words: inheritance, selfish motive, fraud, inheritance, forensic methods.

У межах дослідження кримінальних правопорушень, пов'язаних із незаконним заволодінням спадковим майном, мотив виступає як усвідомлена потреба суб'єкта в отриманні матеріальних благ спадкодавця.

Визначення мотиву є важливим джерелом доказової бази у кримінальному провадженні на стадії досудового розслідування [2, с. 94]. Вчені О.М. Бандурка та О.М. Литвинов вважають, що мотив є центральною ланкою мотивації поведінки [1, с. 110]. Вчена Я.В. Крушельницька визначає мотив, як спонукання людини до активності, пов'язане з намаганням задовольнити певні потреби [2, с. 95]. Науковець В.А. Якушин трактує поняття мотиву через поняття суб'єктивного зобов'язання роз'яснюючи, що юридичне значення у процесі

доведення вини мають лише ті обставини діяння, які усвідомлювались винним [3, с. 529]. Науковець О.С. Коробка мотив визначає як внутрішні спонукання, якими керується суб'єкт при вчиненні кримінального правопорушення; мотив завжди передує здійсненню правопорушення і, оскільки є його підставою, служить виправданням його здійснення в очах самого суб'єкта. Вчений Р.В. Вереша визначає мотив як свідоме і вольове спонукання до досягнення мети, обумовлене потребами особистості, що має суспільно–небезпечний характер і тягне за собою кримінальну відповідальність [3, с. 530].

Аналіз судової практики дозволяє диференціювати ключові мотиви злочинних посягань у кримінальних правопорушеннях щодо заволодіння спадковим майном на наступні групи:

– корисливі мотиви, до яких відноситься безпосереднє прагнення до незаконного збагачення шляхом повного або часткового усунення інших законних спадкоємців від спадку, бажання розв'язати власні фінансові проблеми за рахунок спадкового майна, страх втратити майно, яким винна особа тривалий час користувалася за життя спадкодавця, але на яке не має законних прав після його смерті (наприклад, проживання у квартирі померлого). Яскравим прикладом реалізації такого корисливого мотиву є ухвала Гайсинського районного суду Вінницької області у справі № 144/321/22 від 24 лютого 2023 року, у якій обвинувачена ОСОБА_4, керуючись прагненням до особистого незаконного збагачення, вступила у злочинну змову з третіми особами, щоб заволодіти спадковим майном померлої громадянки ОСОБА_7, на яке насправді мала право ОСОБА_6. Суть корисливого мотиву полягала у намаганні безкоштовно та протиправно отримати у власність земельну ділянку з кадастровим номером: 0523785000:02:002:0467, площею 2,1892 га та вартістю близько 96 329 гри. 63 коп. Для реалізації цього наміру обвинувачена використала завідомо підроблене свідоцтво про право на спадщину за заповітом, оформлене на її ім'я. На підставі свідоцтва, діючи через представника, ОСОБА_4 обманом змусила державного реєстратора внести запис про її право власності до Державного реєстру речових прав. Хоча суд закрив справу через закінчення строків давності (з моменту шахрайства минуло понад 5 років), матеріали провадження чітко зафіксували умисел на незаконне привласнення чужих спадкових прав шляхом обману [5];

– мотиви особистої неприязні, помсти чи тривалих сімейних конфліктів. У таких випадках протиправні дії спрямовані не стільки на власну вигоду, скільки на заподіяння максимальної матеріальної та моральної шкоди іншим членам родини, які сприймаються правопорушником як «суперники» чи «кривдники»;

– мотив так званої «викривленої (суб'єктивної) справедливості». Він притаманний особам, які здійснювали безпосередній догляд за спадкодавцем за його життя або вкладали власні кошти в утримання майна. Не маючи законних підстав на одноосібне спадкування, такі суб'єкти вважають за «справедливе»

заволодіти майном в обхід правових процедур, використовуючи, наприклад, фіктивні правочини або підроблені заповіти. Водночас аналіз судової практики свідчить про необхідність чіткого розмежування злочинних корисливих посягань та законних майнових інтересів добросовісних набувачів. Прикладом правомірної реалізації майнового інтересу є справа Колегії суддів судової палати у цивільних справах Апеляційного суду Сумської області №579/216/15–ц від 28 травня 2015 року, де мотивом ОСОБА_4 було отримання у власність квартири після смерті відчужувача (ОСОБА_7) натомість за надання довічного догляду та утримання відповідно до спадкового договору від 27 грудня 2011 року. Оскільки договір не був розірваний за життя відчужувача, ОСОБА_4 після смерті ОСОБА_7 вважала себе законним власником майна. Суд підтвердив її право власності (рішенням від 28 серпня 2014 року), оскільки ОСОБА_4 довела, що надавала допомогу, поки її не перестали допускати до літньої жінки [4].

Удосконалення механізмів запобігання та протидії злочинним посяганням на спадкове майно має відбуватися через оптимізацію та цифровізацію міжвідомчої взаємодії, інтеграцію реєстрів у реальному часі, удосконалення нормативно–правового регулювання та контролю за документами, цифровий аналіз спадщини без власника.

Отже, мотиви вчинення кримінальних правопорушеннях проти спадкового майна мають складну, переважно корисливу природу, що часто обтяжена сімейними конфліктами. Встановлення реального мотиву злочинного посягання є підґрунтям для побудови ефективної тактики допиту, висунення слідчих версій та виявлення можливих співучасників кримінального правопорушення.

Перелік використаних джерел:

1. Бандурка О.М. Литвинов О.М. Механізм злочинної поведінки. *Вісник кримінологічної асоціації України.* 2016. № 3 (14). С. 110–119

2. Комаринська Ю.Б. Мотиви вчинення кримінальних правопорушень, пов’язаних із домашнім насильством. *Юридична психологія.* 2022. № 1 (30). С. 94–102

3. Шульженко А.В. Мотив у складі кримінально–правової характеристики суб’єктивої сторони злочину. *Харківський національний університет внутрішніх справ:* 25 років досвіду та погляду майбутнє (1994–2019рр.). 2019. С. 528–531

4. Ухвала Колегії суддів судової палати у цивільних справах Апеляційного суду Сумської області. Справа №579/216/15–ц. Провадження 22–ц/788/1051/15. URL: https://reyestr.court.gov.ua/Review/44591208

5. Ухвала Гайсинського районного суду Вінницької області. Справа № 144/321/22. Провадження № 1–кп/129/260/2023. URL: https://reyestr.court.gov.ua/Review/109171169

DOI https://doi.org/10.32837/11300.33552

Клименко Дар'я
студентка 2 курсу Криворізького навчально–наукового інституту Національного університету «Одеська юридична академія», Кривий Ріг, Україна
y–mail: dasaklimenko118@gmail.com

Козаченко Віталій
кандидат юридичних наук, старший викладач кафедри кримінально–правових дисциплін Криворізького навчально наукового інститут Національного університету «Одеська юридична академія», м. Кривий Ріг, Україна
ORCID: https://orcid.org/0009–0003–9802–2020
y–mail:vitalii.kozachenko92@gmail.com

ЦИФРОВІ ФОРМИ НАСИЛЬСТВА ЩОДО ОСІБ ПОХИЛОГО ВІКУ: КРИМІНОЛОГІЧНІ АСПЕКТИ

У тезах досліджуються кримінологічні аспекти цифрових форм насильства щодо осіб похилого віку. Проаналізовано основні способи незаконного впливу через цифрові технології, зокрема телефонне шахрайство, фішинг, психологічний тиск та маніпуляції в онлайн–середовищі. Визначено фактори віктимізації осіб похилого віку в умовах цифровізації суспільства та окреслено основні напрями запобігання таким правопорушенням.

Ключові слова: цифрове насильство, особи похилого віку, кіберпростір, кримінологія, шахрайство, фішинг, віктимізація, цифрова безпека.

Klymenko Daria
2nd year student
Kryvyi Rih Educational and Scientific Institute of the National University «Odesa Law Academy», Kryvyi Rih, Ukraine

Kozachenko Vitalii
PhD in Law, Senior Lecturer of the Department of Criminal Law Disciplines, Kryvyi Rih Educational and Scientific Institute of the National University «Odesa Law Academy», Kryvyi Rih, Ukraine

DIGITAL FORMS OF VIOLENCE AGAINST ELDERLY PEOPLE: CRIMINOLOGICAL ASPECTS

The paper examines criminological aspects of digital forms of violence against elderly people. The main methods of unlawful influence through digital technologies are analysed, including telephone fraud, phishing, psychological pressure, and manipulation in the online environment. The factors of victimisation of elderly people in the context of digitalisation of society are identified, and the main directions for preventing such offenses are outlined.

Keywords: digital violence, elderly people, cyberspace, criminology, fraud, phishing, victimisation, digital security.

Насильство щодо осіб похилого віку в сучасних умовах набуває нових форм і виходить за межі традиційного фізичного чи психологічного впливу. Активне впровадження цифрових технологій у повсякденне життя сприяло появі нових способів незаконного впливу на людей похилого віку через засоби електронної комунікації, мобільний зв'язок, онлайн–сервіси, банківські системи та соціальні мережі. Це створює додаткові ризики для осіб цієї вікової категорії, які нерідко мають недостатній рівень цифрової підготовки та обмежені навички безпечного користування сучасними технологіями.

Особливо поширеними стали випадки дистанційного впливу, коли правопорушники використовують телефонні дзвінки, електронні повідомлення, фішингові ресурси, шахрайські схеми в месенджерах або представляються працівниками державних установ чи соціальних служб. Такі дії найчастіше спрямовані на отримання доступу до коштів, персональних даних або майна потерпілих. Через використання цифрових інструментів особа правопорушника може залишатися прихованою, що значно ускладнює виявлення та документування злочинної діяльності.

Вразливість осіб похилого віку до подібних форм насильства обумовлюється не лише віковими особливостями, а й соціальними чинниками: самотністю, довірливістю, залежністю від сторонньої допомоги та недостатньою поінформованістю про сучасні способи шахрайства. У результаті вони стають однією з найбільш незахищених категорій населення в умовах цифрового середовища.

Кримінологічний аналіз цифрових проявів насильства дозволяє визначити механізми формування віктимної поведінки, виявити найбільш поширені способи посягань і дослідити характерні риси осіб, які вчиняють такі правопорушення. Водночас важливе значення мають криміналістичні методи роботи з цифровими доказами, оскільки відомості про подію можуть міститися у телефонних з'єднаннях, банківських операціях, електронному листуванні, акаунтах та інших електронних джерелах.

У цифровому просторі неможливо захистити себе повністю, але цілком реально убезпечитись від ризиків та загроз. Щоб протидіяти кібернасильству

користувачам необхідно вдосконалювати знання, адаптуватися до нових технологій та знати як його ідентифікувати та діяти у таких випадках.

Способи роспізнання цифрового насильство та чому воно шкідливе, освітленно в межах кампанії «Кібернасильство: знаємо та протидіємо», що реалізується в межах Міжнародної акції «16 днів проти насилля». Її мета – допомогти користувачам соціальних мереж, вебсайтів, месенджерів та інших вебресурсів ідентифіковувати, знати та протидіяти ознакам насильства в цифровому середовищі [1].

З віком людям складніше сприймати нове, змінювати звичний спосіб життя та встановлювати нові соціальні зв'язки. Обмежена мобільність і залежність від оточення також підвищують ризик як психологічних проблем, так і потрапляння у небезпечні ситуації, особливо в умовах бідності чи нестабільного середовища.

Для слідчого робота з такими потерпілими має свої труднощі, пов'язані з їхнім психологічним станом і віковими особливостями. Іноді це може ускладнювати отримання інформації. Тому врахування особистісних характеристик потерпілих є важливим для встановлення обставин злочину, правильної кваліфікації дій винних і ефективного збирання доказів. Водночас у національній практиці ще недостатньо уваги приділяється саме особливостям комунікації з цією категорією осіб, що потребує подальшого вдосконалення [2, с. 62–63].

Зокрема, можна виділити такі види насилля по відношенню до людей похилого віку:

– фізичне насилля – рукоприкладство; побиття; погроза фізичним насиллям; обмеження рухів; свободи; усвідомлене тілесне пошкодження, що призводять до смерті; вбивство;

– психологічне насилля – словесні образи; обзивання; виклик страху можливим поганим поводженням чи відправкою в будинок пристарілих; погрози; ізоляція; вимогливість; поведінка або відношення, які викликають у похилої людини відчуття безнадійності та відчаю; безжалісність; безсердечність;

– економічне насилля – фінансова експлуатація; відмова у наданні пенсії, заробітку; викрадення грошів; використання сили та юридичних заходів для нанесення збитку похилим людям;

– соціальне насилля – негативна реакція та поведінка по відношенню до людей похилого віку; не прийняття їх як повноправних членів суспільства; зневажливе ставлення молодого покоління.

– окремою формою є сексуальне насильство, під яким розуміються будь–які дії сексуального характеру без добровільної згоди особи похилого віку [3].

Цифрове насильство щодо осіб похилого віку сьогодні стає все більш помітною проблемою, оскільки багато людей старшого віку почали користуватися телефонами, онлайн–банкінгом, месенджерами та різними електронними сервісами, але не завжди можуть повністю оцінити можливі ризики. Саме тому

вони нерідко стають об'єктами обману та психологічного впливу через цифрові засоби зв'язку.

Досить поширеним явищем є телефонне шахрайство. Людині можуть телефонувати нібито працівники банку, соціальної служби або інших установ і переконувати терміново виконати певні дії: повідомити код, переказати гроші чи надати особисті дані. У таких ситуаціях розрахунок часто робиться не на технічну необізнаність, а на довірливість і хвилювання людини.

Ще одним поширеним способом є фішинг і різні банківські схеми. Через повідомлення або посилання літніх людей можуть перенаправляти на підроблені сторінки, які зовні майже не відрізняються від справжніх. У результаті людина сама вводить свої дані, не підозрюючи, що передає їх стороннім особам.

Окремо варто звернути увагу на випадки, коли діють так звані псевдосоціальні служби. Шахраї представляються працівниками соціального захисту, пропонують оформити виплати чи допомогу та під цим приводом збирають особисту інформацію або отримують доступ до коштів.

Особливість цифрового насильства полягає ще й у тому, що воно часто здійснюється через психологічний вплив у цифровому середовищі. Людину можуть переконувати, залякувати, змушувати швидко приймати рішення або створювати відчуття, що від її дій залежить безпека чи фінансовий стан.

Крім цього, у таких випадках непросто зібрати та зберегти цифрові докази. Повідомлення видаляються, номери змінюються, а встановити особу правопорушника буває складно. Через це виявлення таких випадків і притягнення винних до відповідальності часто потребує більше часу та ресурсів.

Насильство щодо осіб похилого віку є складною соціально–правовою проблемою, яка потребує особливої уваги з боку держави та суспільства. Люди похилого віку належать до вразливої категорії населення через вікові особливості, можливу залежність від сторонньої допомоги, обмежені матеріальні ресурси та складність самостійного захисту своїх прав. Саме тому вони нерідко стають жертвами різних форм насильства – фізичного, психологічного, економічного, соціального або зневаги та неналежного догляду.

Кримінологічний аналіз цього явища дозволяє встановити основні причини та умови його виникнення, визначити характерні ознаки правопорушників і особливості потерпілих. Важливе значення має не лише реагування на вже вчинені випадки насильства, а й розвиток профілактичних заходів, підвищення рівня правової обізнаності населення, підтримка сімей та вдосконалення діяльності соціальних і правоохоронних інституцій. Ефективне запобігання насильству щодо осіб похилого віку можливе лише за умови комплексного підходу, спрямованого на забезпечення поваги до їхньої гідності, прав і безпеки.

Цифрове насильство щодо осіб похилого віку потребує комплексного підходу до протидії, який має поєднувати правові механізми захисту, підвищення цифрової грамотності та розвиток профілактичних заходів.

Перелік використаних джерел:

1. Цифрове насильство – серйозна загроза для психічного і фізичного здоров'я людини. 2024. URL: https://mvs.gov.ua/news/cifrove–nasilstvo–seriozna–zagroza–dlia–psixicnogo–i–fizicnogo–zdorovia–liudini

2.Павлюк О. Психолого–криміналістична характеристика осіб похилого віку й одиноких осіб, які є потерпілими від насильницьких злочинів. Юридична психологія. 2023. № 1 (32). С. 60–67. doi: 10.33270/03233201.60.

3. Все, чим ми володіємо і що маємо, належить тим, хто нас народив і вигодував. 2021. URL: https://vradiivska–gromada.gov.ua/news/1620729761/

DOI https://doi.org/10.32837/11300.33548

Козаченко Віталій
кандидат юридичних наук, старший викладач
кафедри кримінально–правових дисциплін Криворізького навчально
наукового інститут Національного університету «Одеська юридична академія»,
м. Кривий Ріг, Україна
ORCID: https://orcid.org/0009–0003–9802–2020
e–mail:vitalii.kozachenko92@gmail.com

ПРОБЛЕМА ВЕРБАЛЬНОЇ АГРЕСІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ: КРИМІНОЛОГІЧНИЙ АНАЛІЗ

У тезах досліджено феномен вербальної агресії у соціальних мережах як сучасну кримінологічну проблему. Проаналізовано основні форми цифрової агресії, зокрема «мова ненависті», онлайн–погрози, кібербулінг та токсичну комунікацію. Визначено криміногенні фактори поширення агресивної поведінки в умовах цифрової анонімності та алгоритмізації соціальних мереж. Окрему увагу приділено проблемам профілактики та протидії цифровій агресії.

Ключові слова: вербальна агресія, соціальні мережі, кібербулінг, hate speech, цифрова токсичність, кримінологія, кіберпростір.

Vitalii Kozachenko
PhD in Law, Senior Lecturer
of the Department of Criminal Law Disciplines,
Kryvyi Rih Educational and Scientific Institute of the
National University «Odesa Law Academy»,
Kryvyi Rih, Ukraine

VERBAL AGGRESSION IN SOCIAL MEDIA AS A CRIMINOLOGICAL PROBLEM

The abstract examines verbal aggression in social media as a contemporary criminological problem. The main forms of digital aggression are analyzed, including hate speech, online threats, cyberbullying, and toxic communication. The criminogenic factors contributing to aggressive behavior in conditions of digital anonymity and algorithm–driven social media are identified. Particular attention is paid to issues of prevention and counteraction to digital aggression.

Keywords: verbal aggression, social media, cyberbullying, hate speech, digital toxicity, criminology, cyberspace.

Розвиток цифрових технологій і популярність соціальних мереж суттєво змінили характер сучасної комунікації. Поряд із позитивними можливостями для спілкування, обміну інформацією та самовираження онлайн–простір дедалі

частіше стає середовищем прояву агресії. У соціальних мережах поширюються образи, мова ненависті (hate speech), онлайн–погрози, кібербулінг та інші форми деструктивної поведінки. Анонімність користувачів, швидкість поширення інформації та недостатній рівень контролю за контентом сприяють поширенню таких явищ. У кримінологічному аспекті це створює нові виклики для забезпечення безпеки особи та нормального функціонування інформаційного середовища.

За визначенням UNICEF, кібербулінг є однією з форм агресивної поведінки, що реалізується із використанням цифрових технологій та засобів онлайн–комунікації [1]. Такі дії можуть здійснюватися через соціальні мережі, месенджери, форуми, ігрові платформи, мобільний зв'язок та інші цифрові сервіси. Найчастіше кібербулінг проявляється у формі образливих повідомлень, систематичних принижень, поширення неправдивої або компрометуючої інформації, публічних насмішок, погроз чи переслідування в мережі.

Основною метою подібної поведінки є психологічний тиск на потерпілого, його залякування, приниження або соціальна ізоляція. Особливу небезпеку кібербулінгу становить те, що агресивний вплив може тривати безперервно, незалежно від місця перебування особи, а негативний контент здатний швидко поширюватися серед великої кількості користувачів. Крім того, анонімність онлайн–середовища нерідко створює у правопорушників відчуття безкарності, що сприяє повторюваності та ескалації агресивної поведінки [1].

Одним із найбільш небезпечних проявів вербальної агресії у цифровому просторі сьогодні є hate speech – мова ненависті. У Рекомендації Комітету міністрів Ради Європи CM/Rec(2022)16 під «мовою ненависті» розуміються будь–які форми висловлювань, які поширюють, підбурюють, підтримують або виправдовують ненависть, дискримінацію чи ворожнечу щодо окремої особи або групи осіб [2]. Як правило, об'єктами такої агресії стають люди за ознаками раси, національності, етнічного походження, релігії, статі, політичних переконань або інших соціально значущих характеристик.

Особливу небезпеку мова ненависті становить саме в умовах цифрового середовища. Соціальні мережі та інші онлайн–платформи забезпечують надзвичайно швидке поширення інформації, унаслідок чого агресивний контент може за короткий час охоплювати значну аудиторію. Додатковою проблемою є те, що алгоритми окремих платформ нерідко просувають емоційно конфліктний контент через його високу активність серед користувачів. У результаті мова ненависті набуває масового характеру та здатна формувати атмосферу нетерпимості, соціальної напруги й ворожнечі у суспільстві.

Крім того, систематичне поширення «мови ненависті» у мережі сприяє поступовій нормалізації агресивної комунікації. Користувачі починають сприймати образи, приниження та публічне цькування як звичний елемент

онлайн–спілкування, що підвищує загальний рівень цифрової токсичності та створює додаткові криміногенні ризики [2].

У кримінологічному аспекті вербальна агресія у соціальних мережах має низку специфічних ознак. По–перше, цифрова анонімність істотно знижує рівень соціального контролю та відповідальності за агресивну поведінку. По–друге, алгоритми соціальних мереж часто стимулюють поширення емоційно конфліктного контенту через його вищу залученість користувачів. По–третє, агресивна комунікація в інтернеті характеризується високим рівнем латентності та складністю ідентифікації правопорушників.

UNESCO розглядає поширення «мови ненависті» в онлайн–просторі як одну з актуальних глобальних проблем сучасного цифрового суспільства [3]. У доповідях організації наголошується, що мова ненависті в мережі негативно впливає не лише на окремих користувачів, а й на демократичні процеси, суспільну стабільність та загальний рівень безпеки інформаційного середовища. Систематичне поширення агресивного контенту здатне посилювати соціальну поляризацію, провокувати конфлікти та формувати атмосферу нетерпимості у суспільстві.

Окрему увагу UNESCO звертає на те, що сучасні цифрові платформи значно спрощують створення та поширення агресивного контенту [3]. Це пояснюється насамперед високою швидкістю онлайн–комунікації, можливістю миттєвого доступу до великої аудиторії та мінімальними витратами на розповсюдження інформації. Будь–яке повідомлення, коментар або публікація можуть бути поширені серед тисяч користувачів протягом короткого часу, особливо якщо контент викликає емоційну реакцію.

Водночас ефективність механізмів модерації на багатьох онлайн–платформах залишається недостатньою. Автоматизовані системи не завжди здатні своєчасно виявляти агресивні висловлювання, а значний обсяг контенту ускладнює оперативне реагування з боку адміністрації соціальних мереж. У результаті hate speech нерідко тривалий час залишається доступним для широкої аудиторії, що сприяє його подальшому поширенню та нормалізації в цифровому середовищі. Крім того, постійний контакт користувачів із агресивним контентом може негативно впливати на їхній психоемоційний стан, підвищувати рівень тривожності та сприяти формуванню атмосфери ворожості в онлайн–комунікації [3].

Дослідження Джузеппе Фулантеллі та інших науковців підтверджують наявність тісного взаємозв’язку між кібербулінгом і hate speech у соціальних мережах [4]. Автори звертають увагу на те, що обидва явища фактично виступають взаємопов’язаними формами цифрової агресії, які поширюються в умовах онлайн–комунікації та мають схожі механізми впливу на потерпілих.

На думку дослідників, систематичне поширення образливих повідомлень, принижень, публічного цькування та агресивних висловлювань у мережі сприяє психологічній віктимізації користувачів, підвищує рівень емоційного напруження

та формує сприятливе середовище для подальшого поширення онлайн–насильства [4]. Особливо небезпечним є те, що в цифровому просторі такі прояви агресії можуть набувати масового характеру та тривалий час залишатися доступними для широкої аудиторії.

Окрему кримінологічну проблему становить так звана «цифрова токсичність». Йдеться про систематичне використання образ, принижень, погроз, мови ненависті та агресивних коментарів у мережевій комунікації. Подібна поведінка поступово нормалізується в окремих онлайн–спільнотах, що створює сприятливі умови для девіантної поведінки.

Дослідники Мааруф, Прьоллокс та Фойєррігель встановили, що «мова ненависті» у соціальних мережах має високий рівень вірусного поширення [5]. Особливо швидко агресивний контент поширюється через акаунти з високим рівнем аудиторії або суспільного впливу. Це суттєво посилює криміногенний потенціал цифрової агресії.

Суттєвим фактором поширення вербальної агресії є алгоритмізація соціальних мереж. Рекомендації та механізми автоматичного просування контенту орієнтовані насамперед на залучення користувача, а конфліктний та емоційно агресивний контент зазвичай генерує більшу кількість реакцій. Унаслідок цього соціальні мережі фактично можуть виступати каталізатором цифрової агресії.

Кримінологічне значення має також зв’язок між онлайн–агресією та реальною офлайн–віктимізацією. Дослідження у сфері цифрової безпеки свідчать, що систематичне онлайн–переслідування нерідко супроводжується психологічним тиском та загрозами у реальному житті [6].

Особливу вразливість до цифрової агресії демонструють неповнолітні, жінки, представники меншин, журналісти, громадські активісти та публічні особи. В окремих випадках систематичне онлайн–переслідування може призводити до депресивних розладів, тривожності, соціальної ізоляції та суїцидальної поведінки [1].

Важливою проблемою залишається недостатня ефективність механізмів протидії «мови ненависті» у соціальних мережах. Європейський Союз та Рада Європи наголошують на необхідності комплексного підходу, який має включати правові механізми, цифрову освіту, удосконалення систем модерації контенту та міжнародну співпрацю у сфері протидії онлайн–ненависті [2; 7].

Таким чином, вербальна агресія у соціальних мережах є комплексною кримінологічною проблемою сучасного цифрового суспільства. Її суспільна небезпечність полягає не лише у психологічній віктимізації окремих осіб, але й у формуванні атмосфери соціальної ворожнечі, девіантної нормалізації агресії та підвищенні рівня конфліктності в суспільстві. Ефективна протидія цифровій агресії потребує поєднання кримінологічних, правових, технологічних та превентивних механізмів.

Перелік використаних джерел:

1. Cyberbullying: What is it and how to stop it. UNICEF. URL: https://www.unicef.org/stories/how–to–stop–cyberbullying

2. Recommendation CM/Rec(2022)16 on Combating Hate Speech. Council of Europe. URL: https://www.coe.int/en/web/combating–hate–speech/recommendation–on–combating–hate–speech

3. Countering online hate speech. UNESCO. URL: https://www.unesco.org/en/articles/countering–online–hate–speech

4. Fulantelli G. et al. Cyberbullying and Cyberhate as Two Interlinked Instances of Cyber–Aggression in Adolescence. Future Internet. 2022. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9196243/

5. Maarouf A., Pröllochs N., Feuerriegel S. The Virality of Hate Speech on Social Media. 2022. URL: https://arxiv.org/abs/2210.13770

6. Chatzakou D. et al. Detecting Cyberbullying and Cyberaggression in Social Media. 2019. URL: https://arxiv.org/abs/1907.08873

7. EU Code of conduct on countering illegal hate speech online. European Commission. URL: https://commission.europa.eu/strategy–and–policy/policies/justice–and–fundamental–rights/combatting–discrimination/racism–and–xenophobia/eu–code–conduct–countering–illegal–hate–speech–online_en

DOI https://doi.org/10.32837/11300.33627

Кубаєнко Андрій
кандидат юридичних наук, доцент,
доцент кафедри оперативно–розшукової та поліцейської діяльності
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–6648–9764
e–mail: kav1312@ukr.net

ЕФЕКТИВНІСТЬ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНИХ ЗАГРОЗ

Досліджено ефективність поліцейської діяльності в умовах цифровізації кримінальних загроз. Обґрунтовано необхідність оновлення правових, організаційних, технологічних і кадрових засад діяльності поліції, розвитку цифрової криміналістики, предиктивної аналітики та міжвідомчої взаємодії для підвищення спроможності правоохоронної системи протидіяти кіберзлочинності.

Ключові слова: поліцейська діяльність, ефективність поліцейської діяльності, цифровізація, кіберзлочинність, цифрові загрози, кіберполіція, цифрова криміналістика, цифрові докази, інформаційна безпека, штучний інтелект.

Kubaienko Andrii
PhD in Law, Associate Professor,
Associate Professor of the Department of Operational–Search and Policing Activity,
National University «Odesa Law Academy»,
Odesa, Ukraine

EFFICIENCY OF POLICE ACTIVITY IN THE CONDITIONS OF DIGITALIZATION OF CRIMINAL THREATS

The study examines the effectiveness of police activity in the context of the digitalization of criminal threats. The necessity of updating the legal, organizational, technological, and personnel foundations of police activity, developing digital forensics, predictive analytics, and interagency cooperation to enhance the capacity of the law enforcement system to combat cybercrime is substantiated.

Keywords: police activity, effectiveness of police activity, digitalization, cybercrime, digital threats, cyber police, digital forensics, digital evidence, information security, artificial intelligence.

Проблематика ефективності поліцейської діяльності в умовах цифровізації кримінальних загроз набуває особливого теоретико–методологічного та

прикладного значення у зв'язку з якісною трансформацією сучасної злочинності, яка дедалі частіше набуває технологічно опосередкованого, транскордонного та латентного характеру. У 2025 році підрозділами Національної поліції України було зареєстровано 26,9 тис. кіберзлочинів, повідомлено про підозру 3,5 тис. особам у вчиненні 9 тис. кримінальних правопорушень, а до суду з обвинувальним актом скеровано майже 9,1 тис. кримінальних правопорушень. При цьому потерпілим забезпечено відшкодування з урахуванням арештованого та вилученого майна понад 784,8 млн грн, що становить 102,39 % від завданих збитків [1]. Наведені показники свідчать, що цифровізація злочинності вже не є периферійним викликом для правоохоронної системи, а перетворюється на один із ключових критеріїв оцінки її інституційної спроможності.

Водночас цифрове середовище істотно ускладнює традиційні підходи до оцінювання ефективності поліції, оскільки результативність її діяльності не може зводитися виключно до кількісних показників зареєстрованих проваджень, повідомлень про підозру чи направлених до суду обвинувальних актів. У щорічному звіті Департаменту кіберполіції Національної поліції України за 2025 рік наголошено, що воєнний стан, зростання попиту на гуманітарні, соціальні та військові товари, а також активний розвиток віртуальних активів створили сприятливе середовище для поширення кіберзлочинності, фінансового шахрайства, легалізації незаконних доходів і транснаціональних цифрових схем [2]. За таких умов ефективність поліцейської діяльності повинна визначатися не лише через репресивно–статистичні індикатори, а й через рівень спроможності поліції забезпечувати цифрову аналітику, міжвідомчу координацію, міжнародну взаємодію та оперативну адаптацію до новітніх технологій злочинної діяльності.

Глобальний безпековий контекст підтверджує, що цифровізація кримінальних загроз є стійкою світовою тенденцією. Європейське агентство з мережевої та інформаційної безпеки (ENISA) у звіті Threat Landscape 2025 проаналізувало 4875 кіберінцидентів за період з 1 липня 2024 року до 30 червня 2025 року, констатувавши домінування атак на доступність цифрових сервісів, ransomware–атак, використання легітимних хмарних платформ для приховування злочинної діяльності та посилення геополітичного чинника у структурі кібероперацій [3]. У зв'язку з цим ефективність поліцейської діяльності набуває комплексного змісту та охоплює не лише здатність держави реагувати на вже вчинені кримінальні правопорушення, а й спроможність правоохоронної системи прогнозувати цифрові ризики, мінімізувати їхній вплив на публічну безпеку та забезпечувати належний рівень захисту прав людини в умовах технологічно ускладненого криміногенного середовища.

У науковій літературі означена проблематика досліджується з кількох взаємопов'язаних позицій. А. В. Бенескул, аналізуючи нормативно–правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки, констатує відсутність достатніх правових основ, пов'язаних з розумінням цифрової злочинності, а також наголошує на тому, що правопорушення, які

вчиняються з використанням цифрових технологій, практично приховані від зовнішнього спостереження, відбуваються дистанційно та дозволяють злочинцям діяти з–за меж юрисдикції держави, що суттєво ускладнює їх виявлення та притягнення винних до відповідальності [4].

І. В. Гора, В. А. Колесник та І. І. Попович обґрунтовують необхідність інституційного розвитку цифрової криміналістики як нового напряму криміналістичних знань, що має стати інструментальною основою ефективного виявлення та документування кіберзлочинів, підкреслюючи, що цифровізація злочинності вимагає відповідного технологічного і методологічного переоснащення правоохоронних органів [5].

О. П. Метелєв та Є. В. Коваленко акцентують увагу на недостатній гармонізації кримінального процесуального законодавства із законодавством, що регулює контррозвідувальну й оперативно–розшукову діяльність, що негативно позначається на допустимості цифрових доказів у кримінальному провадженні та знижує ефективність виконання оперативними підрозділами своїх завдань [6].

Наведені теоретичні підходи та статистичні показники дають підстави визначити основні напрями вдосконалення поліцейської діяльності в умовах цифровізації кримінальних загроз.

Підвищення її ефективності має здійснюватися комплексно та охоплювати правовий, організаційний, технологічний і кадровий виміри. Першочергового значення набуває оновлення законодавчого регулювання у сфері протидії цифровій злочинності, зокрема щодо цифрових доказів, інформаційно–аналітичних систем, застосування штучного інтелекту в правоохоронній діяльності та правового режиму віртуальних активів. Наявна фрагментарність правового регулювання ускладнює формування сталої правозастосовної практики й може спричиняти процесуальні колізії під час виявлення, документування та розслідування кримінальних правопорушень. Тому доцільним є розроблення цілісної концепції нормативного забезпечення цифрової безпеки в діяльності Національної поліції України з урахуванням європейських стандартів і положень Будапештської конвенції про кіберзлочинність.

Водночас результативність поліції у цифровому середовищі безпосередньо залежить від рівня її технологічної спроможності. Ідеться про необхідність упровадження автоматизованих систем кримінального аналізу, технологій великих даних, інтелектуальних аналітичних платформ, засобів моніторингу цифрових комунікацій та алгоритмів прогнозування криміногенних ризиків. Використання таких інструментів дає змогу поступово перейти від переважно реактивної моделі реагування на вже вчинені правопорушення до проактивної моделі запобігання цифровим загрозам, орієнтованої на їх раннє виявлення, попередження та нейтралізацію.

Окремого значення набуває розвиток цифрової криміналістики та спеціалізованої підготовки працівників поліції. У сучасних умовах якість

розслідування значною мірою визначається здатністю правоохоронців працювати з цифровими слідами, електронними носіями інформації, хмарними сервісами, віртуальними активами та іншими об'єктами цифрового середовища. Це потребує створення спеціалізованих лабораторій цифрових досліджень, упровадження міжнародних стандартів поводження з цифровими доказами, а також формування системи безперервного підвищення кваліфікації працівників Національної поліції України.

Отже, ефективність поліцейської діяльності в умовах цифровізації кримінальних загроз має оцінюватися не лише за традиційними статистичними показниками розкриття кримінальних правопорушень, а й за рівнем цифрової стійкості суспільства, якістю аналітичного прогнозування, спроможністю захищати інформаційну інфраструктуру, ефективністю міжвідомчої та міжнародної взаємодії, а також рівнем суспільної довіри до правоохоронної системи. Саме поєднання правових, технологічних, організаційних і кадрових механізмів здатне забезпечити формування сучасної моделі поліцейської діяльності, адекватної викликам цифрового криміногенного середовища.

Перелік використаних джерел:

1.Звіт про результати роботи підрозділів кіберполіції Національної поліції України за 2025 рік. Національна поліція України URL: https://npu.gov.ua/static–objects/npu/sites/1/zvit–npu–po–kb–2025.pdf

2.Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік. Департамент кіберполіції Національної поліції України URL: https://cyberpolice.gov.ua/news/shhorichnyj–zvit–7096/

3.ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (ENISA) URL: https://www.enisa.europa.eu/topics/cyber–threats/threat–landscape

4.Бенескул А. В. Нормативно–правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Т. 2, № 78. С.145–153.

5.Гора І. В., Колесник В. А., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Т. 4, № 85. С. 63–70.

6.Метелєв О. П., Коваленко Є. В. До питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно–розшукової діяльності. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Т. 2, № 80. С.177–182.

DOI https://doi.org/10.32837/11300.33624

Лукащук Каріна
доктор філософії в галузі права, начальник юридичного відділу,
доцент кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–9862–2884
e–mail: lukashchuk611@gmail.com

ЦИФРОВІЗАЦІЯ ВИКОНАННЯ ПОКАРАНЬ, НЕ ПОВ'ЯЗАНИХ ІЗ ПОЗБАВЛЕННЯМ ВОЛІ: МІЖНАРОДНИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

У тезах досліджено міжнародний досвід цифровізації виконання покарань, не пов'язаних із позбавленням волі, зокрема використання електронного моніторингу, автоматизованих систем оцінки ризиків та елементів штучного інтелекту у діяльності органів пробації. Визначено основні проблеми та перспективи розвитку цифрової пробації в Україні.

Ключові слова: пробація, цифровізація, електронний моніторинг, штучний інтелект, кримінальне провадження, кримінальний процес, кримінально–виконавча система, ресоціалізація, кібербезпека.

Karina Lukashchuk
Doctor of Philosophy in Law,
Head of the Legal Department,
Associate Professor of the Department of Criminal Procedure,
National University «Odesa Law Academy»,
Odesa, Ukraine

DIGITALIZATION OF NON–CUSTODIAL SENTENCES: INTERNATIONAL EXPERIENCE AND PROSPECTS FOR UKRAINE

The theses examine the international experience of digitalization of non–custodial sentences, including the use of electronic monitoring, automated risk assessment systems, and artificial intelligence elements in probation activities. The main challenges and prospects for the development of digital probation in Ukraine are identified.

Key words: probation, digitalization, electronic monitoring, artificial intelligence, criminal proceedings, criminal trial, penal system, resocialization, cybersecurity.

Сучасний розвиток інформаційних технологій суттєво впливає на функціонування систем державного управління, включаючи сферу кримінальної

юстиції та виконання покарань. Одним із найбільш актуальних напрямів реформування кримінально–виконавчої системи є цифровізація механізмів виконання покарань, не пов'язаних із позбавленням волі. У багатьох країнах світу застосування цифрових технологій у діяльності органів пробації стало важливим інструментом забезпечення ефективного нагляду, ресоціалізації правопорушників та запобігання повторній злочинності.

Для України питання розвитку цифрових інструментів пробації набуває особливої актуальності в умовах реформування системи кримінальної юстиції, євроінтеграційних процесів та необхідності забезпечення ефективного використання державних ресурсів. Запровадження сучасних цифрових рішень дозволяє не лише оптимізувати діяльність органів пробації, але й забезпечити дотримання прав людини та міжнародних стандартів поводження із засудженими.

Цифровізація системи виконання покарань, не пов'язаних із позбавленням волі, сьогодні є одним із ключових напрямів модернізації кримінально–виконавчої політики багатьох держав. Її основою виступає інтеграція інформаційно–комунікаційних технологій у діяльність органів пробації, що дозволяє здійснювати ефективний контроль за поведінкою правопорушників без ізоляції їх від суспільства.

Одним із найбільш поширених інструментів цифровізації є електронний моніторинг засуджених. У країнах Європейського Союзу така практика використовується протягом тривалого часу та демонструє позитивні результати у сфері профілактики рецидивної злочинності. Досвід Естонії, Іспанії, Португалії та Франції свідчить про ефективність використання електронних браслетів та систем дистанційного контролю, які дозволяють забезпечити нагляд за особою без застосування ізоляції від суспільства [1].

Французька система пробації активно використовує електронний моніторинг щодо значної кількості засуджених. Під час співпраці з українськими органами пробації французькі фахівці наголошували на ефективності таких технологій у забезпеченні контролю та ресоціалізації осіб, які відбувають покарання без позбавлення волі [2].

У Великій Британії, Нідерландах та скандинавських країнах цифрові технології використовуються не лише для контролю, але й для комплексного управління пробаційними процесами. Сучасні інформаційні системи дозволяють вести електронні реєстри засуджених, автоматизувати оцінку ризиків повторного правопорушення, здійснювати дистанційну комунікацію між працівниками пробації та суб'єктами пробації, а також формувати індивідуальні програми ресоціалізації [3].

Особливу увагу привертає використання елементів штучного інтелекту у діяльності органів пробації. В Україні вже застосовується програмне забезпечення «Кассандра», яке дозволяє аналізувати ймовірність повторного вчинення правопорушень та оцінювати криміногенні ризики [4]. Такі системи сприяють підвищенню об'єктивності оцінювання поведінки правопорушників та

допомагають працівникам пробації приймати більш ефективні управлінські рішення.

Важливим елементом цифровізації є також розвиток дистанційних форм взаємодії із засудженими. Сучасні мобільні додатки, електронні кабінети та онлайн–платформи дозволяють забезпечувати постійний зв'язок між органами пробації та особами, які перебувають на обліку. Це особливо актуально в умовах воєнного стану, коли окремі території можуть бути тимчасово недоступними або існують труднощі із фізичним переміщенням громадян [5].

Разом із позитивними аспектами цифровізація системи пробації породжує низку проблем. Однією з основних є забезпечення інформаційної та кібербезпеки. У процесі функціонування електронних систем органи пробації здійснюють збір, обробку та зберігання значних обсягів персональних даних засуджених, що потребує належного рівня захисту інформації. Науковці наголошують на необхідності формування комплексної системи кібербезпеки у сфері пробації, яка має включати організаційні, технічні та кадрові заходи [5].

Окремою проблемою залишається недостатній рівень технічного забезпечення органів пробації України. Як свідчать результати попередніх етапів впровадження електронного моніторингу, значна частина технічних засобів виявилася непридатною до експлуатації через відсутність належного фінансування та технічної підтримки [6]. Це свідчить про необхідність комплексного підходу до цифрової трансформації кримінально–виконавчої системи.

Міжнародний досвід демонструє, що ефективна цифровізація пробації неможлива без належного нормативно–правового забезпечення та міжнародної співпраці. Україна активно взаємодіє з європейськими партнерами у межах міжнародних проєктів, спрямованих на розвиток пробації та альтернативних видів покарань. Важливу роль у цьому процесі відіграють програми Європейського Союзу, Нідерландів та інших держав, які сприяють впровадженню сучасних цифрових інструментів у діяльність українських органів пробації [7].

Перспективними напрямами розвитку цифровізації виконання покарань в Україні є створення єдиної цифрової платформи пробації, розширення застосування електронного моніторингу, інтеграція систем штучного інтелекту для оцінки ризиків, впровадження електронного документообігу, розвиток дистанційних сервісів для суб'єктів пробації, удосконалення системи кіберзахисту, підвищення рівня цифрової компетентності персоналу органів пробації.

Таким чином, цифровізація виконання покарань, не пов'язаних із позбавленням волі, є важливим напрямом модернізації сучасної кримінально–виконавчої системи. Міжнародний досвід свідчить, що використання електронного моніторингу, автоматизованих систем оцінки ризиків, дистанційних платформ взаємодії та елементів штучного інтелекту сприяє підвищенню

ефективності пробації, зменшенню рівня рецидивної злочинності та оптимізації бюджетних витрат.

Для України впровадження цифрових технологій у сфері пробації є необхідною умовою подальшого реформування системи кримінальної юстиції відповідно до європейських стандартів. Водночас успішна цифровізація потребує належного нормативно–правового забезпечення, достатнього фінансування, розвитку технічної інфраструктури та забезпечення високого рівня інформаційної безпеки.

Перелік використаних джерел:

1.Сіренко К. Ю. Зарубіжний досвід становлення та розвитку інституту пробації. Науковий вісник Сіверщини. Серія: Освіта. Соціальні та поведінкові науки. 2024. № 1 (12). С. 255–267.

2.Електронний моніторинг: досвід впровадження в системі кримінального правосуддя Франції. URL: https://putylska–gromada.gov.ua/news/1726130409/?utm_source=chatgpt.com

3.Пробація: 10 років змін та досягнень : колективна монографія/ В. О. Аніщенко, І. Г. Богатирьов, І. Б. Волеваха та ін. ; за заг. ред. д–ра юрид. наук, проф. С. К. Гречанюка. Чернігів : Пенітенціарна академія України, 2025. 272 с.

4.У роботі органу пробації – «Касандра» штучний інтелект. URL: https://ing–org.gov.ua/u–roboti–organu–probacii–kasandra–shtuchnij–intelekt.html?utm_source=chatgpt.com

5.Таволжанський О., Демидова Є. До питання інформаційної і кібербезпеки в діяльності органів пробації. Право та інновації. № 1 (53). 2026. С. 63–69.

6.Як працюватиме електронний моніторинг як елемент пробації. URL: https://sud.ua/ru/news/video/142327–yak–pratsyuvatime–elektronniy–monitoring–yak–element–probatsiyi–video?utm_source=chatgpt.com

7.»MATRA» (Нідерланди) проєкт завершено. URL: https://probation.gov.ua/matra–niderlandi?utm_source=chatgpt.com

DOI https://doi.org/10.32837/11300.33608

Луцюк Павло
кандидат юридичних наук,
прокурор Рівненської окружної прокуратури Рівненської області
м.Рівне, Україна
ORCID: https://orcid.org/0009–0002–4357–3194
e–mail:fres@ukr.net

ПРОБЛЕМИ ВИЗНАЧЕННЯ ВЧИНЕННЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ ВПЕРШЕ У КРИМІНАЛЬНОМУ ПРАВІ ТА СУДОВІЙ ПРАКТИЦІ

Проаналізовано основні аспекти визначення поняття вчинення кримінального правопорушення вперше. Наведено особливості застосування звільнення особи від кримінальної відповідальності у разі вчинення кримінального правопорушення вперше, зокрема співвідношення понять «вчинення кримінального правопорушення вперше» та «погашення і зняття судимості». Досліджено судову практику встановлення факту вчинення кримінального правопорушення вперше у випадку вчинення особою двох або більше кримінальних правопорушень (ідеальна сукупність).

Ключові слова: вчинення кримінального правопорушення вперше, погашення судимості, зняття судимості, ідеальна сукупність.

Lutsiuk Pavlo
Candidate of Juridical Sciences,
Prosecutor at the Rivne District Prosecutor's Office,
Rivne, Ukraine

PROBLEMS OF DEFINING THE FIRST–TIME COMMISSION OF A CRIMINAL OFFENSE IN CRIMINAL LAW AND JUDICIAL PRACTICE

The key aspects of defining the concept of first–time commission of a criminal offense are analyzed. The paper outlines the particularities of releasing an individual from criminal liability in cases of a first–time commission of a criminal offense, including the relationship between the notions of «first–time commission of a criminal offense» and «extinguishment and expungement of conviction.» Judicial practice is examined regarding the establishment of the fact of first–time commission of a criminal offense where a person has committed two or more criminal offenses (ideal concurrence).

Keywords: first–time commission of a criminal offense, extinguishment of conviction, expungement of conviction, ideal concurrence.

В українській мові слово «вперше» є прислівником, що має значення: один раз; у перший раз; спершу. [1]

У кримінальному та кримінальному процесуальному праві поняття «вперше» має інший зміст і означає відсутність у особи юридичного минулого щодо вчинення нею кримінальних правопорушень, тісно пов'язуючись з інститутами зняття та погашення судимості. Крім того, вчинення кримінального правопорушення вперше може безпосередньо впливати на його кваліфікацію, а також на наявність чи відсутність обставин, що обтяжують покарання (зокрема, повторність злочину та рецидив злочинів), і слугувати однією з обов'язкових підстав для звільнення особи від кримінальної відповідальності.

Слід виокремити загальні та спеціальні підстави звільнення особи від кримінальної відповідальності, яка вчинила кримінальне правопорушення вперше.

До загальних підстав звільнення особи від кримінальної відповідальності, яка вчинила кримінальне правопорушення вперше, слід віднести підстави, передбачені ст. 45 Кримінального кодексу України (надалі – КК України) – звільнення від кримінальної відповідальності у зв'язку з дійовим каяттям; ст. 46 КК України – звільнення від кримінальної відповідальності у зв'язку з примиренням винного з потерпілим; ст. 47 КК України – звільнення від кримінальної відповідальності у зв'язку з передачею особи на поруки; ст. 48 КК України – звільнення від кримінальної відповідальності у зв'язку із зміною обстановки); а також ст. 97 КК України – звільнення від кримінальної відповідальності із застосуванням примусових заходів виховного характеру. [2]

У разі застосування спеціальних підстав звільнення особи від кримінальної відповідальності, яка вчинила кримінальне правопорушення вперше, законодавець пов'язує таке звільнення з учиненням конкретного кримінального правопорушення.

До спеціальних підстав звільнення особи від кримінальної відповідальності, яка вперше вчинила кримінальне правопорушення, законодавець відносить випадки, передбачені частиною четвертою статті 289 КК України. Зокрема, суд може звільнити від кримінальної відповідальності особу, яка вперше вчинила дії, передбачені частиною першою цієї статті, якщо вона добровільно повідомила про це правоохоронні органи, повернула транспортний засіб власнику та повністю відшкодувала завдані збитки. Також звільнення можливе відповідно до частини п'ятої статті 401 КК України. Особа, яка під час дії воєнного стану вперше вчинила кримінальне правопорушення, передбачене статтями 407 або 408 цього Кодексу, може бути звільнена від кримінальної відповідальності за умови, що вона добровільно звернулася з клопотанням до слідчого, прокурора або суду щодо наміру повернутися до військової частини або місця служби для продовження проходження військової служби та має письмову згоду командира (начальника) військової частини (установи) на продовження служби. Звільнення здійснюється

відповідно до порядку, передбаченого кримінальним процесуальним законодавством України.

У юриспруденції поняття вчинення кримінального правопорушення вперше фактично пов'язується з трьома такими критеріями:

особа раніше взагалі не вчиняла злочинів чи кримінальних проступків;

вчинене особою раніше кримінальне правопорушення втратило юридичне значення (судимість знята або погашена);

особа, яка притягувалася до кримінальної відповідальності, була звільнена від кримінальної відповідальності (у зв'язку з дійовим каяттям, примиренням винного з потерпілим тощо).

Статтею 62 Конституції України визначено, що особа вважається невинуватою у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку та встановлено обвинувальним вироком суду.[3]

Відповідно до статті 88 КК України особа визнається такою, що має судимість, з дня набрання законної сили обвинувальним вироком суду і до погашення або зняття судимості. Особи, засуджені за вироком суду без призначення покарання або зі звільненням від покарання, а також такі, що відбули покарання за діяння, кримінальну протиправність і караність якого усунено законом, визнаються такими, що не мають судимості. До осіб, які не мають судимості, законодавець також відносить осіб, які були реабілітовані. Порядок і підстави зняття та погашення судимості визначено статтями 89–91 КК України.

Водночас на практиці часто постає питання співвідношення поняття вчинення кримінального правопорушення вперше з правовим статусом особи, у якої судимість знята чи погашена. Адже в такому випадку особа фактично раніше вчиняла кримінальне правопорушення, і з логічної точки зору не можна стверджувати, що вона вчинила його вперше. Водночас такий висновок суперечить вимогам статті 89 КК України, якою юридично встановлено, що особа, у якої судимість знята чи погашена, вважається такою, що не має судимості.

При вирішенні цього питання слід враховувати кримінально–правовий зміст поняття «вчинення злочину вперше». Це означає, що особа визнається такою, яка вчинила кримінальне правопорушення вперше, і у випадку, якщо кримінальне правопорушення фактично було вчинене нею не вперше, але на день його вчинення існували юридичні підстави, що виключали можливість визнання такого кримінального правопорушення повторним або рецидивом злочинів. Це має місце, зокрема, якщо за раніше вчинене кримінальне правопорушення:

а) особу було звільнено від кримінальної відповідальності на підставах, установлених КК України (у тому числі у зв'язку із закінченням строків давності), згідно із законом про амністію або на підставі акта про помилування;

б) особа хоча і була засуджена за раніше вчинене кримінальне правопорушення, однак на момент вчинення нового кримінального правопорушення судимість була знята або погашена;

в) особа не підлягає кримінальній відповідальності, оскільки кримінальну караність вчиненого діяння скасовано новим кримінальним законом (стаття 5 КК України). [4, с. 179]

У цій роботі не можна оминути питання співвідношення поняття вчинення кримінального правопорушення вперше з інститутом сукупності кримінальних правопорушень.

Досить часто виникає питання, як оцінювати діяння, коли особа одним діянням вчиняє два кримінальні правопорушення, і чи вважається це вчиненням кримінального правопорушення вперше.

Статтею 33 КК України визначено, що сукупністю кримінальних правопорушень визнається вчинення особою двох або більше кримінальних правопорушень, передбачених різними статтями або різними частинами однієї статті Особливої частини цього Кодексу, за жодне з яких її не було засуджено.

На законодавчому рівні види сукупності кримінальних правопорушень не визначено. Проте в юридичній літературі розрізняють два види сукупності кримінальних правопорушень: ідеальну та реальну.

Ідеальна сукупність виникає у випадку, коли особа одним діянням одночасно вчиняє два або більше кримінальних правопорушення. Наприклад, службова особа, яка одержала як хабар наркотичні засоби, однією дією вчиняє злочин, передбачений статтею 368 КК України, та злочин, передбачений статтею 308 КК України. Ознаками ідеальної сукупності є вчинення злочинів: а) одним діянням; б) в одному місці; в) одночасно; г) за наявності всіх необхідних ознак, передбачених двома чи більше різними статтями КК України.

Реальна сукупність має місце у випадку, коли особа в різний час кількома різними та відокремленими одне від одного діяннями вчинила два або більше кримінальних правопорушень. Кожне з кримінальних правопорушень, що утворюють сукупність, кваліфікується окремо за відповідною статтею або частиною статті КК України. [5, с. 112]

Так, Верховний Суд у справі № 761/1571/23 зазначив, що однією з умов, передбачених статтею 45 КК України, є вчинення особою кримінального правопорушення (кримінального проступку або необережного нетяжкого злочину) вперше. Тому особу, у діях якої вбачається повторність, сукупність (крім ідеальної) або рецидив, не можна звільнити від кримінальної відповідальності на підставі цієї статті.

Аналогічна правова позиція висловлена у справі № 157/1091/22, у якій Верховний Суд зазначив, що поза увагою судів попередніх інстанцій залишилося те, що у цьому провадженні особа обвинувачувалася у пособництві в підробленні документа, вчиненому за попередньою змовою групою осіб (ч. 5 ст. 27, ч. 3 ст. 358

КК України), а також у використанні завідомо підробленого документа (ч. 4 ст. 358 КК України).

Суд установив, що вчинені особою кримінальні правопорушення утворюють реальну сукупність, оскільки обвинувачена своїми відокремленими одна від одної діями вчинила два різні злочини. Отже, у суду першої інстанції не було підстав для застосування статті 47 КК України через відсутність такої обов'язкової об'єктивної умови, як вчинення злочину вперше.

Отже, у випадку вчинення особою кількох кримінальних правопорушень, що утворюють ідеальну сукупність, вважається, що такі кримінальні правопорушення особа вчинила вперше, а тому її може бути звільнено від кримінальної відповідальності.

Окрім того, вчинення особою кримінального правопорушення вперше безпосередньо впливає на міру покарання.

Так, у справі № 127/19722/17 Верховний Суд, надаючи оцінку доводам прокурора щодо необхідності застосування більш суворого покарання стосовно особи, зазначив, що обраний захід примусу відповідає тяжкості злочину, а касаційна скарга прокурора не містить вагомих аргументів щодо невідповідності призначеного судом покарання особі засудженого (притягнення до кримінальної відповідальності вперше, молодий вік, стан здоров'я) через його м'якість. У зв'язку із цим у Верховного Суду не виникло сумнівів у законності та обґрунтованості оскаржуваних судових рішень.

Таким чином, у кримінальному праві вчинення особою кримінального правопорушення вперше безпосередньо впливає на рішення суду щодо правопорушника, оскільки є як однією з підстав для звільнення особи від кримінальної відповідальності, так і обставиною, що впливає на міру покарання. Зокрема, це дозволяє суду призначити покарання ближче до нижньої межі, визначеної санкцією відповідної статті, а також часто є підставою для застосування статті 75 КК України, тобто звільнення від відбування покарання з випробуванням.

Перелік використаних джерел:

1.Словник української мови: в 11 т. Т. 1: А–В / АН УРСР, Ін–т мовознавства; за ред. І. К. Білодіда. Київ : Наукова думка, 1970. Стаття «вперше». URL: http://sum.in.ua/s/vpershe

2.Кримінальний кодекс України: Закон України від 05.04.2001 № 2341–III. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text

3.Конституція України: Закон України від 28.06.1996 № 254к/96–ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96–вр#Text

4.Кримінальний кодекс України. Науково–практичний коментар: у 2 т. Т. 1 : Загальна частина / за заг. ред. В.Я. Тація, В.П. Пшонки, В.І. Борисова, В.І. Тютюгіна. 5–те вид., допов. Харків: Право, 2013. 376 с.

5.Науково–практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. 7–ме вид., переробл. та допов. Київ : Юридична думка, 2010. 1288 с.

DOI https://doi.org/10.32837/11300.33607

Сидорчук Владислав
доктор філософії в галузі права, доцент кафедри кримінального процесу Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–8457–1633
e–mail: vladislam6@gmail.com

Сидорчук Інна
викладач Академічного фахового коледжу ОНЮА, м. Одеса, Україна
ORCID: https://orcid.org/0009–0005–6894–1872
e–mail: inna21511@gmail.com

КІБЕРТЕРОРИЗМ: ПОНЯТТЯ, ОЗНАКИ ТА НАПРЯМКИ ПРОТИДІЇ

У тезах розглянуто вплив інформаційних технологій в сучасному суспільстві, досліджені поняття кібетероризму, та виділені окремі ознаки відповідної діяльності на підставі яких запропоновані можливі загальні напрями протидії кібертероризму.

Ключові слова: кібертероризм, боротьба з кібертероризмом, протидія кібертероризму.

Sydorchuk Vladyslav
Doctor of Philosophy in Law, Associate Professor of the Department of Criminal Procedure, National University «Odesa Law Academy», Odesa, Ukraine

Sydorchuk Inna
Teacher, Academic Professional College ONUA, Odesa, Ukraine

CYBERTERRORISM: CONCEPT, SIGNS AND DIRECTIONS OF COUNTERACTION

The theses consider the impact of information technologies in modern society, explore the concepts of cyberterrorism, and highlight certain features of the corresponding activity, on the basis of which possible general directions of counteraction are proposed cyberterrorism.

Keywords: cyberterrorism, fight against cyberterrorism, countering cyberterrorism.

Розвиток інформаційних технологій підвищує швидкість, рівень автоматизації та ефективність виробничих процесів, сприяє формуванню комфортного середовища перебування та проживання осіб, мінімізує витрати часу на рутинні, повсякденні речі. Серед позитивних наслідків впливу широкого впровадження інформаційних технологій у виробничу діяльність, побутове життя та інші сфери життєдіяльності, варто виділити: економія часу, ресурсів та як наслідок їх вивільнення, що дає змогу використати їх в інших видах діяльності, підвищуючи ефективність їх використання; пришвидшення процесів; точність процесів та процедур, з мінімізацією помилок або людського фактору; відсутність обмеженості часу діяльності тощо.

Однак, окрім безпосереднього позитивного впливу впровадження інформаційних технологій в абсолютну більшість сфер життєдіяльності, наявні негативні наслідки або ризики, серед яких необхідно виділити наступні: деградація людського ресурсу щодо виконання окремих задач, дій або розуміння структури процесів, які виконують інформаційні технології, незважаючи на відносно недавню їх інтеграцію; тотальна залежність і віра в інформаційні технології, що знижує увагу, ретельність та критичність до інформаційного продукту; а також, залежність стабільності роботи системи від конкретних інформаційних технологій, апаратне або програмне виведення з ладу яких зупиняє наявні процеси до моменту полагодження системи або формування нової процедури без використання або з обмеженим використанням інформаційних технологій, що в окремих випадках може призводити до тяжких наслідків тощо.

Наявність зазначених нами негативних наслідків або ризиків формують вразливість окремих осіб, груп індивідів, компаній та навіть цілих держав, внаслідок чого ми часто зустрічаємо інформаційні повідомлення про випадки соціальної інженерії, шахрайства з використанням інформаційних технологій, кіберзлочинів, актів кібервійни та кібертероризму. Зважаючи на останні події в Україні нами вбачається за доцільне дослідити питання кібертероризму в Україні, визначитись із його змістом, можливими кількісними та якісними показниками в Україні та можливими напрямами протидії відповідному явищу.

Так, що стосується поняття кібертероризму, то закон України «Про основні засади забезпечення кібербезпеки України» містить визначення даного поняття – «кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням» [2]. Зважаючи на короткість відповідного визначення, що не дозволяє в повній мірі розкрити його зміст, вбачаємо за доцільне для визначення ознак, що в повній мірі характеризують кібертероризм, звернути увагу на наявні в літературі визначення відповідного поняття.

В літературі, характеризуючи кібертероризм, автори виділяють доволі специфічну мету зазначеної діяльності, яка пов’язана із політичною вмотивованістю здійснюваних дій, із забезпеченням насильства, формуванням тяжких наслідків, створення небезпеки для життя чи здоров’я людей, залякування

населення та порушення громадської безпеки, створення загроз інтересам держави та суспільства:

«кібертероризм як сплановані та політично вмотивовані атаки на інформаційні системи, комп'ютерні системи, комп'ютерні програми та сховища даних, які призводять до насильства проти некомбатантів з боку субдержавних груп або таємних організацій» [9];

«кібертероризм – це комплексна модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту» [4];

«кібертероризм виникає у сфері кібербезпеки. Загрози національній безпеці України в інформаційній сфері це сукупність умов і факторів, що створюють загрозу важливим інтересам держави, суспільства та особи внаслідок можливості негативного інформаційного впливу на свідомість і поведінку громадян, а також про інформаційні ресурси та інформаційну інфраструктуру» [6];

«кібертероризм виражається в атаках на комп'ютери, комп'ютерні програми та мережеву інформацію, ці атаки спрямовані на створення в суспільстві атмосфери страху та безнадійності в ім'я реалізації цілей та інтересів суб'єктів терористичної діяльності. Тероризм у сфері комп'ютерних технологій має такі ознаки: анонімність, віддаленість дійової особи, відносна дешевизна, відсутність необхідності використання вибухівки і самогубних акцій, великий розголос інформації» [1];

«кібертероризм як використання комп'ютерних мережевих інструментів для припинення функціонування критичних об'єктів національної інфраструктури (зокрема, енергетичних, транспортних, урядових), або для примусу або залякування уряду або цивільного населення» [8];

«кібертероризмом є залякування суспільства шляхом використання високих технологій для досягнення політичних, релігійних чи ідеологічних цілей, а також дії, які призводять до відключення, виведення з ладу об'єктів критичної інфраструктури або знищення інформації» [10];

«кібертероризмом слід розуміти навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту» [5].

Варто погодитись з тим, що «кібертероризм не слід плутати з комп'ютерними злочинами, скоєними злочинними групами, або діяльністю хакерів, оскільки тероризм має політичну мету і виникає як організаційна поведінка» [2, с. 92]. Отже однією з ключових ознак кібертероризму, яка відрізняє

його від інших видів протиправної поведінки з використанням інформаційних технологій є політична вмотивованість.

Окремо варто звернути увагу на те, що в кібертероризмі кіберпростір, інформаційні технології використовується не тільки як самоціль, кінцева мета або об'єкт посягання, але і як інструментарій для досягнення проміжних результатів в терористичній діяльності. Так, наприклад зазначається, що наявні «вісім основних способів використання терористами Інтернет–сайтів: а) ведення психологічної війни, б) пошук необхідної інформації, в) навчання терористів, г) збирання коштів, д) пропаганда тероризму, е) вербування кадрів, є) організація мережі, ж) планування та координування дій» [7], при цьому дані способи використання мережі Інтернет, використовуються для підготовки до терористичної діяльності, а не до її безпосередньої реалізації. Отже, ще одна ознака, яка характеризує кібертероризм – використання кіберпростору для підготовки до терористичного акту.

Виділені нами ознаки не є вичерпними і повно не характеризують категорію кібертероризму, однак на їх підставі можна запропонувати окремі напрями для протидії відповідній злочинній діяльності. Так, зважаючи на політичний мотив кібертероризму, варто зазначити, що саме він є першоджерелом для формування умислу, а отже має використовуватись для усунення причин агресії. Що ж стосується використання мережі Інтернет або інформаційних технологій чи ресурсів для підготовки до терористичного акту, то дана діяльність може розглядатись в криміналістичному плані, оскільки дозволяє виявити на етапі підготовки діяльність терористів чи кібертерористів.

Перелік використаних джерел:

1.Гавва С. К., Головко С. Г. Сучасний кібертероризм як загроза національній безпеці. Наукові праці. Свобода, безпека та незалежність: правовий вимір: матеріали XIII Міжнародної науково–практичної конференції, м. Київ, 24 лютого 2023 р. С. 54–56.

2.Дінжос І.В., Замула А.Ю. Кібертероризм як потенційно реалістична загроза. UNIVERSUM. 2024, № 15. С. 90–103

3.Про основні засади забезпечення кібербезпеки України: закон України від 05 жовтня 2017 року, № 2163– VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

4.Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. – СПб.: БХВ – Петербург; Арліт 2002. – 496 с.

5.Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально–правовими та кримінологічними засобами. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf

6.Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162–169.

7.Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko // Vienna: Premier Publish– ing s. r. o., 2018. 284 p.

8.James A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. URL: https://csis–prod.s3.amazonaws.com/s3fs–public/legacy_files/files/media/csis/pubs/02 1101_ risks_of_cyberterror.pdf

9.Pollitt, M. M. (1998). Cyberterrorism– Fact or Fancy?, Computer Freud&Security, 8–10.

10.Tafoya W.L. Cyber Terror. FBI Law Enforcement Bulletin. 2011. URL: http://www.fbi.gov/ stats–services/publications/law–enforcementbulletin/november–2011/cyber–terror

DOI https://doi.org/10.32837/11300.33603

Степаненко Оксана
доктор юридичних наук, доцент, завідувач кафедри кримінального права Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–4677–9868
e–mail:oksanastepanenko2015@gmail.com

КІБЕРНАСИЛЬСТВО ЯК САМОСТІЙНА ФОРМА ДОМАШНЬОГО НАСИЛЬСТВА

У тезах досліджено поняття, ознаки та основні прояви кібернасильства, а також проаналізовано практику Європейського суду з прав людини щодо визнання кібернасильства однією з форм домашнього насильства. Обґрунтовано доцільність виокремлення кібернасильства як самостійної форми домашнього насильства.

Ключові слова: кібернасильство, домашнє насильство, ЄСПЛ, цифрове насильство, права людини.

Oksana Stepanenko
Doctor of Law, Associate Professor, Head of the Department of Criminal Law, National University «Odesa Law Academy», Odesa, Ukraine

CYBERVIOLENCE AS AN INDEPENDENT FORM OF DOMESTIC VIOLENCE

The theses examine the concept, characteristics, and main manifestations of cyberviolence, as well as analyse the case law of the European Court of Human Rights regarding the recognition of cyberviolence as one of the forms of domestic violence. The expediency of distinguishing cyberviolence as an independent form of domestic violence is substantiated.

Key words: cyberviolence, domestic violence, ECtHR, digital violence, human rights.

Сучасний розвиток інформаційно–комунікаційних технологій та активне використання цифрових платформ зумовили появу нових форм протиправної поведінки, які реалізуються в онлайн–середовищі. Однією з таких форм є кібернасильство, яке набуває все більшого поширення як у публічному просторі, так і у сфері сімейних відносин. Використання електронних засобів комунікації для переслідування, контролю, психологічного тиску, шантажу, залякування чи поширення приватної інформації свідчить про трансформацію традиційних форм

насильства та необхідність адаптації правових механізмів реагування до нових цифрових викликів.

Особливість кібернасильства полягає в тому, що воно здійснюється за допомогою інформаційно–комунікаційних технологій, а його наслідки можуть бути значно тривалішими, ніж у випадку офлайн–насильства. Поширення образливого або інтимного контенту в мережі Інтернет часто має необмежене коло осіб, а цифрові матеріали можуть зберігатися тривалий час та повторно використовуватися, що спричиняє повторну віктимізацію потерпілої особи.

Ще у 2018 році Спеціальний доповідач Ради ООН з прав людини з питань насильства щодо жінок, його причин і наслідків у доповіді про насильство в Інтернеті щодо жінок і дівчат наголосив, що форми насильства, які здійснюються із використанням інформаційно–комунікаційних технологій, набувають дедалі більшого поширення. У документі зазначено, що сучасні цифрові технології трансформують способи комунікації між людьми та створюють нові цифрові простори, у межах яких можуть реалізовуватися різні форми насильства. Зокрема, акцентується увага на тому, що технології дозволяють вчиняти насильницькі дії дистанційно, анонімно та без фізичного контакту із жертвою [1].

У доповіді Спеціального доповідача підкреслюється, що кібернасильство щодо жінок охоплює будь–які акти гендерно зумовленого насильства, які здійснюються, посилюються або поширюються за допомогою цифрових технологій. До найбільш поширених форм такого насильства віднесено кіберпереслідування, доксинг, секс–шантаж, тролінг, неузгоджене поширення інтимного контенту, використання фейкових акаунтів, погрози та інші прояви цифрового контролю чи приниження. Також наголошується, що цифровий контент може швидко поширюватися по всьому світу та практично не підлягати повному видаленню, що суттєво посилює негативні наслідки для потерпілої особи [1].

У науковій літературі відсутній єдиний підхід до визначення поняття кібернасильства. Водночас більшість дослідників розглядають його як умисні агресивні дії, що здійснюються із використанням засобів електронних комунікацій та спрямовані на приниження, залякування, переслідування або психологічний вплив на особу. Комітет Конвенції про кіберзлочинність визначає кібернасильство як використання комп’ютерних систем для спричинення, сприяння або погрози насильством щодо осіб, що може призводити до фізичної, сексуальної, психологічної чи економічної шкоди [2].

Серед характерних ознак кібернасильства слід виділити: агресивний характер поведінки, використання інформаційно–комунікаційних технологій, спрямованість на приниження чи психологічний тиск. Крім того, кібернасильство часто має систематичний характер та супроводжується відчуттям постійного контролю або небезпеки для потерпілої особи.

У сучасній науці до форм кібернасильства відносять: надсилання електронних повідомлень із погрозами чи образами; незаконний доступ до електронних акаунтів; злам електронної пошти чи соціальних мереж; створення та використання фейкових профілів; розповсюдження неправдивої чи конфіденційної інформації; поширення інтимних фотографій або відео без згоди особи; кіберсталкінг; кібербулінг; онлайн–переслідування та інші форми цифрового контролю [3].

Особливо небезпечним є кібернасильство у сфері домашніх відносин, оскільки воно нерідко виступає продовженням офлайн–насильства. Кібернасильство дозволяє кривднику здійснювати контроль над потерпілою особою навіть після припинення особистого контакту. Використання GPS–відстеження, доступ до соціальних мереж, контроль електронного листування чи поширення інтимних матеріалів стають інструментами психологічного впливу та маніпуляції.

Важливе значення для формування сучасного підходу до розуміння кібернасильства має практика Європейського суду з прав людини. Так, у справі «Бутуруга проти Румунії» ЄСПЛ вперше визнав кібербулінг різновидом насильства щодо жінок [4]. Заявниця стверджувала, що її колишній чоловік без дозволу отримував доступ до її електронної пошти, соціальних мереж, приватного листування та копіював особисті фото і відео. Попри це, національні органи влади не розглядали такі дії в аспекті домашнього насильства та фактично не забезпечили належного захисту заявниці.

У зазначеному рішенні ЄСПЛ наголосив, що домашнє насильство не обмежується виключно фізичним насильством, а охоплює також психологічне насильство, переслідування та інші форми контролю над особою. Суд зазначив, що незаконне стеження за листуванням партнера, втручання в його цифрові акаунти та маніпуляція особистою інформацією можуть становити прояви домашнього насильства.

Ще одним важливим рішенням у цій сфері є справа «Володіна проти Росії». У даній справі заявниця скаржилася на відсутність належного захисту з боку держави від кібернасильства, яке здійснював її колишній партнер. Зокрема, йшлося про публікацію інтимних фотографій без згоди особи, створення фейкових профілів, кіберпереслідування та GPS–відстеження.

ЄСПЛ визнав, що зазначені дії порушують право особи на повагу до приватного життя, гарантоване ст. 8 Конвенції про захист прав людини і основоположних свобод. Суд підкреслив, що держава має позитивний обов’язок забезпечити ефективний захист потерпілих від кібернасильства, а також належне розслідування відповідних діянь.

Особливо важливим є те, що у справі «Володіна проти Росії» ЄСПЛ фактично визначив основні форми кібернасильства щодо жінок, серед яких: злам акаунтів, видавання себе за іншу особу, цифрове переслідування, спостереження, погрози, поширення конфіденційної чи інтимної інформації та інші прояви

цифрового контролю. Суд наголосив, що онлайн–насильство є тісно пов'язаним із офлайн–насильством та становить одну із форм домашнього насильства.

Практика ЄСПЛ свідчить про поступове формування міжнародного підходу, відповідно до якого кібернасильство розглядається як самостійний різновид насильства щодо особи. Водночас важливо враховувати, що кібернасильство має власну специфіку, яка проявляється у використанні цифрових технологій як засобу вчинення протиправних дій, можливості дистанційного впливу на потерпілу особу та складності усунення наслідків такого впливу [5].

Варто також зазначити, що у 2022 році Європейська комісія запропонувала державам–членам ЄС посилити заходи реагування на кібернасильство щодо жінок та забезпечити криміналізацію відповідних проявів протиправної поведінки [6]. Це свідчить про міжнародне визнання суспільної небезпечності кібернасильства та необхідності формування ефективних механізмів протидії йому.

У рішенні Валківського районного суду Харківської області від 04 грудня 2023 року у справі № 615/2288/23 простежується важливий підхід до розуміння психологічного та цифрового компоненту домашнього насильства [7].

Суд встановив, що після розірвання шлюбу колишній чоловік систематично здійснював щодо заявниці психологічне насильство, яке проявлялося у погрозах фізичною розправою, нецензурній лексиці, переслідуванні та контролі. Особливу увагу у справі привертає використання цифрових засобів комунікації та відеозаписів як інструменту психологічного впливу. Зокрема, кривдник записував відео за участю дітей, під час яких змушував їх повторювати образливі та нецензурні висловлювання щодо матері.

У контексті дослідження кібернасильства це рішення є показовим, оскільки демонструє використання інформаційно–комунікаційних технологій для здійснення психологічного тиску та приниження постраждалої особи. Хоча суд прямо не використовує термін «кібернасильство», фактичні обставини справи свідчать про наявність елементів цифрового насильства, а саме використання відеофіксації та електронних засобів комунікації як способу психологічного впливу на заявницю та дітей.

Суд наголосив, що психологічне насильство включає словесні образи, погрози, переслідування, залякування та інші дії, які викликають у постраждалої особи побоювання за власну безпеку чи завдають шкоди психічному здоров'ю. Важливим є те, що суд врахував ризик негативного впливу на психічний стан дітей через їх залучення до приниження матері та використання їх як інструменту психологічного тиску.

Значення даного рішення для аналізованої тематики полягає також у тому, що суд застосував обмежувальний припис, який передбачав, зокрема, заборону вести листування, телефонні переговори та контактувати із постраждалою особою через інші засоби зв'язку. Це свідчить про визнання судом того, що засоби

електронної комунікації можуть використовуватися як інструмент домашнього насильства та потребують відповідного правового реагування.

Аналізоване рішення підтверджує сучасну тенденцію розширення підходів до розуміння домашнього насильства та врахування цифрових способів психологічного впливу. Воно демонструє, що навіть за відсутності прямого нормативного закріплення терміна «кібернасильство» судова практика фактично визнає окремі його прояви як форму психологічного домашнього насильства.

Таким чином, кібернасильство є сучасною формою насильницької поведінки, яка характеризується використанням інформаційно–комунікаційних технологій для здійснення психологічного, емоційного чи іншого протиправного впливу на особу. Аналіз міжнародних документів, наукових підходів, вітчизняної судової практики та практики ЄСПЛ свідчить про те, що кібернасильство у сфері сімейних відносин має всі ознаки домашнього насильства.

Враховуючи специфіку кібернасильства, його суспільну небезпечність, поширеність та сучасну практику ЄСПЛ, доцільним є виокремлення кібернасильства як самостійної форми домашнього насильства. Такий підхід сприятиме удосконаленню кримінально–правових механізмів реагування, забезпеченню ефективного захисту потерпілих осіб та приведенню національного законодавства у відповідність до міжнародних стандартів у сфері захисту прав людини.

Перелік використаних джерел:

1.Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (A/HRC/38/47, 18 June 2018). Original: English. URL: https://documents–dds–ny.un.org/doc/UNDOC/GEN/G18/184/58/PDF/G1818458.pdf?OpenElement

2.Cybercrime Convention Committee (T–CY). URL: https://rm.coe.int/t–cy–mapping–study–on–cyberviolence–final/1680a1307c.

3.Руфанова В. Ґендерно зумовлене кібернасильство в світлі практики Європейського суду з прав людини. Knowledge, Education, Law, Management. 2021. № 6 (42). С. 212.

4.Buturugă V. Romania (Requête no 56867/15). 11 février 2020. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001–200842%22]}

5.Степаненко О. В. Кібернасильство як форма домашнього насильства. Держава та регіони. Серія: Право. 2022. № 4 (78). С. 224–228. https://doi.org/10.32840/1813–338X–2022.4.34

6.Пропозиція Європейської комісії щодо директиви щодо боротьби з насильством щодо жінок і домашнім насильством від 08 березня 2022 року. URL: https://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX%3A52022PC0105

7.Рішення Валківського районного суду Харківської області від 04 грудня 2023 року у справі № 615/2288/23 URL: https://reyestr.court.gov.ua/Review/115361482

DOI https://doi.org/10.32837/11300.33601

Тітуніна Катерина
кандидат юридичних наук,
головний науковий співробітник відділу дослідження проблем протидії кіберзлочинам та загрозам інформаційній безпеці
Міжвідомчого науково–дослідного центру з проблем боротьби з організованою злочинністю при РНБО України,
м. Київ, Україна
ORCID: https://orcid.org/0000–0003–2800–345X
e–mail: titunina_kateryna@ukr.net

ПРОТИДІЯ РАДИКАЛІЗАЦІЇ ТА ГІБРИДНИМ ЗАГРОЗАМ В УСТАНОВАХ ВИКОНАННЯ ПОКАРАНЬ В УМОВАХ ВОЄННОГО СТАНУ

У тезах досліджено виклики національній безпеці, пов’язані з ризиками радикалізації засуджених та використанням пенітенціарного середовища спецслужбами РФ для гібридної агресії. Обґрунтовано необхідність впровадження інструментів оцінки ризиків (VERA–2R), залучення інституту капеланства для деконструкції екстремістських наративів та посилення контррозвідувального профайлінгу лідерів злочинного світу. Проаналізовано феномен «кримінального колабораціонізму» та запропоновано шляхи інтеграції оперативних підрозділів установ виконання покарань у загальнодержавну систему антитерористичної діяльності.

Ключові слова: пенітенціарна система, радикалізація, гібридні загрози, кримінальний колабораціонізм, національна безпека, воєнний стан.

Titunina Kateryna
PhD in Law, Chief Researcher of the Department for Researching Problems of Countering Cybercrime and Information Security Threats, Interagency Scientific and Research Center on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine
Kyiv, Ukraine

COUNTERING RADICALIZATION AND HYBRID THREATS IN PENITENTIARY INSTITUTIONS UNDER MARTIAL LAW

These papers examine national security challenges related to the risks of prisoner radicalization and the exploitation of the penitentiary environment by Russian intelligence services for hybrid warfare. The study justifies the need for implementing risk assessment tools (VERA–2R), engaging chaplaincy to deconstruct extremist narratives, and strengthening counterintelligence profiling of organized crime leaders.

The phenomenon of «criminal collaboration» is analyzed, and ways to integrate operational units of correctional facilities into the national counter–terrorism system are proposed.

Keywords: penitentiary system, radicalization, hybrid threats, criminal collaboration, national security, martial law.

В умовах триваючої збройної агресії РФ проти України та глобального зростання терористичної активності, установи виконання покарань перетворилися на об'єкт підвищеного інтересу як для міжнародних терористичних організацій, так і для ворожих спецслужб. Пенітенціарне середовище, з його концентрацією осіб, схильних до насильства та критично налаштованих до державної системи, виступає потенційним «інкубатором» для вербування агентури, поширення радикальних ідеологій та формування диверсійного резерву ворога.

Стратегія безпеки у цьому напрямі має базуватися не на реактивних заходах, а на проактивному моніторингу, що включає два взаємопов'язані вектори: протидію ідеологічній радикалізації та нейтралізацію гібридних загроз з боку РФ. Для потреб національної безпеки пропонується впровадження комплексної системи індикаторів та контрзаходів, адаптованої до стандартів ЄС.

Впровадження інструментарію оцінки ризиків (Risk Assessment Tools). Українська пенітенціарна система потребує імплементації спеціалізованих діагностичних протоколів, зокрема протоколу VERA–2R (Violent Extremism Risk Assessment), що довів свою ефективність у країнах Євросоюзу. Сутність методу полягає у структурованому професійному судженні, яке дозволяє психологам та оперативним працівникам виявляти когнітивні та поведінкові маркери ідеологічних змін у засудженого на докримінальній стадії.

Індикаторами раннього попередження можуть бути:

– раптова зміна зовнішнього вигляду, відмова від імені на користь псевдоніма;

– агресивний прозелітизм (нав'язування своєї віри іншим);

– категорична сегрегація від родини та персоналу, яких таврують як «ворогів віри» або «представників ворожої системи»;

– поява специфічної символіки (татуювань, графіті), що глорифікує тероризм.

Задля нівелювання таких процесів ефективнім є використання «м'якої сила». Репресивні методи боротьби з релігійним екстремізмом часто є контрпродуктивними, створюючи образ «мученика».

Також важливим є переривання каналів комунікації між лідерами терористичних осередків. Утримання ідеологів у камерах малого наповнення або приміщеннях камерного типу (ПКТ) для недопущення створення ними «тюремних джамаатів» (радикальних громад). Тобто інформаційна та фізична ізоляція ідеологів. Зауважимо, що в умовах війни традиційна організована злочинність трансформувалася в інструмент гібридної агресії. Оперативний аналіз свідчить

про спроби спецслужб країни–агресора (ФСБ, ГРУ) відновити контроль над «тюремним світом» України через підконтрольних «злодіїв у законі», які перебувають на території РФ.

Україна отримала унікальний досвід стикнувшись із феноменом «Кримінального колабораціонізму» – організація тюремних бунтів, масових непокор або нападів на персонал з метою дестабілізації ситуації в тилу за вказівкою російських кураторів. На відміну від ідеологічного колабораціонізму, кримінальні елементи співпрацюють з ворогом з меркантильних мотивів або задля збереження статусу.

Крім того, починаючи ще з 2014 року існує небезпечний прецедент масових спроб вербування в'язнів до ворожих ПВК та диверсійної роботи. Через нелегальні засоби зв'язку засудженим (особливо з бойовим досвідом) пропонують амністію та фінанси в обмін на диверсії в установі (підпали, пошкодження інфраструктури) або співпрацю після звільнення.

Дієвими засобами протидії є запровадження контррозвідувального профайлінгу кримінальних авторитетів. Будь–який контакт лідера ОЗУ із зовнішнім світом (адвокати, родичі з окупованих територій) має розглядатися як потенційний канал передачі ворожих інструкцій.

Також, ефективним вбачається створення спільної бази даних ДКВС та Департаменту військової контррозвідки СБУ щодо осіб, які брали участь у НЗФ «Л/ДНР» або мають стійкі зв'язки з РФ. Посилений моніторинг їхніх комунікацій у месенджерах (Telegram, Signal, Max тощо).

Крім того, Україна стикнулась з проблемою зрощування криміналітету з ворожими диверсійно–розвідувальними групами (трафік зброї). ОЗУ намагаються налагодити канали постачання трофейної зброї з прифронтових зон для потреб кримінального світу.

В цьому аспекті вбачається за необхідне інтеграція ОРД в УВП у загальнодержавну систему антитерористичної діяльності. Це надасть оперативникам виявляти ланцюжки постачання зброї ще на етапі «замовлення» засудженими.

Отже, сучасні безпекові виклики вимагають переосмислення підходів до діяльності оперативних підрозділів та переходу від пасивного спостереження до системної оперативної аналітики ідеологічних процесів і ризиків радикалізації. У зв'язку з цим оперативний працівник нового покоління повинен володіти не лише спеціальними навичками оперативно–розшукової діяльності, а й базовими знаннями у сфері психології тероризму та радикалізації, що дозволить своєчасно відрізняти прояви релігійних переконань від ознак екстремістської діяльності. Водночас в умовах гібридної війни особливої актуальності набуває необхідність законодавчого визнання лідерів злочинних спільнот, які підтримують зв'язки зі спецслужбами РФ, як учасників деструктивної діяльності проти національної безпеки України. Це обумовлює доцільність застосування до таких осіб окремих

механізмів воєнного права, зокрема спеціальної ізоляції як суб'єктів підвищеної загрози державній безпеці, а у випадку доведення співпраці з державою–агресором – можливості використання процедур, пов'язаних з обміном полоненими.

Сучасні виклики у сфері національної безпеки та трансформація криміногенних процесів в умовах воєнного стану обумовлюють необхідність комплексного вдосконалення оперативно–розшукової діяльності в установах виконання покарань України. Проведений аналіз засвідчив, що ефективне функціонування пенітенціарної системи безпосередньо пов'язане зі спроможністю держави своєчасно протидіяти організованій злочинності, корупційним проявам, терористичним загрозам, радикалізації та іншим деструктивним процесам, які можуть використовуватися для дестабілізації внутрішньої безпеки держави.

DOI https://doi.org/10.32837/11300.33625

Цехан Дмитро
доктор юридичних наук, професор,
завідувач кафедри оперативно–розшукової та поліцейської діяльності
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–6503–6985
e–mail: dimatsekhan@gmail.com

ІДЕОЛОГІЯ ФОРМУВАННЯ ТА ФУНКЦІОНУВАННЯ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Проаналізовані основні аспекти щодо трансформаційних процесів формування та функціонування злочинних угруповань в умовах збройного конфлікту. Визначені основні напрями трансформації організованих форм кримінальної активності, зокрема й у частині створення організованих злочинних угруповань, а також особливості встановлення впливу на окремі соціальні процеси в умовах збройного конфлікту.

Ключові слова: збройний конфлікт, організована злочинність, організоване злочинне угруповання, ідеологія формування та функціонування організованих злочинних угруповань.

Tsekhan Dmytro
Doctor of Legal Sciences, Professor,
Chief of the Department of Operational Investigation and Police Activities
National University «Odesa Law Academy»,
Odesa, Ukraine

IDEOLOGY OF THE FORMATION AND FUNCTIONING OF ORGANIZED CRIMINAL GROUPS IN CONDITIONS OF ARMED CONFLICT

The main aspects of the transformation processes of the formation and functioning of criminal groups in the context of armed conflict are analyzed. The main directions of the transformation of organized forms of criminal activity are determined, in particular in terms of the creation of organized criminal groups, as well as the features of establishing an influence on individual social processes in the context of armed conflict.

Keywords: armed conflict, organized crime, organized criminal group, ideology of the formation and functioning of organized criminal groups.

Формування та подальше функціонування стійких та системно функціонуючих злочинних угруповань завжди супроводжувалось відповідними психологічними[1;6] та ідеологічними засадами[2;3;5], які трансформувались відповідно до конкретних соціально–економічних умов у межах реалізації організованою злочинністю як складним соціальним явищем своєї функції адаптивності. В історичному розрізі це доволі чітко демонструється поступовою трансформацією «злодійської ідеології», для якої були характерні стійкі поведінкові патерни, котрі трансформувались під впливом соціально–економічних змін, зокрема від повної заборони контактів із правоохоронними органами та підтримки держави до встановлення лідерами кримінального середовища неформальних дружніх відносин із представниками органів державної влади, а в окремих випадках паралельне поєднання функції лідерів ОЗУ та виконання функцій представників органів державної влади чи місцевого самоврядування. У той же час, слушно звернути увагу, що триваючий збройний конфлікт закономірно формує нову соціально–економічну реальність, значно впливає на роботу правоохоронних інституцій щодо постійного та системного контролю над організованими формами злочинної діяльності, що створює передумови для розвитку нових ідеологічних підвалин формування та функціонування організованих злочинних угруповань.

У період збройного конфлікту злочинність перестає бути виключно латентним або суто кримінальним явищем, натомість набуває ознак паралельної системи влади, здатної впливати на економічні, політичні, інформаційні та безпекові процеси, що набуває особливо активного вираження у прифронтових регіонах, на тимчасово окупованих територіях, а також на територіях, які були деокуповані ЗСУ і де проведені стабілізаційні поліцейські заходи, але повний контроль над оперативною обстановкою не відновлений. Зважаючи на це, можна відзначити, що ідеологія злочинних угруповань у таких умовах виходить за межі традиційної кримінальної мотивації, трансформуючись у комплексну систему переконань, виправдань, цінностей та механізмів легітимізації протиправної діяльності.

В умовах війни або тривалого збройного протистояння виникає особливий криміногенний простір, у межах якого організовані злочинні угруповання адаптуються до нових соціальних реалій, використовуючи дестабілізацію державного управління, ослаблення контролю за територіями, зростання незаконного обігу зброї, масові міграційні процеси та психологічну травматизацію населення. Саме ці фактори формують підґрунтя для появи специфічної кримінальної ідеології, яка базується на принципах силового домінування, виправдання насильства, культивування автономності від держави та створення альтернативних центрів впливу.

Ідеологія злочинних угруповань у воєнний період виконує не лише функцію внутрішньої консолідації учасників, але й забезпечує формування системи колективної ідентичності, яка дозволяє учасникам сприймати свою діяльність як

соціально допустиму або навіть необхідну. У таких умовах злочинна діяльність часто маскується під псевдопатріотичну, військову, гуманітарну або «захисну» діяльність. Це створює небезпечний ефект розмиття меж між легітимною силовою активністю та організованою злочинністю.

Ключовим елементом ідеології злочинних угруповань у період збройного конфлікту є концепція «силової справедливості», відповідно до якої право сильнішого замінює механізми державного правосуддя. Учасники таких структур формують переконання, що в умовах війни правові обмеження втрачають значення, а досягнення результату будь–якими засобами є виправданим. Подібна деформація правосвідомості створює сприятливі умови для легітимізації рекету, мародерства, незаконного обігу зброї, контрабанди, торгівлі людьми, рейдерства та інших форм організованої злочинної діяльності.

Особливістю функціонування злочинних угруповань в умовах збройного конфлікту є їхня здатність інтегруватися у військові, політичні та економічні процеси. Частина таких структур виникає на основі колишніх кримінальних об’єднань, які адаптуються до нових умов, інша – формується безпосередньо під впливом війни з осіб, які мають бойовий досвід, доступ до зброї та навички силового примусу. У результаті виникає феномен мілітаризованої організованої злочинності, для якої характерні високий рівень дисципліни, жорстка ієрархія, використання тактичного планування та застосування військових методів управління на що зверталась увага у наукових джерелах[4].

Ідеологічна модель таких угруповань часто базується на принципах закритості, абсолютної лояльності, культу сили та домінування інтересів організації над інтересами особи. Усередині угруповань формується власна система норм і правил поведінки, порушення яких карається жорсткими санкціями. Це забезпечує високий рівень внутрішньої керованості та ускладнює проникнення правоохоронних органів у злочинне середовище.

Важливою складовою ідеології злочинних угруповань у воєнний період є інформаційно–психологічний компонент. Злочинні структури активно використовують страх, дезінформацію, пропаганду та маніпуляцію суспільною свідомістю для зміцнення свого впливу. У регіонах з ослабленим державним контролем вони можуть формувати образ «альтернативної влади», яка забезпечує «порядок», «захист» або «економічну стабільність». Подібний механізм особливо небезпечний у ситуаціях тривалого конфлікту, коли населення втрачає довіру до офіційних державних інституцій.

У структурному аспекті ідеологія злочинних угруповань у зоні збройного конфлікту характеризується високою адаптивністю. Такі організації здатні швидко змінювати форми діяльності залежно від оперативної ситуації: від класичної кримінальної активності до участі у воєнізованих схемах, нелегальному постачанні ресурсів, контролі над логістичними маршрутами або використанні корупційних механізмів для проникнення у державний сектор. Унаслідок цього

організована злочинність набуває гібридного характеру, поєднуючи кримінальні, військові та економічні компоненти.

Окрему роль у функціонуванні таких угруповань відіграє економічна ідеологія виживання та надприбутку. Воєнний конфлікт створює дефіцит ресурсів, руйнує офіційні ринки та стимулює розвиток тіньової економіки. Злочинні угруповання використовують ці умови для встановлення контролю над потоками зброї, пального, гуманітарної допомоги, наркотичних засобів, цінних ресурсів та нелегальної міграції. У межах цієї ідеології війна сприймається не як катастрофа, а як середовище для отримання влади, прибутку та розширення сфер впливу.

Водночас необхідно враховувати, що тривале існування злочинних угруповань у воєнних умовах сприяє формуванню специфічної субкультури насильства. Постійна присутність зброї, нормалізація агресії, психологічна десенсибілізація до жорстокості та домінування силових методів вирішення конфліктів створюють передумови для глибокої криміналізації соціального середовища. Це становить особливу небезпеку для післявоєнного періоду, оскільки демобілізовані учасники незаконних структур можуть інтегруватися у мирне суспільство із збереженням кримінальної ідентичності та навичок організованого насильства.

На концептуальному рівні ідеологію створення та функціонування злочинних угруповань в умовах збройного конфлікту доцільно визначати як систему кримінально детермінованих переконань, норм, мотиваційних установок та механізмів легітимізації протиправної діяльності, що формується під впливом воєнної дестабілізації та забезпечує організаційну стійкість, внутрішню консолідацію, виправдання насильства і розширення сфер незаконного впливу в умовах ослаблення державного контролю.

Таким чином, збройний конфлікт виступає не лише фактором дестабілізації безпекового середовища, але й каталізатором трансформації організованої злочинності у більш складну, адаптивну та ідеологічно обґрунтовану форму кримінальної діяльності. Це вимагає формування нових концептуальних підходів до протидії організованій злочинності, які повинні враховувати не лише оперативно–розшуковий чи кримінально–правовий компонент, але й інформаційно–психологічні, соціальні та безпекові аспекти функціонування злочинних угруповань у період війни.

Перелік використаних джерел:

1.Дмітрієва С.М., Самусь І.І. Психологія злочинної групи та її лідера. Вісник Київського інституту бізнесу та технологій. 2016. №3. (31) С.22–26.

2.Дрьомін В.М. Інституційна теорія злочинності та криміналізація суспільства: автореферт дис… докт. юрид. наук: 12.00.08. Одеса. 2010. 40 с.

3.Кушкович А. Зарубіжний досвід дослідження динаміку культу та кримінальної трансформації. Юридичний вісник. 2024. №4. С.167–173.

4.Мартиненок Д.О. Криміналістична класифікація злочинних угруповань парамілітарного типу. Південноукраїнський правничий часопис. 2020. № 4. С.85–90.

5.Рущенко І.П. Соціологія злочинності: монографія. Харків. Вид–во Національного ун–ту внутріш. справ. 2001. 310 с.

6.Цехан Д.М., Яцкевич Р.В. Стійкість організованих злочинних угруповань як міждисциплінарна категорія. Наука і правоохоронна. 2026. Вип. 1 (71). С.73–79.

DOI https://doi.org/10.32837/11300.33626

Цитряк Віктор
кандидат юридичних наук, доцент, доцент кафедри кримінального процесу,
заступник декана факультету прокуратури та слідства (кримінальної юстиції)
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID ID: https://orcid.org/0000–0000–0000–0000
e–mail: tsytriak.viktor@onua.edu.ua

ЕФЕКТИВНІСТЬ ОПЕРАТИВНО–РОЗШУКОВОЇ ДІЯЛЬНОСТІ ЯК ЗАСОБУ ЗАБЕЗПЕЧЕННЯ ПРАВОПОРЯДКУ В ПЕНІТЕНЦІАРНИХ УСТАНОВАХ

Досліджено значення оперативно–розшукової діяльності у забезпеченні правопорядку в пенітенціарних установах. Визначено чинники її ефективності, основні напрями реалізації та перспективи вдосконалення в умовах сучасних безпекових викликів.

Ключові слова: оперативно–розшукова діяльність, пенітенціарні установи, правопорядок, профілактика правопорушень, оперативна інформація, безпека, кримінально–виконавча система.

Tsitryak Viktor
PhD in Law, Associate Professor,
Associate Professor in the Department of Criminal Procedure,
Deputy Dean of the Faculty of Public Prosecution and Investigation (Criminal Justice) at the National University «Odesa Law Academy»,
Odesa, Ukraine

THE EFFECTIVENESS OF OPERATIONAL AND INVESTIGATIVE ACTIVITIES AS A MEANS OF ENSURING LAW AND ORDER IN PRISONS

This study examines the significance of operational and investigative activities in maintaining law and order within correctional institutions. It identifies the factors contributing to their effectiveness, the main areas of implementation, and prospects for improvement in the context of contemporary security challenges.

Key words: operational and investigative activities, prisons, law and order, crime prevention, operational intelligence, security, the penal system.

Забезпечення належного рівня правопорядку в пенітенціарних установах є одним із ключових завдань державної політики у сфері виконання кримінальних

покарань. Специфіка функціонування установ виконання покарань обумовлена постійною концентрацією значної кількості осіб, які мають кримінальний досвід, схильність до протиправної поведінки або підтримують неформальні зв'язки із представниками злочинного середовища за межами установи. У таких умовах особливого значення набуває оперативно–розшукова діяльність, яка виступає важливим інструментом попередження, виявлення та припинення правопорушень, забезпечення безпеки персоналу, засуджених і відвідувачів, а також підтримання стабільного режиму функціонування пенітенціарних установ.

Сучасна пенітенціарна система стикається з численними викликами, пов'язаними з поширенням організованих форм злочинної діяльності, незаконним обігом наркотичних засобів, психотропних речовин, зброї та заборонених предметів, координацією злочинної діяльності з місць позбавлення волі, проявами екстремізму, корупційними ризиками та іншими загрозами безпеці. Наявність таких факторів зумовлює необхідність використання комплексу правових, організаційних, профілактичних та оперативно–розшукових заходів, спрямованих на своєчасне отримання інформації про протиправні наміри та діяльність окремих осіб або груп.

Оперативно–розшукова діяльність у пенітенціарних установах має специфічний характер, що відрізняє її від аналогічної діяльності інших правоохоронних органів. Її основною особливістю є здійснення в умовах обмеженого простору, постійного контролю за поведінкою засуджених та наявності широких можливостей для безпосереднього спостереження за процесами, що відбуваються серед контингенту установи. Разом із тим такі умови не усувають необхідності використання спеціальних оперативних методів отримання інформації, оскільки значна частина протиправної діяльності має латентний характер і ретельно приховується від адміністрації.

Ефективність оперативно–розшукової діяльності значною мірою визначається здатністю оперативних підрозділів своєчасно виявляти осіб, схильних до вчинення правопорушень, встановлювати неформальні зв'язки між засудженими, виявляти канали надходження заборонених предметів та прогнозувати розвиток криміногенних процесів усередині установи. Оперативні працівники повинні не лише фіксувати вже вчинені порушення режиму, а й здійснювати систематичний аналіз оперативної обстановки, виявляти тенденції її розвитку та формувати профілактичні заходи, спрямовані на нейтралізацію потенційних загроз [1].

Важливим критерієм ефективності оперативно–розшукової діяльності є рівень попередження злочинів. Саме профілактична функція становить одну з головних переваг оперативно–розшукових заходів у пенітенціарному середовищі. Завдяки своєчасному отриманню оперативної інформації можливо запобігати підготовці втеч, масових заворушень, актів насильства щодо персоналу або інших засуджених, організації каналів постачання наркотичних засобів та інших

небезпечних дій. Запобігання таким проявам дозволяє уникнути значних негативних наслідків як для конкретної установи, так і для суспільства загалом.

Особливу увагу слід приділяти протидії діяльності організованих злочинних груп у місцях позбавлення волі. Незважаючи на ізоляцію окремих осіб від суспільства, кримінальні зв'язки нерідко зберігаються та продовжують функціонувати через використання засобів зв'язку, корупційних механізмів або осіб, які перебувають на волі. У таких випадках оперативно–розшукова діяльність стає одним із найбільш ефективних інструментів виявлення та документування злочинної активності. Збір та аналіз інформації про структуру неформальних угруповань, їх лідерів, джерела фінансування та канали комунікації дозволяє своєчасно реагувати на загрози та мінімізувати вплив кримінального середовища на функціонування установи.

Одним із важливих напрямів оперативно–розшукової діяльності є виявлення та перекриття каналів надходження заборонених предметів до пенітенціарних установ. Практика свідчить, що незаконне переміщення мобільних телефонів, наркотичних засобів, алкогольних напоїв, колючо–ріжучих предметів та інших речей часто здійснюється із залученням як засуджених, так і сторонніх осіб. У деяких випадках до таких схем можуть бути причетні представники персоналу установ, що істотно підвищує суспільну небезпеку подібних правопорушень. Саме тому ефективність оперативно–розшукової діяльності значною мірою залежить від здатності оперативних підрозділів виявляти корупційні ризики та забезпечувати належний рівень внутрішньої безпеки.

Суттєве значення має інформаційно–аналітичне забезпечення оперативно–розшукової діяльності. Сучасні умови потребують використання цифрових технологій, електронних баз даних, автоматизованих систем обробки інформації та аналітичних інструментів прогнозування ризиків. Аналіз поведінки засуджених, їх соціальних зв'язків, дисциплінарної практики, психологічних характеристик та інших показників дозволяє формувати обґрунтовані прогнози щодо можливих проявів протиправної активності. Водночас використання таких технологій повинно здійснюватися з дотриманням законодавчих вимог щодо захисту персональних даних та прав людини.

Ефективність оперативно–розшукової діяльності безпосередньо пов'язана з рівнем професійної підготовки персоналу. Оперативний працівник повинен володіти знаннями у сфері кримінального права, кримінального процесу, криміналістики, психології, конфліктології та інформаційної безпеки. Важливого значення набувають навички аналізу оперативної інформації, встановлення психологічного контакту, оцінки достовірності отриманих відомостей та прийняття управлінських рішень в умовах дефіциту часу. Високий професіоналізм оперативного персоналу сприяє підвищенню результативності діяльності та мінімізації помилок при реалізації оперативних заходів.

Не менш важливою складовою ефективності є належна взаємодія оперативних підрозділів пенітенціарних установ із іншими правоохоронними

органами. Обмін інформацією між оперативними підрозділами Державної кримінально–виконавчої служби, Національною поліцією, Службою безпеки України, органами прокуратури та іншими суб'єктами забезпечення правопорядку створює передумови для комплексного реагування на кримінальні загрози. Особливої актуальності така взаємодія набуває під час документування діяльності організованих злочинних груп, які здійснюють координацію злочинної активності як усередині установ виконання покарань, так і за їх межами.

Разом із позитивними аспектами існують і певні проблеми, що впливають на результативність оперативно–розшукової діяльності. До них належать недостатнє матеріально–технічне забезпечення окремих установ, кадровий дефіцит, обмеженість фінансових ресурсів, недосконаліть окремих нормативно–правових механізмів, а також постійна адаптація кримінального середовища до заходів контролю [2]. Крім того, розвиток сучасних засобів комунікації створює нові можливості для прихованої координації злочинної діяльності, що потребує вдосконалення оперативних методів та технологій протидії.

Перспективним напрямом підвищення ефективності оперативно–розшукової діяльності є впровадження ризик–орієнтованого підходу до оцінки оперативної обстановки, використання сучасних аналітичних систем, розширення міжвідомчої взаємодії, удосконалення системи професійної підготовки персоналу та посилення заходів внутрішньої безпеки. Важливим завданням залишається забезпечення балансу між необхідністю підтримання правопорядку та дотриманням прав і свобод людини, оскільки ефективність діяльності правоохоронних органів повинна оцінюватися не лише за кількісними показниками виявлених правопорушень, а й за рівнем законності застосовуваних заходів.

Отже, оперативно–розшукова діяльність є одним із ключових засобів забезпечення правопорядку в пенітенціарних установах, оскільки дозволяє своєчасно виявляти, попереджати та припиняти правопорушення, здійснювати контроль за криміногенною обстановкою, протидіяти організованій злочинності та забезпечувати безпеку персоналу і засуджених. Її ефективність визначається комплексом організаційних, правових, кадрових та технічних факторів, а подальше вдосконалення оперативно–розшукової роботи має стати важливою умовою підвищення результативності функціонування всієї пенітенціарної системи України.

Перелік використаних джерел:

1. Юхно А.О. Актуальні аспекти взаємодії оперативних підрозділів підчас запобігання, припинення, виявлення і розкриття злочинів. Попередження злочинів суб'єктами оперативно–розшукової діяльності: Матер. наук.–практ. конф. (Харків, 17грудня 2010 р.). Харків: ХНУВС, 2010. 248 с.

2. Романов М.С. Контррозвідувальний пошук в установах виконання покарань та слідчих ізоляторах Державної кримінально–виконавчої служби України Міністерства юстиції України. Збірник наукових праць Національної академії СБ України. 2017. № 63. 232 с.

Секція 5
КРИМІНАЛЬНО–ПРОЦЕСУАЛЬНІ, ОПЕРАТИВНО–РОЗШУКОВІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ У ЦИФРОВИЙ ЧАС

DOI https://doi.org/10.32837/11300.33546

Албул Сергій
кандидат юридичних наук, професор,
професор кафедри оперативно–розшукової та поліцейської діяльності
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–3253–9225
e–mail:omaxy@ukr.net

КРИМІНАЛЬНА РОЗВІДКА ЯК СИСТЕМНИЙ ЕЛЕМЕНТ КОМПЛЕКСНОЇ МОДЕЛІ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ

Розглянуто проблемні аспекти становлення в Україні кримінальної розвідки, як сучасної форми реалізації правоохоронної функції держави. Акцентовано увагу на аналітичній складовій кримінальної розвідки як системного елементу комплексної (ре– та проактивної) моделі поліцейської діяльності.

Ключові слова: аналітика, аналітичний продукт, кримінальна розвідка, моделі поліцейської діяльності, оперативно–розшукова діяльність.

Albul Serhii
Candidate of Legal Sciences, Professor,
Professor of the Department of Operational Investigation and Police Activities
National University «Odesa Law Academy»,
Odesa, Ukraine

CRIMINAL INTELLIGENCE AS A SYSTEMIC ELEMENT OF A COMPREHENSIVE MODEL OF POLICE ACTIVITIES

The problematic aspects of the formation of criminal intelligence in Ukraine as a modern form of implementing the law enforcement function of the state are considered. Attention is focused on the analytical component of criminal intelligence as a systemic element of a complex (re– and proactive) model of police activity.

Key words: analytics, analytical product, criminal intelligence, police activity models, operational and investigative activities.

В умовах євроінтеграційних процесів, зростання суспільного запиту на прозору, ефективну та правомірну роботу правоохоронних органів, що

відбуваються на фоні глобальних загроз організованої злочинності, новелізації, у тому числі цифровізації злочинних технологій, формування сучасної концепції кримінальної розвідки як форми реалізації правоохоронної функції держави, набуває особливої актуальності. Становлення в Україні кримінальної розвідки, яка являє собою заснований на аналітиці та прогнозуванні особливий вид діяльності уповноважених державних органів, що полягає у здійсненні системи гласних та негласних заходів, застосуванні спеціальних засобів, та спрямований на своєчасне запобігання, виявлення, припинення та розкриття кримінальних правопорушень, розшук осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від відбування кримінального покарання, зниклих безвісті, встановленні невпізнаних осіб, ідентифікації невпізнаних трупів, а також нейтралізації реальних і потенційних загроз національній безпеці України, здійснюється шляхом поетапної трансформації оперативно–розшукової діяльності [3, с. 13]. При цьому, трансформація – це глибока зміна, перетворення форми, виду або суттєвих властивостей об'єкта, системи чи процесу, що веде до їх якісно нового стану [7, с. 327]. Принагідно слід наголосити, що концептуальна трансформація оперативно–розшукової діяльності не є руйнуванням, не є відмовою та/чи термінологічною заміною. В контексті трансформації оперативно–розшукової діяльності у кримінальну розвідку це не поверхневе оновлення, а фундаментальна перебудова, модернізація для підвищення ефективності, досягнення вищого рівня функціональності, адаптації до нових умов та сучасних викликів. Кримінальна розвідка має реалізовуватися на стратегічному та тактичному рівнях. Стратегічна кримінальна розвідка застосовується задля забезпечення національної безпеки, виявлення патернів загроз, прогнозування та відстеження системних ознак зростання злочинної активності, встановлення пріоритетів діяльності уповноважених правоохоронних органів. На стратегічному рівні здійснюється ідентифікація та оцінювання кримінальних загроз, визначення вразливостей правоохоронної системи або криміногенного середовища, формування управлінських рішень щодо запобігання вчиненню кримінальних правопорушень і протидії злочинності з метою підготовки стратегічних управлінських рішень та визначення ризиків розвитку криміногенної ситуації. У свою чергу, на тактичному рівні кримінальна розвідка орієнтується на знання про види злочинних організацій та груп, включає аналіз тих злочинів, які через їх складність, тяжкість або характер повторюваності не можуть бути ефективно виявлені шляхом проведення досудового розслідування окремого кримінального провадження. На тактичному рівні здійснюється аналіз злочинності та злочинів на конкретній території за невеликий проміжок часу, за певним видом злочину чи протиправної діяльності певної групи з метою напрацювання тактичних заходів з розкриття злочинів, затримання злочинців, виявлення ризиків і попередження конкретних правопорушень. Основою кримінальної розвідки виступає аналітична робота з опрацювання кримінально–розвідувальної інформації. У свою чергу, результатом аналітичної роботи є створення аналітичного продукту, що містить

інформацію кримінальної розвідки. На наше переконання, такий підхід забезпечить впровадження в органах Національної поліції України концептуально нової моделі поліцейської діяльності [8].

За твердженням науковців, аналітичною роботою оперативних підрозділів є «інтелектуальна операція з обробки даних, накопичених в інформаційних ресурсах вказаних підрозділів» [3, с. 15]. При цьому, логічний підсумок результатів аналітичного дослідження створюється в електронному або письмовому вигляді, з обов'язковим зазначенням використаних аналітичних інструментів і ґрунтується на основі аналізу інформації [3, с. 16]. Підтримуючи зазначену точку зору, слід наголосити, що у кримінальній розвідці аналітична робота являє собою інтелектуальний процес аналітичної обробки, систематизації, оцінювання, встановлення змісту та сутності первинної інформації, виявлення додатково необхідної інформації, отримання та обґрунтування нових знань, інтерпретації кримінально–розвідувальної інформації, яка має значення для виконання завдань кримінальної розвідки, моделювання, прогнозування та надання пропозицій, спрямований на формування кінцевого аналітичного продукту, що містить узагальнену інформацію кримінальної розвідки. В процесі аналітичної роботи кримінально–розвідувальна інформація перетворюється у інформацію кримінальної розвідки, трансформуючись у декілька етапів: а) первинна кримінально–розвідувальна інформація; б) інформація, отримана в результаті попередньої обробки; в) інформація, отримана в результаті комплексної обробки різнорідних відомостей, що належать до одного об'єкту, взаємна логічна ув'язка та уточнення, аналітичне визначення характеристик об'єкта тощо; г) узагальнена кримінально–розвідувальна інформація, як новий аналітичний продукт [2, с. 37]. Результативність такого процесу, за справедливим твердженням фахівців, багато в чому залежить від комплексності використання наявних аналітичних інструментів та сучасних методик обробки розвідувальної інформації [6, с. 544]. У свою чергу, аналітичний продукт – це результат аналітичного дослідження, складений у письмовій або цифровій формі. На наше переконання, визначення найменування аналітичного продукту (аналітична довідка, аналітичний висновок, аналітичне зведення, довідка–меморандум тощо) має бути єдиним для всіх суб'єктів кримінальної розвідки, а його форма відповідати усім властивостям документа, що передбачені ст. 99 КПК України [4, с. 8; 5].

Принагідно слід наголосити, що кримінальна розвідка, як сучасна форма реалізації правоохоронної функції держави, являє собою синергетичне об'єднання теоретико–праксеологічного надбання та досвіду оперативно–розшукової діяльності з новітніми інструментами, такими, як кримінальний аналіз (стратегічний, операційний, тактичний), стратегічне прогнозування та аналіз ризиків (предикатна аналітика) [1, с. 5]. На наше переконання, реалізуючись шляхом здійснення аналітичної діяльності, кримінально–розвідувальних заходів

та негласного співробітництва, кримінальна розвідка може бути інтегрована у сучасні проактивні моделі поліцейської діяльності, зокрема у модель поліцейської діяльності, орієнтованої на потреби громад (Community Policing, CoP), проблемно–орієнтовану модель (Problem–Oriented Policing), поліцейську діяльність, керовану аналітичною розвідкою (Intelligence–Led Policing), прогностичну модель (Predictive Policing), модель стратегічного управління CompStat, модель запобігання скоєння тяжких злочинів через зосередження роботи поліції в місцях концентрації незначних правопорушень (модель «Broken Windows/Розбитих Вікон» (BWT), модель поліцейської діяльності на основі даних (Data–Driven Policing / Data–Driven Approaches to Crime and Traffic Safety / DDACTS), модель «діяльність поліції у гарячих точках» (Hot Spots Policing), модель «поліцейська діяльність, заснована на доказах» (Evidence–Based Policing – EBP), модель запобігання злочинності «Превенція злочинів за допомогою зміни навколишньої інфраструктури» (Crime Prevention Through Environmental Design – CPTED), цілеспрямованого стримування «перетягування важелів» «Pulling Levers» Focused Deterrence, а також стати системним елементом комплексної (ре– та проактивної) моделі поліцейської діяльності сучасної України.

Перелік використаних джерел:

1.Албул С.В. Аналітична діяльність як складова кримінальної розвідки. Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів: матеріали Всеукраїнської науково–практичної конференції (23 травня 2025 р., м. Одеса). Одеса: ОДУВС. С. 4–7. URL: https://lnk.ua/QZt1eG1E2

2.Албул С.В. Категорії «розвідувальна інформація» та «інформація розвідки» в оперативно–розшуковій діяльності Національної поліції України. Економічна та інформаційна безпека: актуальні питання та інновації: матеріали Міжнародної науково–практичної конференції (м. Дніпро, 04 листопада 2021 р.). Дніпро: ДДУВС, 2021. С. 37–38.

3.Албул С.В. Концептуальні засади становлення кримінальної розвідки в Україні. Аналітично–порівняльне правознавство. 2026. № 1. Частина 3. С. 9–13. DOI: https://doi.org/10.24144/2788–6018.2026.01.3.1

4.Василинчук В.І., Погорецький М.М., Тіхонов С.А. Аналітичний висновок у оперативно–розшуковій діяльності та кримінальному процесі. Вісник кримінального судочинства. 2023. № 1–2. С. 8–18. DOI: https://doi.org/10.17721/2413–5372.2023.1–2/8–18

5.Кримінальний процесуальний кодекс України : закон України від 13.04.2012 № 4651–VI із змін. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/4651–17/print.

6.Маміч В.В., Максименко Ю.А., Шаршаткін Д.Ю., Дідик В.О., Кікоть М.В. Дослідження особливостей обробки розвідувальної інформації. Національні інтереси України. 2026. № 3 (20). С. 536–545. URL: https://surl.lu/jitcje

7.Новий тлумачний словник української мови: у 3 томах; Т. 3 : П–Я./ В. Яременко, О. Сліпушко. Київ: Аконіт, 2008. 862 с.

8.Федчак І.А. Концептуальні основи та науково–практичні аспекти проактивних моделей правоохоронної діяльності : монографія. Львів : ЛьвДУВС, 2024. 628 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/7420

DOI https://doi.org/10.32837/11300.33559

Ващук Олеся
доктор юридичних наук, професор,
дослідник Гданського університету,
м. Гданськ, Республіка Польща
ORCID: https://orcid.org/0000–0003–3161–2870
e–mail: earth.olesia@gmail.com

ПРОБЛЕМИ ДОСТОВІРНОСТІ ФОТО– ТА ВІДЕОДОКАЗІВ ВОЄННИХ ЗЛОЧИНІВ В УМОВАХ РОЗВИТКУ DEEPFAKE–ТЕХНОЛОГІЙ

У тезах досліджено проблеми достовірності фото– та відеодоказів воєнних злочинів в умовах стрімкого розвитку deepfake–технологій та генеративного ШІ. Висвітлено значення цифрових фото– та відеоматеріалів у процесі документування воєнних злочинів, а також проаналізовано основні криміналістичні ризики, пов'язані з можливістю створення AI–генерованого контенту, здатного впливати на достовірність доказової інформації. Запропоновано розглядати системи цифрової автентифікації контенту, криптографічного підтвердження походження файлів та технології захищеного збереження цифрового сліду як перспективні напрями забезпечення достовірності фото– та відеодоказів у кримінальному провадженні щодо воєнних злочинів.

Ключові слова: воєнні злочини, цифрові докази, deepfake, штучний інтелект, криміналістика, верифікація доказів, OSINT, цифрова автентифікація, метадані.

Vashchuk Olesia
Doctor of Law, Professor,
researcher at the University of Gdansk,
Gdansk, Republic of Poland

PROBLEMS OF THE RELIABILITY OF PHOTO AND VIDEO EVIDENCE OF WAR CRIMES IN THE CONTEXT OF THE DEVELOPMENT OF DEEPFAKE TECHNOLOGIES

The theses examine the problems of reliability of photo and video evidence of war crimes in the context of the rapid development of deepfake technologies and generative artificial intelligence. The study highlights the importance of digital photo and video materials in the process of documenting war crimes and analyzes the main forensic risks associated with the creation of AI–generated content capable of affecting the reliability of evidentiary information. The paper proposes considering systems of digital content authentication, cryptographic verification of file origin, and technologies for secure

preservation of digital traces as promising directions for ensuring the reliability of photo and video evidence in criminal proceedings related to war crimes.

Keywords: war crimes, digital evidence, deepfake, artificial intelligence, criminalistics, evidence verification, OSINT, digital authentication, chain of custody, metadata.

В умовах сучасних воєнних злочинів цифрові фото– та відеоматеріали фактично перетворилися на один із ключових видів доказів під час документування саме воєнних злочинів. Значна кількість доказової інформації формується не лише правоохоронними органами, а й цивільним населенням, журналістами, волонтерами, військовими, операторами безпілотних літальних апаратів, супутниковими системами спостереження та учасниками OSINT–спільнот. Тобто цифрові матеріали дозволяють фіксувати наслідки ракетних ударів, місця масових поховань, факти катувань, незаконного утримання осіб, використання заборонених засобів ведення війни, переміщення військової техніки, а також встановлювати часові та географічні параметри подій. У сучасних умовах фото– та відеодокази активно використовуються не лише у межах національних кримінальних проваджень, але й під час діяльності міжнародних слідчих груп, правозахисних організацій, моніторингових місій та Міжнародного кримінального суду.

Разом із тим стрімкий розвиток генеративного ШІ створив принципово нові криміналістичні ризики, пов’язані з можливістю створення deepfake–контенту. Сучасні алгоритми ШІ дозволяють формувати високореалістичні відеозаписи, змінювати зовнішність осіб, імітувати голос, синхронізувати міміку та створювати штучні сцени подій. Особливу небезпеку становить той факт, що окремі deepfake–матеріали можуть бути складними для виявлення без застосування спеціальних технічних засобів аналізу та спеціальних експертних досліджень. У контексті документування воєнних злочинів це створює ризики як штучного формування неправдивих доказів, так і дискредитації автентичних цифрових матеріалів.

Практика сучасних інформаційних конфліктів свідчить про те, що deepfake–технології можуть використовуватися для проведення інформаційно–психологічних операцій, маніпулювання міжнародною громадською думкою, створення фальшивих звернень політичних або військових керівників, а також формування недостовірних матеріалів. Крім того, навіть сама можливість існування deepfake створює додаткові процесуальні ризики, оскільки сторона захисту може ставити під сумнів справжність цифрових доказів, посилаючись на потенційну можливість їх AI–генерації. У результаті формується так званий «ефект недовіри до цифрових доказів», який суттєво ускладнює процес доказування у кримінальних провадженнях щодо воєнних злочинів.

У зв’язку з цим особливого значення набуває вдосконалення криміналістичних методик перевірки автентичності фото– та відеодоказів. На

сучасному етапі одним із ключових напрямів є комплексний аналіз метаданих цифрових файлів, який дозволяє встановлювати час створення матеріалу, характеристики пристрою фіксації, координати місця зйомки, ознаки редагування та зміни структури файлу. Практичне значення має також використання технологій цифрової верифікації, зокрема аналізу піксельних аномалій, світлотіньових співвідношень, артефактів компресії відео, синхронізації аудіодоріжок та особливостей міміки людини, які можуть свідчити про застосування deepfake–технологій.

Окремої уваги потребує використання систем ШІ для виявлення AI–генерованого контенту. На сьогодні вже застосовуються алгоритми, здатні аналізувати окремі технічні невідповідності цифрового контенту, зокрема неприродні рухи очей, дефекти генерації зображення, невідповідності між аудіо– та відеорядом, а також статистичні відхилення у структурі цифрового файлу. Водночас такі технології не можуть розглядатися як безумовний та самодостатній механізм встановлення достовірності доказів, оскільки генеративні моделі ШІ постійно вдосконалюються, а ефективність систем виявлення deepfake залежить від якості алгоритмів, обсягу навчальних даних та методики проведення дослідження.

Науково–практична проблема полягає також у необхідності подальшого розвитку міжнародних стандартів перевірки цифрових доказів у справах про воєнні злочини. На сьогодні вже існують окремі міжнародні підходи до роботи з цифровими відкритими джерелами, зокрема Berkeley Protocol on Digital Open Source Investigations, який визначає основні принципи збору, аналізу, збереження та перевірки цифрової інформації. Однак розвиток deepfake–технологій вимагає подальшої спеціалізації таких підходів щодо виявлення, перевірки та процесуальної оцінки AI–генерованих фото– та відеоматеріалів у кримінальному провадженні.

У зв’язку з цим доцільним є впровадження обов’язкових процедур цифрової автентифікації доказів, які повинні включати перевірку джерела походження матеріалу, аналіз метаданих, встановлення ланцюга збереження цифрового доказу, фіксацію змін файлу та застосування спеціалізованих експертних методик дослідження. Особливого значення набуває також забезпечення належного документування процесу отримання цифрових доказів, оскільки порушення процедури збереження або передачі файлів може негативно впливати на їх допустимість та достовірність у судовому процесі.

Перспективним напрямом протидії фальсифікації цифрових доказів може стати впровадження систем цифрової автентифікації контенту, які дозволятимуть фіксувати цифровий слід створення та модифікації фото– і відеоматеріалів безпосередньо на етапі їх формування. Такі технології можуть передбачати автоматичне збереження захищених метаданих, цифрових підписів, часових міток та інших елементів цифрового сліду, необхідних для подальшої криміналістичної верифікації доказів. Практичне впровадження подібних механізмів у мобільних

пристроях, дронах, камерах відеофіксації та інших засобах створення цифрового контенту могло б суттєво підвищити рівень довіри до цифрових доказів у справах про воєнні злочини.

Додатково перспективним напрямом є використання технологій криптографічного підтвердження походження контенту, blockchain–механізмів, систем цифрового маркування та захищеного збереження метаданих, які дозволятимуть встановлювати історію створення, редагування та передачі цифрових матеріалів. У подальшому це може стати основою для створення міжнародних механізмів цифрової сертифікації доказів у сфері документування воєнних злочинів.

Крім того, практично необхідним є створення спеціалізованих міждисциплінарних груп, до складу яких повинні входити криміналісти, фахівці з кібербезпеки, експерти у сфері ШІ, цифрової аналітики та комп'ютерно–технічних досліджень. Саме комплексний підхід дозволить забезпечити належний рівень перевірки цифрових доказів.

Таким чином, розвиток deepfake–технологій формує принципово новий комплекс криміналістичних та процесуальних викликів у сфері документування воєнних злочинів. За сучасних умов проблема достовірності цифрових доказів виходить за межі виключно технічного питання та набуває важливого міжнародно–правового значення. Ефективна протидія таким загрозам потребує комплексного вдосконалення криміналістичних методик, подальшого розвитку міжнародних стандартів цифрової верифікації, використання спеціалізованих AI–систем виявлення deepfake та формування належного нормативного регулювання використання цифрових доказів у кримінальному провадженні.

DOI https://doi.org/10.32837/11300.33565

Волос Владислав
аспірант кафедри криміналістики, судових експертизи та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса Україна
ORCID: https://orcid.org/0009–0003–6009–0044
e–mail: volosvlad@gmail.com

ОСОБЛИВОСТІ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

Досліджено криміналістичні особливості виявлення та фіксації цифрових слідів під час розслідування злочинів, учинених організованими групами. Визначено значення цифрових слідів як джерела доказової інформації та окреслено проблеми їх процесуального використання.

Ключові слова: цифрові сліди, цифрова криміналістика, організована злочинність, електронні докази, криміналістика.

Volos Vladyslav
Postgraduate student of the Department of Criminalistics,
Forensic Examinations and Polygraphology of the National University
«Odesa Law Academy»,
Odesa, Ukraine

FEATURES OF DETECTION AND RECORDING OF DIGITAL TRACES IN THE INVESTIGATION OF CRIMES COMMITTED BY ORGANIZED GROUPS

The paper examines forensic features of detecting and recording digital traces in investigations of crimes committed by organized groups. The role of digital traces as a source of evidentiary information and problems of their procedural use are analysed.

Keywords: digital traces, digital forensics, organized crime, electronic evidence, criminalistics.

Стрімкий розвиток цифрових технологій істотно вплинув на характер сучасної злочинності. Організовані групи активно використовують електронні комунікації, мережеві сервіси, криптовалютні платформи, засоби анонімізації та шифрування даних для підготовки, координації та приховування злочинної діяльності. За таких умов особливого значення набувають цифрові сліди, які дедалі частіше виступають основним джерелом криміналістично значущої інформації під час розслідування кримінальних правопорушень [1].

Цифрові сліди доцільно розглядати як інформаційні відображення діяльності особи або функціонування технічних систем, що виникають у цифровому середовищі та можуть містити відомості про подію кримінального правопорушення. На відміну від традиційних матеріальних слідів, вони характеризуються нематеріальною природою, значною динамічністю, можливістю багаторазового копіювання та ризиком швидкого знищення або модифікації [2].

Для злочинів, учинених організованими групами, цифрові сліди мають особливу доказову цінність. Вони дозволяють встановлювати структуру злочинного формування, визначати ролі його учасників, відтворювати комунікаційні зв'язки між співучасниками, аналізувати фінансові операції та встановлювати механізм реалізації злочинного задуму. При цьому цифрове середовище формує нову криміналістичну слідову картину, у якій традиційні речові докази поєднуються з електронною інформацією.

Практика свідчить, що найбільш поширеними джерелами цифрових слідів є мобільні телефони, персональні комп'ютери, планшети, серверне обладнання, хмарні сховища даних, акаунти соціальних мереж, месенджери та криптовалютні гаманці. Особливу цінність становлять журнали подій, історія мережевих з'єднань, геолокаційні дані, метадані файлів, листування та інші відомості, які дозволяють реконструювати злочинну діяльність [3].

Однією з ключових проблем є своєчасне виявлення цифрових слідів. Організовані групи все частіше використовують механізми автоматичного видалення інформації, наскрізне шифрування, віддалене блокування пристроїв та інші технології протидії правоохоронній діяльності. У зв'язку з цим під час проведення обшуку чи огляду місця події необхідно забезпечити належне збереження цифрової інформації шляхом мінімізації втручання у функціонування електронних систем та недопущення їх підключення до мережі Інтернет.

Не менш важливим є питання належної фіксації цифрових слідів. Традиційні способи криміналістичної фіксації не завжди забезпечують необхідний рівень збереження електронної інформації. Саме тому у цифровій криміналістиці застосовуються спеціальні методи створення копій носіїв інформації, обчислення контрольних хеш–значень, документування метаданих та використання спеціалізованого програмного забезпечення. Такі дії дозволяють підтвердити цілісність інформації та забезпечити її подальше використання як допустимого доказу у кримінальному провадженні [4].

Важливого значення набуває також питання процесуальної допустимості електронних доказів. Виявлена інформація повинна бути отримана відповідно до вимог кримінального процесуального законодавства, а її походження та автентичність мають бути належним чином підтверджені. Недотримання процесуального порядку вилучення або дослідження цифрових носіїв може поставити під сумнів доказове значення отриманих відомостей [5].

Перспективним напрямом розвитку криміналістичного забезпечення розслідування злочинів, учинених організованими групами, є використання засобів штучного інтелекту та цифрової аналітики. Такі технології дозволяють обробляти значні масиви інформації, виявляти приховані закономірності та встановлювати зв'язки між учасниками злочинної діяльності. Водночас результати автоматизованого аналізу повинні оцінюватися у сукупності з іншими доказами та не можуть підміняти процес доказування.

Таким чином, цифрові сліди стають одним із ключових елементів доказової бази у справах щодо діяльності організованих груп. Їх ефективне використання потребує поєднання традиційних криміналістичних підходів із сучасними технологіями цифрової криміналістики, належного процесуального забезпечення та постійного вдосконалення професійної підготовки суб'єктів розслідування. Подальший розвиток методик роботи з цифровими слідами є важливим напрямом модернізації криміналістики в умовах цифрової трансформації суспільства.

Перелік використаних джерел:

1. Шепітько В. Ю. Криміналістика : підручник. Харків : Право, 2024. 752 с.
2. Коваленко В. В. Інформаційні технології у криміналістичній діяльності: монографія. Київ : Юрінком Інтер, 2022. 248 с.
3. Біленчук П. Д., Удовенко Ж. В. Організована злочинність у цифровому середовищі: криміналістичний аспект. Юридична Україна. 2024. № 5. С. 84–92.
4. Пиріг І. В. Тактика роботи з електронними доказами під час проведення обшуку. Вісник кримінального судочинства. 2024. № 2. С. 95–101.
5. Тертишник В. М. Кримінальний процес України: підручник. Київ : Алерта, 2023. 856 с.
6. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651–VI.

DOI https://doi.org/10.32837/11300.33568

Волошина Владлена
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–8772–4172
e–mail:vkvoloshyna@gmail.com

ПРОЦЕСУАЛЬНИЙ ПОРЯДОК ОТРИМАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОБЛЕМИ ПРАВОЗАСТОСУВАННЯ

У тезах розглянуто процесуальні механізми отримання електронних доказів у кримінальному провадженні. Проаналізовано прогалини КПК України та судову практику. Запропоновано шляхи вдосконалення законодавства.

Ключові слова: електронні докази, кримінальне провадження, тимчасовий доступ, обшук, допустимість, цифрові дані.

Voloshyna Vladlena
Candidate of Legal Sciences, Associate Professor,
Associate Professor of the Department of Criminal Procedure
National University «Odesa Law Academy»,
Odesa, Ukraine

PROCEDURAL ORDER FOR OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: PROBLEMS OF LAW ENFORCEMENT

The theses examine the procedural mechanisms for obtaining electronic evidence in criminal proceedings. The gaps in the Criminal Procedure Code of Ukraine and judicial practice are analyzed. Ways to improve legislation are proposed.

Key words: electronic evidence, criminal proceedings, temporary access, search, admissibility, digital data.

Цифровізація суспільства поставила перед кримінальним процесом питання, на які чинне законодавство відповідає з помітним запізненням. Нині переважна більшість злочинів так чи інакше залишає цифровий слід у месенджерах, хмарних сховищах, банківських додатках, системах геолокації. Однак КПК України, ухвалений у 2012 році, не містить ані визначення поняття «електронний доказ», ані спеціальних процесуальних механізмів, адаптованих до специфіки цифрового середовища. Це й породжує більшість практичних проблем, з якими стикаються слідчі, прокурори та суди.

Відповідно до чинного КПК України, отримання електронних доказів здійснюється в межах загальних процесуальних форм. Основними є: тимчасовий доступ до речей і документів (статті 159–166 КПК), обшук (статті 234–236 КПК), огляд (статті 237–239 КПК), а також негласні слідчі (розшукові) дії зокрема, зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем (статті 263–264 КПК). Кожна з цих форм має свої підстави, порядок і коло суб'єктів, уповноважених їх застосовувати. Проте жодна з них не враховує повною мірою технічних особливостей роботи з цифровими даними [1].

Найбільш поширеним способом отримання електронних доказів на практиці залишається тимчасовий доступ до речей і документів. Разом з тим застосування цього інституту до електронних носіїв інформації викликає низку запитань. Зокрема, КПК не розмежовує доступ до фізичного носія (смартфона, жорсткого диска) та доступ до інформації, яка на ньому міститься. Це суттєво, адже зміст переписки у месенджері та сам телефон принципово різні об'єкти з точки зору права на приватність. Крім того, ухвала слідчого судді про тимчасовий доступ нерідко формулюється надто широко, без конкретизації обсягу даних, що підлягають вилученню, що відкриває можливість для фактично необмеженого втручання у цифрове середовище особи [2].

Окремої уваги заслуговує питання проведення обшуку з метою отримання електронних доказів. Чинне законодавство не передбачає спеціальних правил для обшуку електронних пристроїв, тоді як у низці держав, зокрема США та Великій Британії такі правила давно сформульовані як на нормативному рівні, так і в судовій практиці. В Україні ж нерідко виникають ситуації, коли під час обшуку вилучається вся наявна техніка без належного обґрунтування необхідності такого обсягу вилучення, що прямо суперечить принципу пропорційності [3].

Самостійною і вкрай болючою проблемою є забезпечення цілісності електронних доказів після їх отримання. На відміну від речових доказів традиційного типу, цифрова інформація може бути змінена або знищена непомітно у тому числі внаслідок ненавмисних дій слідчого. Відсутність законодавчо закріпленої процедури створення криміналістичних копій носіїв, фіксації хеш–значень файлів та дотримання ланцюга зберігання доказів (chain of custody) призводить до того, що у суді часто виникають обґрунтовані сумніви у незмінності цифрових матеріалів. Верховний Суд у своїй практиці неодноразово зазначав, що такі сумніви є достатньою підставою для визнання доказів недопустимими [4].

Практика Європейського суду з прав людини формує чіткі орієнтири щодо допустимих меж втручання держави у сферу приватного цифрового простору особи. Зокрема, ЄСПЛ наголошує, що будь–який моніторинг електронних комунікацій повинен мати законну підставу, переслідувати легітимну мету та бути пропорційним їй [5]. Ці стандарти є обов'язковими для України як держави члена Ради Європи, однак їх практична імплементація у вітчизняному кримінальному процесі залишається недостатньою.

Варто також вказати на проблему використання хмарних сервісів. Дані, що зберігаються на серверах іноземних компаній (Google, Apple, Meta тощо), перебувають поза межами безпосередньої юрисдикції України. Їх отримання потребує або міжнародного співробітництва у рамках механізмів правової допомоги, або взаємодії з відповідними платформами через спеціальні процедури. Обидва шляхи є тривалими і нерідко результативними лише частково, що суттєво ускладнює розслідування злочинів, скоєних із використанням цифрового простору.

З огляду на викладене, вбачається кілька першочергових напрямів удосконалення законодавства. По–перше, необхідне нормативне визначення поняття «електронний доказ» та закріплення спеціальних правил його отримання, зберігання й оцінки у КПК України. По–друге, доцільно запровадити обов'язкову процедуру криміналістичного копіювання цифрових носіїв з фіксацією хеш–сум та забезпеченням незмінності оригіналу. По–третє, слід розробити відомчі методичні рекомендації для слідчих і прокурорів щодо роботи з різними категоріями цифрових даних. По–четверте, потребує вирішення питання про порядок отримання доказів від іноземних цифрових платформ у рамках чинних міжнародно–правових механізмів.

Підсумовуючи, слід констатувати: прогалина між технологічними реаліями та процесуальним законодавством стає дедалі відчутнішою. Заповнення цієї прогалини не просто питання юридичної техніки, а передумова забезпечення права обвинуваченого на справедливий судовий розгляд та ефективності кримінального судочинства загалом.

Перелік використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651–VI. Відомості Верховної Ради України. 2013. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text

2. Завидняк В. І., Шильнікова А. О. Деякі проблемні питання забезпечення допустимості електронних доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2020. № 6. URL: https://lsej.org.ua/6_2020/56.pdf

3. Авдєєва Г. Цифрові докази у кримінальному провадженні. URL: https://ibn.idsi.md/sites/default/files/imag_file/370–374_5.pdf

4. Узагальнення судової практики Верховного Суду щодо електронних доказів. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

5. Administration of unlawfully obtained evidence in criminal proceedings. European Court of Human Rights. URL: https://ks.echr.coe.int/documents/d/echr–ks/administration–of–unlawfully–obtained–evidence–ukr

DOI https://doi.org/10.32837/11300.33570

Гончарук Владислава
аспірантка кафедри криміналістики, судових експертиз та поліграфології,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0005–0223–7022
e–mail: honcharuk.vladyslava.ihorivna@gmail.com

СОЦІАЛЬНІ МЕРЕЖІ ЯК ДЖЕРЕЛО КРИМІНАЛІСТИЧНИХ СЛІДІВ: ІННОВАЦІЙНІ МЕТОДИ РОЗСЛІДУВАННЯ ТРАФІКІНГУ

У тезах розглянуто особливості використання соціальних мереж як джерела криміналістичних слідів при розслідуванні трафікінгу. Проаналізовано інноваційні методи у виявленні та розслідуванні торгівлі людьми. Акцентовано увагу на ролі штучного інтелекту при ідентифікації жертв та трафікерів, прогнозуванні ризиків та формуванні нових стратегій протидії вербуванню та експлуатації осіб у цифровому середовищі.

Ключові слова: трафікінг, криміналістичний слід, соціальні мережі, розслідування, інноваційні методи, торгівля людьми, протидія експлуатації, штучний інтелект.

Honcharuk Vladyslava
Postgraduate Student of the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

SOCIAL NETWORKS AS A SOURCE OF FORENSIC TRACES: INNOVATIVE METHODS FOR INVESTIGATING TRAFFICKING

The abstracts examine the specifics of using social networks as a source of forensic evidence in trafficking investigations. Innovative methods in the detection and investigation of human trafficking are analyzed. Emphasis is placed on the role of artificial intelligence in identifying victims and traffickers, predicting risks, and developing new strategies to counter the recruitment and exploitation of individuals in the digital environment.

Key words: trafficking, forensic evidence, social networks, investigation, innovative methods, human trafficking, countering exploitation, artificial intelligence.

В умовах цифровізації та розвитку штучного інтелекту соціальні мережі є масштабним інструментом комунікації, який використовують злочинні угруповання для вербування та експлуатації осіб. Цифрове середовище ускладнює виявлення та розслідування трафікінгу, що зумовлює необхідність у

поглибленому вивченні цифрових слідів, впровадженні технологій штучного інтелекту та розробці інноваційних методів розслідування злочинів торгівлі людьми.

Криміналістичними цифровими слідами, джерелом яких є соціальні мережі та які дозволяють ідентифікувати осіб, причетних до трафікінгу, є: сторінки (профілі в соціальних мережах та масенджерах); метадані файлів (дані про час, місце, пристрій, які залишаються при публікаціях та при пересиланні повідомлень); геолокаційні дані (для встановлення місцезнаходження трафікерів та утримуваних жертв); електронні сліди реєстрації (IP–адреси, засоби зв'язку, час створення акаунтів, прив'язка до банківських карток або криптовалютних гаманців); алгоритми взаємодії користувачів (для виявлення потенційно загрозливих акаунтів); повідомлення та інформація, що міститься після знищення даних у месенджерах (інформація, що підлягає відновленню з використанням спеціалізованого криміналістичного обладнання зберігається на серверах, хмарних сховищах, у кеші пристроїв жертв/злочинців).

Враховуючи вищевикладене, за допомогою технологій штучного інтелекту вдається ідентифікувати осіб (до прикладу, з використанням технології Clearview AI) шляхом розпізнавання їх облич та пошуку у соціальних мережах чи інших електронних базах даних [1, с. 358].

Окрім цього, штучний інтелект здатний: ідентифікувати приховані мережі вербувальників, прогнозувати ризики щодо експлуатації осіб за різними ознаками (віком, соціальним станом, рівнем матеріального забезпечення, країною походження тощо); формувати психологічний портрет трафікерів за ключовими психологічними, інтелектуальними й поведінковими характеристиками для завчасного виявлення дій торговців людьми.

Проте, слід зауважити, що з розвитком цифровізації існують реальні загрози та ризики зловживання штучним інтелектом та використання інформаційних технологій у організованій злочинній діяльності. Зокрема, злочинні угруповання використовують генеративні моделі для створення недостовірних інформаційних матеріалів (deepfakes) з метою психологічного та маніпулятивного тиску, використовуючи неправдиві пропозиції працевлаштування та вдаване сприяння в допомозі [2, с. 2].

Наразі інноваційними методами у виявленні та розслідуванні торгівлі людьми можуть слугувати:

Впровадження OSINT – інструментів (Open source intelligence). Використання спеціального програмного забезпечення надає можливість відслідковувати типові для вербування потенційних жертв оголошення з пошуку роботи, знайомств, надання послуг або соціальної допомоги при складних життєвих обставинах тощо. Розвідка на основі відкритих джерел (OSINT) дає змову виявляти фейкові профілі вербувальників та блокувати їх до встановлення безпосереднього контакту з жертвами.

Поширення алгоритмів розпізнавання. Застосування штучного інтелекту для розпізнавання осіб та порівняння їх з даними зниклих осіб, які піддавалися експлуатації слугує аналізу соціальних мереж та відстеженню поведінкових характеристик і стратегій маніпуляцій, які використовують вербувальники для заволодіння довірою жертв.

Цифрова криміналістика (Digital Forensics). Використання інноваційного комплексу відібрання криміналістичних даних (до прикладу, програмного забезпечення Cellebrite) сприяє аналізу даних з хмарних сховищ, дослідженню зашифрованих чатів, відновленню видалених файлів (EnCase, FTK Imager) та журналів дзвінків з вилучених технічних приладів [3, с.48].

Створення цифрових платформ та чат–ботів. Глобальні технологічні платформи застосовують власні інструменти для виявлення матеріалів про сексуальну та трудову експлуатацію. Створення спеціалізованих гарячих ліній та чат–ботів дозволить жертвам оперативно та безпечно передавати правоохоронним органам інформацію про випадки трафікінгу [4]. Нейромережі здатні сканувати інформаційне наповнення соціальних мереж та розпізнавати сліди експлуатації, приховані метадані зображень й, таким чином, зіставляти обличчя з базами даних зниклих безвісти або розшукуваних осіб.

Впровадження технологій NLP (синтез природної мови) та GNN (графові нейронні мережі). Штучний інтелект здатний розпізнавати приховані ознаки: коди, специфічні скорочення, закономірні помилки у типових повідомленням й дописах в соціальних мережах, зокрема з пропозиціями роботи або інтернет–знайомств. Графовий аналіз дозволяє виявляти зв’язки між пов’язанними IP–адресами, акаунтами та дописами, якщо трафікер публікує оголошення у різних соціальних мережах з різних акаунтів, але з прив’язкою до одного ж засобу зв’язку або електронного гаманця.

З огляду на вищевикладене, сучасна цифрова криміналістика невід’ємно пов’язана з криміналістичними інноваціями. Інтеграція технологій штучного інтелекту у традиційні методи розслідування відкриває нові можливості для дослідження соціальних мереж як джерела криміналістичних слідів у злочинах, пов’язаних з вербуванням та експлуатацією осіб. Отже, соціальні мережі стають простором для збору доказової інформації, а інноваційні методи розслідування з використанням штучного інтелекту – інструментом її відбору, систематизації, побудування алгоритмів та прогнозування ризиків, що сприятиме ефективній протидії сучасним формам трафікінгу.

Перелік використаних джерел:

1.Шевчук, В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. Law, Society, Economy Journal. 2024. № 6. С. 88–96. URL: https://lsej.org. ua/6_2024 /90.pdf

2.S. Lannier, «Using US Artificial Intelligence to Fight Human Trafficking in Europe», 2023, Vol. 18(1), eucrim, pp 67–72. URL: https://eucrim.eu/media/articles/pdf/eucrim–article–2023–002.pdf

3.Василова, О. В. Роль інноваційних технологій у розслідуванні та попередженні злочинів: сучасні виклики. Науковий вісник Чернівецького національного університету імені Ю. Федьковича. Серія: Право. 2025. Вип. 87, № 4. С. 6–12. URL: https://visnyk–juris–uzhnu.com/wp–content/uploads/2025/03/8–3.pdf

4.The Exodus Road. Human Trafficking and Social Media. The Exodus Road. 2024. URL: https://theexodusroad.com/human–trafficking–and–social–media/

DOI https://doi.org/10.32837/11300.33574

Гребенюк Сергій
заступник завідувача лабораторії трасологічних, дактилоскопічних досліджень та обліку Державного науково–дослідного експертно–криміналістичного центру МВС України, м. Одеса, Україна
ORCID: https://orcid.org/0009–0002–8040–6774
e–mail: HrebenyukSM@dndekc.mvs.gov.ua

Кушніренко Наталія
завідувач відділу дактилоскопічних досліджень лабораторії трасологічних, дактилоскопічних досліджень та обліку Державного науково–дослідного експертно–криміналістичного центру МВС України, м. Одеса, Україна
e–mail: nneki@navs.edu.ua

СУДОВО–ДАКТИЛОСКОПІЧНА ІДЕНТИФІКАЦІЯ НЕВПІЗНАНИХ ТРУПІВ ТА ЇХ ОСТАНКІВ ЗА ЦИФРОВИМИ ЗОБРАЖЕННЯМИ ВІДБИТКІВ ПАЛЬЦІВ РУК ІЗ БІОМЕТРИЧНИХ ДОКУМЕНТІВ

У статті досліджено можливості судової дактилоскопічної експертизи при ідентифікації тіл (останків) невпізнаних трупів, за зображеннями відбитків пальців рук, що містяться на електронних носіях біометричних документів. Розглянуто особливості використання дактилоскопічних даних (відцифрованих зображень дактилоскопічних карт та відбитків пальців рук) у процесі встановлення особи невпізнаного трупу, переваги цифрових біометричних технологій, а також проблемні питання отримання, зчитування та дослідження дактилоскопічної інформації з безконтактних електронних носіїв.

Ключові слова: судова дактилоскопія, дактилоскопічна експертиза, біометричний документ, електронний носій, відбитки пальців рук, ідентифікація особи, папілярні узори, воєнний стан, криміналістика.

Hrebeniuk Serhii
Deputy Head of the Laboratory of Traceological and Dactyloscopic Research and Records of the State Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine, Kyiv, Ukraine

Kushnirenko Nataliia
Head of the Fingerprint Examination Department of the Laboratory of Traceological and Dactyloscopic

Research and Records of the State Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine, Kyiv, Ukraine

FORENSIC FINGERPRINT IDENTIFICATION OF UNIDENTIFIED CORPSES AND THEIR REMAINS USING DIGITAL IMAGES OF FINGERPRINTS FROM BIOMETRIC DOCUMENTS

The article examines the capabilities of forensic fingerprint examination in the identification of bodies (remains) of unidentified corpses using digital images of fingerprints stored on electronic media of biometric documents. The study considers the specific features of using fingerprint data (digitized images of fingerprint cards and fingerprints) in the process of establishing the identity of an unidentified corpse, the advantages of digital biometric technologies, as well as problematic issues related to obtaining, reading, and examining fingerprint information from contactless electronic media.

Key words: forensic dactyloscopy, fingerprint examination, biometric document, electronic media, fingerprints, personal identification, papillary patterns, martial law, criminalistics.

Повномасштабна збройна агресія російської федерації проти України призвела до значної кількості людських жертв, певну частину яких становлять невпізнані тіла та фрагментовані останки загиблих осіб. За таких умов особливої актуальності набуває питання оперативної, достовірної ідентифікації загиблих осіб. Встановлення особи загиблого має важливе кримінально–процесуальне, гуманітарне та соціальне значення, оскільки забезпечує реалізацію прав родичів, сприяє документуванню воєнних злочинів та веденню офіційного обліку жертв збройного конфлікту.

Одним із ефективних засобів встановлення особи є судова дактилоскопічна експертиза. Особливого значення в сучасних умовах набуває використання дактилоскопічних даних, що зберігаються на електронних носіях біометричних документів, зокрема паспортів громадянина України у формі ID–картки, паспортів громадянина України для виїзду за кордон, посвідок на проживання та інших документів, які містять безконтактний електронний носій.

Цифровізація біометричної інформації значно розширила можливості криміналістичної ідентифікації, оскільки дозволяє використовувати електронні зображення відбитків пальців рук як порівняльний матеріал у судово–експертній діяльності.

Сучасні біометричні документи містять електронний носій, на якому зберігаються персональні та біометричні дані особи, у тому числі відцифровані відбитки пальців рук особи (вказівних пальців рук особи, а у разі відсутності

можливості парні відбитки інших пальців рук або два будь–які відбитки пальців руки).

Відцифровані відбитки пальців рук особи вносяться до безконтактного електронного носія таких документів: паспорта громадянина України для виїзду за кордон, дипломатичного паспорта України, службового паспорта України, посвідчення особи моряка, посвідчення члена екіпажу, посвідчення особи без громадянства для виїзду за кордон, посвідки на постійне проживання, посвідки на тимчасове проживання, посвідчення біженця, проїзного документа біженця, посвідчення особи, яка потребує додаткового захисту, проїзного документа особи, якій надано додатковий захист, картки мігранта); а також за згодою особи – паспорта громадянина України.

Такі дані формуються під час оформлення відповідних документів із використанням спеціалізованих дактилоскопічних сканерів. Отриманні з використання даних спеціалізованих приладів зображення відбитків пальців рук як правило відповідають вимогам щодо їх якості й придатності для проведення порівняльних дактилоскопічних досліджень.

Об’єктами судової дактилоскопічної експертизи у таких випадках можуть виступати:

цифрові зображення відбитків пальців рук, що містяться на безконтактному електронному носії біометричного документа;

відбитки/відтиски пальців рук (дактилоскопічні карти), отримані шляхом дактилоскопіювання тіл, невпізнаних трупів або їх останків.

Використання зображень відбитків пальців рук з електронних носіїв біометричних документів у судовій дактилоскопічній експертизі дозволяє:

встановлювати особу невпізнаних тіл та останків;

підтверджувати належність біометричного документа конкретній особі;

ідентифікувати особу навіть за відсутності паперових дактилокарт.

Специфіка такого дослідження полягає у необхідності використання спеціального програмного та технічного забезпечення для зчитування інформації з електронного носія біометричних документів.

Використання зображень відбитків пальців рук з електронних носіїв біометричних документів у кримінальному провадженні повинно здійснюватися для конкретних і законних цілей, визначених за згодою суб’єкта даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством, з дотриманням вимог кримінального процесуального законодавства, законодавства про захист персональних даних, нормативних актів, що регламентують функціонування Єдиного демографічного реєстру та норм етичного використання.

Для забезпечення допустимості та належності доказів важливе значення мають:

належна процесуальна фіксація отримання біометричних даних;

забезпечення цілісності електронної інформації;

документування процедури зчитування даних;

використання сертифікованого обладнання та програмного забезпечення;

забезпечення можливості перевірки достовірності цифрових файлів.

При використані цифрових біометричних даних, на практиці виникає низка проблемних питань.

До основних із них належать:

пошкодження або відсутність біометричного документа у загиблої (померлої) особи;

обмежений доступ до електронних носіїв та реєстрів (отримання біометричної інформації потребує дотримання встановлених процедур доступу до персональних даних та використання спеціалізованого обладнання);

необхідність належного технічного забезпечення (необхідність в забезпечені спеціалізованим програмними комплексами та засобами зчитування електронних носіїв);

низька якість відбитків (через значні посмертні зміни іноді неможливо отримати придатні для порівняння відбитки пальців рук);

фрагментарність об’єктів дослідження (в окремих випадках вибухової травми або сильного термічного впливу зберігатися лише окремі ділянки папілярних узорів).

У зв’язку з цим актуальним є подальше вдосконалення нормативно–правового регулювання використання цифрової біометричної інформації у судово–експертній діяльності, включаючи питання конфіденційності, захисту даних та етичних аспектів.

Судова дактилоскопічна експертиза із використанням зображень відбитків пальців рук, що зберігаються на електронних носіях біометричних документів, є одним із перспективних напрямів ідентифікації тіл (останків) невпізнаних трупів (у тому числі військовослужбовців загиблих унаслідок збройної агресії російської федерації проти України).

Використання цифрових біометричних даних забезпечує достовірність ідентифікації, оперативність проведення експертних досліджень та можливість інтеграції з автоматизованими ідентифікаційними системами. Класичні та сучасні методи дактилоскопії дають змогу отримувати придатні для порівняння дактилоскопічні ознаки й здійснювати встановлення особи померлого (загиблого) навіть за наявності значних посмертних змін.

Перспективним напрямом є більш детальне дослідження та, за умови підтвердження ефективності, впровадження в експертну практику систем обробки біометричних даних, які б забезпечували «реконструкцію» втраченого папілярного узору у цифрових зображеннях відбитків невпізнаних трупів. Йдеться про повне або часткове відновлення зображення папілярного узору на основі фрагментарно збережених, слабовиражених чи пошкоджених ділянок шкірних покривів.

Застосування сучасних технологій для покращення якості зображення відбитків, видалення фонових шумів та візуалізації невидимих чи маловидимих деталей, значно підвищило б якість ідентифікаційної інформації.

Дослідження та комплексне поєднання окремих ознак папілярних узорів (пор, країв папілярних ліній, деталей їх будови) дозволило б відтворювати цілісну структуру узору, створювати його «віртуальну модель» (зокрема шляхом 3D–реконструкції) та використовувати її для проведення експертних досліджень і встановлення особи невпізнаного трупа. Такий підхід ґрунтувався б на фундаментальних властивостях папілярних узорів – індивідуальності, незмінності та відновлюваності – і міг би стати надійним засобом ідентифікації тіл (останків) невпізнаних осіб.

Перелік використаних джерел:

1. Конституція України: Закон України від 28.06.1996 № 254к/96–ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: rada.gov.ua
2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651–VI : станом на 2026 р. // Відомості Верховної Ради України. – 2013. – № 9–10, № 11–12, № 13. – Ст. 88. – URL: rada.gov.ua
3. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341–III // Відомості Верховної Ради України. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341–14
4. Про захист персональних даних : Закон України від 01.06.2010 № 2297–VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481. – URL: rada.gov.ua
5. Про захист інформації в інформаційно–комунікаційних системах : Закон України від 05.07.1994 № 80/94–ВР : станом на 2026 р. // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286. – URL: https://zakon.rada.gov.ua/go/80/94–вр
6. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20 лист. 2012 р. № 5492–VI. Відомості Верховної Ради України. 2013. № 51. Ст. 716. (Офіц. вид.)
7. Про затвердження Порядку отримання, вилучення з Єдиного державного демографічного реєстру та знищення відцифрованих відбитків пальців рук особи : Постанова Кабінету Міністрів України від 26 листоп. 2014 р. № 669. Офіційний вісник України. 2014. № 97. С. 2780. URL: https://zakon.rada.gov.ua/laws/show/669–2014–п
8. Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних від 08.01.2014. Уповноважений Верховної Ради України з прав людини. URL: https://zakon.rada.gov.ua/laws/show/n0003715–14#Text

9. Методика дактилоскопічних досліджень / [Кузнєцов В. А., Кушніренко Н. В., Щавелєв А. В., Димитрова Ю. В.]. Київ : ДНДЕКЦ МВС України, 2023. 53 с.

DOI https://doi.org/10.32837/11300.33599

Гриневич Вікторія
в.о. директора Центру поліграфологічних досліджень та тестування,
асистент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0001–2347–5629
e–mail: vkgrem@gmail.com

МІЖ ЕФЕКТИВНІСТЮ ТА ВЕРХОВЕНСТВОМ ПРАВА: ПРАВОВІ Й ЕТИЧНІ МЕЖІ ЗАСТОСУВАННЯ НЕТРАДИЦІЙНИХ МЕТОДІВ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

У роботі досліджено правові та етичні межі застосування нетрадиційних методів у діяльності правоохоронних органів в умовах активного розвитку криміналістичних технологій, штучного інтелекту, алгоритмічного профілювання та біометричної ідентифікації. Особливу увагу приділено проблемі відсутності належного нормативного врегулювання таких методів, як психофізіологічні дослідження із застосуванням поліграфа, одорологічна ідентифікація, предиктивне поліцейське патрулювання, розпізнавання облич у публічному просторі та окремі спеціальні техніки допиту.

Ключові слова: нетрадиційні методи, правоохоронні органи, допустимість доказів, верховенство права, штучний інтелект, поліграф, предиктивна поліцейська діяльність, права людини

Hrynevych Viktoria
Acting Director of the Center for Polygraph Research and Testing,
Assistant Professor of the Department of Criminalistics,
Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

BETWEEN EFFICIENCY AND THE RULE OF LAW: LEGAL AND ETHICAL LIMITS OF THE APPLICATION OF NON–TRADITIONAL METHODS IN LAW ENFORCEMENT ACTIVITIES

The paper examines the legal and ethical limits of applying non–traditional methods in law enforcement activities in the context of the rapid development of forensic technologies, artificial intelligence, algorithmic profiling and biometric identification. Particular attention is paid to the problem of insufficient legal regulation of such methods as psychophysiological examinations using a polygraph, odorological identification, predictive policing, facial recognition in public spaces and certain special interrogation techniques.

Key words: non–traditional methods, law enforcement agencies, admissibility of evidence, rule of law, artificial intelligence, polygraph, predictive policing, human rights.

Розвиток криміналістичних технологій та поширення систем штучного інтелекту у сфері публічної безпеки ставлять перед правовою наукою питання, яке залишається без системної відповіді: де проходить межа між допустимим поліцейським інструментарієм та порушенням гарантованих прав особи? Поліграфологічні дослідження, алгоритмічне профілювання, технології дистанційної біометричної ідентифікації усе це вже є частиною правоохоронної практики, однак відповідного законодавчого врегулювання вони так і не отримали. Мета цієї роботи – визначити концептуальні правові й етичні межі застосування нетрадиційних методів через аналіз чинного законодавства, судової практики та теоретичних напрацювань вітчизняної науки.

Нетрадиційні методи у правоохоронній діяльності охоплюють засоби отримання криміналістично значущої інформації, які або не мають прямого нормативного закріплення в процесуальному законодавстві, або перебувають у зоні правової невизначеності з точки зору допустимості одержаних таким чином результатів. До цієї категорії відносять психофізіологічні дослідження із застосуванням поліграфа, одорологічну ідентифікацію, предиктивне профілювання на основі алгоритмів, системи розпізнавання облич у публічному просторі, а також деякі спеціальні техніки допиту. Проблема полягає не в самому факті існування цих методів, а в тому, що правоохоронці вдаються до них у практичній діяльності за відсутності чітких процесуальних гарантій для осіб, яких вони стосуються. Спостерігається характерна розбіжність: той самий метод може бути інституційно дозволеним для оперативного чи кадрового використання і водночас позбавленим доказової сили в суді. Це не лише правова, а й етична проблема, оскільки особа не завжди може ефективно захиститися від наслідків застосування такого методу, навіть якщо його результати офіційно не долучені до справи. Запровадження нетрадиційних методів потребує диференційованого нормативного підходу – не загальної заборони і не безумовного дозволу, а системи правових стандартів, побудованих на принципах пропорційності, судового контролю та добровільної згоди особи.

Чинний Кримінальний процесуальний кодекс України у ст. 94 закріплює критерії оцінки доказів – належність, допустимість, достовірність і достатність, – однак не визначає процесуального статусу жодного з нетрадиційних методів. Ця прогалина призвела до формування судової практики, яка фактично взяла на себе регуляторну функцію. Зокрема, Касаційний кримінальний суд Верховного Суду у постанові від 26 січня 2023 року у справі № 183/3452/19 констатував, що «чинним законодавством не передбачено застосування поліграфа для перевірки показань свідків, потерпілих та обвинувачених чи підозрюваних та використання

отриманих даних після такої перевірки як доказу» [1]. Водночас Кабінет Міністрів України своєю постановою № 449 від 11 травня 2017 року затвердив Порядок проведення психофізіологічного дослідження із застосуванням поліграфа у Державному бюро розслідувань [2], що свідчить про визнання методу на рівні виконавчої влади за повної відсутності відповідних норм у процесуальному законодавстві. Описана суперечність є показовою: держава одночасно інституціоналізує метод і відмовляється надавати йому доказову силу. Дослідники В.М. Шевчук та С. Матулєне справедливо вказують, що відсутність нормативної визначеності щодо нових технологій у правоохоронній діяльності є системною проблемою, а не окремим казусом, і потребує законодавчого врегулювання з урахуванням міжнародних стандартів захисту прав людини [3].

Питання стає ще більш актуальним з огляду на євроінтеграційний курс України: Регламент ЄС 2024/1689 (Акт про штучний інтелект) відносить системи дистанційної біометричної ідентифікації, що використовуються в режимі реального часу у публічних місцях для цілей правоохоронної діяльності, до категорії неприйнятного ризику та допускає їх використання лише у суворо визначених виняткових випадках [4]. Цей підхід прямо суперечить практиці низки українських міст, де системи відеоаналітики з функцією розпізнавання облич вже функціонують у тестовому або повноцінному режимі, однак правові підстави та обмеження їх застосування законодавчо не визначені. Ілюстративним є й досвід предиктивного поліцейського патрулювання: І.А. Федчак у своєму дисертаційному дослідженні детально аналізує проактивні моделі правоохоронної діяльності та доводить, що алгоритмічне прогнозування кримінальної активності може суттєво підвищити ефективність роботи поліції, проте за умови, що його запровадження супроводжується чіткими правовими обмеженнями, незалежним аудитом і механізмами оскарження для осіб, що підпадають під профілювання [5]. Відсутність таких механізмів в Україні означає, що нетрадиційні методи де–факто застосовуються поза будь–яким правовим контролем – що є неприйнятним як з точки зору верховенства права, так і з позиції відповідності зобов’язанням у сфері прав людини.

Аналіз стану правового регулювання нетрадиційних методів у діяльності правоохоронних органів України дає підстави стверджувати про наявність системного розриву між технологічними можливостями правоохоронних органів та нормативно–процесуальним забезпеченням їх реалізації. Цей розрив не є нейтральним: він створює реальні ризики для прав особи і підриває довіру до інститутів правосуддя. Подолання окреслених проблем потребує внесення змін до КПК України в частині визначення процесуального статусу нових криміналістичних методів, розробки підзаконної нормативної бази щодо умов їх застосування та запровадження інституту незалежного судового контролю. Практична цінність запропонованих підходів полягає в тому, що вони не блокують використання ефективних методів протидії злочинності, а встановлюють для

цього прозорі правові рамки – відповідно до стандартів, що діють у державах – членах ЄС.

Перелік використаних джерел:

1.Назаров О.А. Правові позиції Верховного Суду щодо застосування поліграфа в кримінальному судочинстві в Україні. Судово–психологічна експертиза. Застосування поліграфа та спеціальних знань в юридичній практиці: Електронний журнал. К., 2023. № 3 (23). ISSN 2521–1463. DOI: https://doi.org/10.53672/ej.3.2023.01

2.Постанова Кабінету Міністрів України «Про затвердження Порядку проведення психофізіологічного дослідження із застосуванням поліграфа у Державному бюро розслідувань» від 11 травня 2017 р. № 449. URL: https://www.kmu.gov.ua/npas/250108285

3.Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. Теорія та практика судової експертизи і криміналістики. 2022. Вип. 4 (29). DOI: https://doi.org/10.32353/khrife.4.2022.02

4.Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L, 2024/1689, 12.7.2024. URL: https://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX:32024R1689

5.Федчак І.А. Теорія та практика застосування проактивних моделей правоохоронної діяльності: дис. ... д–ра юрид. наук: 12.00.09 / Львівський державний університет внутрішніх справ. Львів, 2024. 598 с.

DOI https://doi.org/10.32837/11300.33602

Дрига Єлизавета
аспірантка кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0000–0565–3543
e–mail: dryha.l@ukr.net

ВЗАЄМОДІЯ СЛІДЧИХ ТА ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ПІД ЧАС ПРОВЕДЕННЯ ТАКТИЧНИХ ОПЕРАЦІЙ ПРИ РОЗСЛІДУВАННІ НЕЗАКОННОГО ОБІГУ ЗБРОЇ ТА БОЄПРИПАСІВ В УМОВАХ ВОЄННОГО СТАНУ

Досліджено особливості взаємодії слідчих та оперативних підрозділів під час проведення тактичних операцій при розслідуванні незаконного обігу зброї та боєприпасів в умовах воєнного стану, визначено основні форми координації та проблеми практичної реалізації.

Ключові слова: незаконний обіг зброї, воєнний стан, тактичні операції, слідчі, оперативні підрозділи, взаємодія, боєприпаси.

Dryha Yelyzaveta
postgraduate student of the Department of Criminalistics,
Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

COOPERATION BETWEEN INVESTIGATIVE AND OPERATIONAL UNITS DURING TACTICAL OPERATIONS IN THE INVESTIGATION OF THE ILLEGAL TRAFFICKING OF WEAPONS AND AMMUNITION UNDER MARTIAL LAW

This study examines the nature of the interaction between investigative and operational units during tactical operations in the investigation of the illicit trafficking of weapons and ammunition under martial law, and identifies the main forms of coordination and the challenges involved in their practical implementation.

Key words: illegal arms trafficking, martial law, tactical operations, investigators, operational units, coordination, ammunition.

Взаємодія слідчих та оперативних підрозділів під час проведення тактичних операцій при розслідуванні незаконного обігу зброї та боєприпасів в умовах воєнного стану є одним із ключових елементів забезпечення ефективності кримінального провадження, своєчасного документування злочинної діяльності та нейтралізації підвищених безпекових ризиків. В умовах збройної агресії, активних

бойових дій, переміщення значної кількості військової техніки, озброєння та боєприпасів територією держави істотно збільшується ризик потрапляння зброї до незаконного обігу. Частина зброї втрачається під час бойових зіткнень, частина незаконно вивозиться із районів проведення бойових дій, а окремі види озброєння стають предметом діяльності організованих злочинних угруповань. За таких умов традиційні форми розслідування виявляються недостатніми, що зумовлює необхідність проведення комплексних тактичних операцій із широким залученням оперативних можливостей правоохоронних органів.

Особливістю розслідування незаконного обігу зброї та боєприпасів є підвищений рівень латентності таких кримінальних правопорушень, конспіративний характер діяльності злочинців, використання міжрегіональних каналів переміщення зброї, наявність корупційних зв’язків, використання спеціальних засобів зв’язку та високий рівень мобільності учасників злочинної діяльності. У зв’язку з цим ефективне документування таких злочинів практично неможливе без постійної взаємодії між слідчими, оперативними працівниками, спеціальними підрозділами, експертами, аналітичними службами та іншими суб’єктами кримінального провадження. Саме узгодженість дій різних підрозділів забезпечує швидке отримання криміналістично значущої інформації, своєчасне реагування на зміну слідчої ситуації та належне процесуальне оформлення здобутих доказів.

Взаємодія слідчих та оперативних підрозділів у таких провадженнях реалізується у процесуальних та організаційних формах. Процесуальна форма передбачає виконання оперативними підрозділами доручень слідчого або прокурора щодо проведення слідчих та негласних слідчих (розшукових) дій, встановлення місцезнаходження осіб, документування каналів постачання зброї, проведення контролю за вчиненням злочину, оперативних закупок, аудіо– та відеоконтролю, спостереження, встановлення контактів підозрюваних та інших заходів. Організаційна форма взаємодії проявляється у спільному плануванні тактичних операцій, обміні інформацією, координації дій, створенні слідчо–оперативних груп, проведенні оперативних нарад, визначенні сил та засобів, розподілі функцій між учасниками операції.

В умовах воєнного стану значно зростає роль оперативної складової розслідування. Оперативні підрозділи нерідко першими отримують інформацію про незаконне зберігання, переміщення або збут зброї, встановлюють канали її надходження, осіб–посередників, місця схову та логістичні маршрути. Саме тому ефективність розслідування значною мірою залежить від своєчасної передачі такої інформації слідчому та її правильного використання у кримінальному провадженні. Водночас слідчий забезпечує процесуальну легалізацію отриманих відомостей, формує доказову базу та визначає загальну стратегію розслідування.

Однією з найбільш поширених форм взаємодії під час розслідування незаконного обігу зброї є створення слідчо–оперативних груп [1]. До їх складу

можуть входити слідчі, оперативні працівники карного розшуку, підрозділів стратегічних розслідувань, працівники Служби безпеки України, спеціалісти вибухотехнічних служб, криміналісти, кінологи та представники інших підрозділів залежно від характеру слідчої ситуації. Основним завданням такої групи є комплексне забезпечення проведення тактичної операції, швидке реагування на зміну обстановки та забезпечення безпеки учасників провадження.

Особливого значення набуває взаємодія під час проведення тактичних операцій із затримання осіб, причетних до незаконного обігу зброї. Такі операції характеризуються підвищеним рівнем небезпеки, оскільки підозрювані можуть бути озброєними, мати бойовий досвід, використовувати засоби спостереження, контрспостереження або підтримку інших учасників злочинної групи. У зв'язку з цим підготовка до проведення операції повинна включати детальне вивчення особи підозрюваного, встановлення наявності зброї, можливих шляхів відходу, кількості співучасників, системи охорони приміщення, можливості застосування вибухових пристроїв та інших факторів ризику. Оперативні підрозділи здійснюють збір відповідної інформації, тоді як слідчий координує процесуальне забезпечення операції та визначає обсяг доказової інформації, яку необхідно отримати.

Тактичні операції під час розслідування незаконного обігу зброї часто мають комплексний характер та включають одночасне проведення декількох слідчих і негласних слідчих (розшукових) дій. Наприклад, одночасно можуть проводитися обшуки за декількома адресами, затримання підозрюваних, вилучення зброї, блокування каналів зв'язку, накладення арешту на транспортні засоби та документування контактів між учасниками злочинної діяльності. У таких умовах ефективність взаємодії визначається рівнем координації дій, наявністю єдиного плану операції та безперервним інформаційним обміном між усіма учасниками.

Окрему роль у забезпеченні взаємодії відіграє використання сучасних інформаційно–аналітичних систем та цифрових технологій. В умовах воєнного стану злочинці активно використовують месенджери, анонімні акаунти, зашифровані канали зв'язку та електронні платформи для продажу зброї. Це зумовлює необхідність залучення кіберпідрозділів, спеціалістів з цифрової криміналістики та аналітичних центрів. Оперативні працівники здійснюють моніторинг електронних ресурсів, встановлюють IP–адреси, акаунти, маршрути передачі інформації, а слідчі забезпечують належне процесуальне оформлення електронних доказів та їх подальше використання у кримінальному провадженні.

Важливим напрямом взаємодії є проведення контролю за вчиненням злочину під час документування фактів збуту зброї та боєприпасів. Такі тактичні операції передбачають поєднання оперативних заходів із процесуальними рішеннями та потребують високого рівня координації. Оперативні підрозділи забезпечують встановлення контакту із підозрюваними, контрольоване придбання зброї, приховане спостереження, аудіо– та відеофіксацію зустрічей, тоді як

слідчий здійснює процесуальний супровід операції, забезпечує отримання необхідних дозволів та документування результатів. Помилки у взаємодії на цьому етапі можуть призвести до втрати доказів або визнання їх недопустимими.

Суттєве значення має взаємодія під час проведення обшуків та оглядів місць зберігання зброї. Такі слідчі дії нерідко супроводжуються ризиком виявлення вибухонебезпечних предметів, мін, розтяжок або саморобних вибухових пристроїв. Тому до проведення обшуків залучаються вибухотехнічні підрозділи, спеціалісти–криміналісти, кінологи та працівники спеціальних підрозділів. Оперативні працівники забезпечують зовнішнє спостереження, блокування території та встановлення можливих співучасників, тоді як слідчий здійснює безпосереднє керівництво слідчою дією та фіксує її результати.

В умовах воєнного стану важливою проблемою залишається незаконне переміщення зброї через блокпости, гуманітарні коридори, транспортні маршрути та прифронтові території. Це потребує налагодження взаємодії не лише між слідчими та оперативними підрозділами Національної поліції, але й між військовими формуваннями, прикордонною службою, Службою безпеки України та іншими суб'єктами сектору безпеки й оборони. Ефективність такої взаємодії залежить від швидкості обміну інформацією, узгодженості дій та створення спільних інформаційних баз щодо викраденої або втраченої зброї [2].

Проблемним аспектом взаємодії є недостатня узгодженість між процесуальними та оперативними механізмами документування злочинної діяльності. На практиці нерідко виникають ситуації, коли оперативна інформація не отримує своєчасної процесуальної реалізації, або окремі дії проводяться без належної координації зі слідчим. Це може призводити до втрати доказової інформації, розголошення оперативних заходів або зриву тактичної операції. Тому важливого значення набуває спільне планування розслідування, визначення єдиної тактичної концепції та постійний контроль за виконанням поставлених завдань.

Таким чином, взаємодія слідчих та оперативних підрозділів під час проведення тактичних операцій при розслідуванні незаконного обігу зброї та боєприпасів в умовах воєнного стану є складною багаторівневою системою спільної діяльності, спрямованою на своєчасне виявлення, припинення та документування злочинної діяльності. Ефективність такої взаємодії визначається рівнем координації дій, швидкістю обміну інформацією, належним поєднанням процесуальних та оперативних можливостей, використанням сучасних технологій і здатністю правоохоронних органів адаптуватися до динамічних умов воєнного стану. Саме комплексний характер взаємодії забезпечує формування належної доказової бази, підвищення результативності тактичних операцій та мінімізацію ризиків для учасників кримінального провадження і суспільства в цілому.

Перелік використаних джерел:

1. Яковлєв О. Взаємодія слідчого з оперативними підрозділами під час проведення слідчих (розшукових) дій. Науковий часопис Національної академії прокуратури України. 2017. №1. С. 217–224.

2. Свинаренко Ю.П. Шкута О.О. Особливості взаємодії оперативних підрозділів з органами дізнання та досудового слідства. Держава та регіони. Серія: Право, 2024 р., № 1 (83) том 2 С. 42–46.

DOI https://doi.org/10.32837/11300.33604

Завтур Віктор
кандидат юридичних наук, доцент, доцент кафедри кримінального процесу Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–7171–2369
e–mail:vzavtur93@gmail.com

ЦИФРОВИЙ ОБШУК У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ОКРЕМІ ПИТАННЯ НОРМАТИВНОЇ МОДЕЛІ

Тези присвячено окремим питанням розробки перспективної моделі цифрового обшуку у кримінальному процесуальному законодавстві. Наголошено, що вона повинна включати в себе як вичерпне визначення допустимих форм цифрового обшуку, так і необхідність ефективного судового контролю з чітко визначеним предметом перевірки.

Ключові слова: кримінальне провадження, засади кримінального провадження, право на повагу до приватного і сімейного життя, обшук, цифровий обшук.

Zavtur Viktor
Candidate of Science of Law, Associate Professor, Associate Professor of the Department of Criminal Process, National University «Odesa Law Academy», Odesa, Ukraine

DIGITAL SEARCH IN CRIMINAL PROCEEDINGS: SELECTED ISSUES OF THE REGULATORY MODEL

The theses are devoted to certain issues related to the development of a prospective model of digital search within criminal procedure legislation. It is emphasized that such a model should include both a comprehensive definition of its permissible forms and the necessity of effective judicial control with a clearly defined subject matter of review.

Keywords: criminal proceedings, principles of criminal proceedings, right to respect for private and family life, search, digital search.

Стрімка та всеохоплююча діджиталізація суспільних відносин не могла оминути сферу кримінального провадження. Однак, цілком природньо, що науково–технічний прогрес є набагато більш динамічним явищем, ніж законотворча діяльність. Остання характеризується відносною статикою, а відтак пристосування до нових цифрових реалій дедалі частіше відбувається на

правореалізаційному рівні. У зв'язку із цим, у доктрині актуалізується низка нагальних питань, наукове осмислення яких є необхідним задля визначення потенційних напрямків удосконалення чинного кримінального процесуального законодавства.

Одним із таких питань є нормативне забезпечення та практика реалізації цифрового обшуку у кримінальному провадженні. Сьогодні, електронні цифрові пристрої, до яких у широкому контексті можна віднести мобільні телефони, ноутбуки, планшети, хмарні сервіси та інші цифрові носії виступають, без перебільшення, основним джерелом доказів у кримінальних провадженнях. Безумовно, роль цих пристроїв у повсякденному житті будь–якої соціально активної людини настільки істотна, що за їх допомогою можна до найменших дрібниць реконструювати стиль та спосіб її життя.

Одразу слід зауважити, що поняття цифрового обшуку не є нормативно визначеним, втім, воно доволі активно використовується у доктринальному обігу. Під ним, як правило, розуміють процесуальні дії, які пов'язані із доступом до цифрових пристроїв, інформаційних систем, електронних носіїв та цифрових даних з метою відшукання та фіксування відомостей, які можуть мати значення для встановлення фактичних обставин кримінального провадження.

Заради справедливості, необхідно відзначити, що вітчизняний законодавець не оминає увагою цей аспект. Зокрема, у ч.6 ст. 236 КПК України встановлено, що «якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку». Крім того, згадана стаття містить і положення про те, що «особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку».

Чи достатньо цитованих положень кодексу, аби можна було стверджувати про правову визначеність у контексті можливості проведення цифрового обшуку. Наукові праці Н.В. Глинської [1], М.І. Пашковського [2], А.В. Скрипника [3], М.В. Філімонова [4] та інших авторів, у яких піднімаються численні проблемні питання визначення належної правової процедури вилучення цифрових пристроїв та ознайомлення із інформацією, яка міститься на них красномовно свідчать, що ні.

Цілком очевидно, що зі схожими правовими проблемами стикається законодавець й у зарубіжних країнах, а відтак необхідно звернутися до цього досвіду задля того, аби визначити потенційні резерви для вдосконалення положень вітчизняного кримінального процесуального законодавства.

Питання цифрового обшуку доволі детально регламентовано законодавством Сполучених штатів Америки (далі – США). Зокрема, правило 41 (b) Федеральних правил кримінального процесу передбачає низку випадків, коли магістратський суддя, який має юрисдикцію в будь–якому окрузі, де могли мати місце дії, пов'язані із кримінальним правопорушенням, уповноважений видати ордер на здійснення віддаленого доступу з метою обшуку електронних носіїв інформації, а також вилучення чи копіювання електронно збереженої інформації, що знаходиться в межах або поза межами такого округу [5].

На розвиток сучасних уявлень про правомірність цифрового обшуку у США достатньо серйозно вплинув висновок Верховного Суду США у справі «Райлі проти Каліфорнії» (Riley v. California). У цій справі апелянта було зупинено офіцерами поліції через порушення правил дорожнього руху. Згодом під час обшуку автомобіля було виявлено два пістолети під капотом, у зв'язку із чим його було затримано. Офіцер вилучив у нього смартфон з широким спектром функцій, заснованих на передових обчислювальних можливостях, великій ємності пам'яті та підключенні до Інтернету. Так він отримав доступ до інформації, яка міститься на ньому і помітив, що деяким словам (ймовірно, у текстових повідомленнях або списку контактів) передували букви «CK» – ярлик, який, на його думку, означав «Crip Killers», сленговий термін для членів злочинного угрупування Bloods [6].

Суду зрештою належало визначити, чи правомірним був обшук смартфона за наведених обставин.

Що цікаво, у рішенні було окремо відзначено, що саме по собі вилучення телефону може бути правомірним, адже воно переслідує мету запобігання знищенню доказів та забезпечення безпеки офіцерів. Але це не стосується змісту самого телефону, адже інформація, яка міститься на ньому, сама по собі не створює ні для кого загрози.

Представники держави стверджували, що пошук даних у телефоні не відрізняється від фізичного пошуку предметів під час обшуку. Щодо цього доводу, Верховний Суд США іронічно відзначив, що це «приблизно те саме, що стверджувати, що їзда на коні нічим не відрізняється від польоту на Місяць». Сучасний телефон є по своїй суті міні–комп'ютером, адже має одночасно функції і камери, і фотоальбому, і щоденника, і відеопрогравача тощо. Тобто якщо фізичний обшук завжди обмежений певним простором, то цифровий обшук відкриває можливість для необмеженого втручання у приватне життя.

У підсумку, Верховний Суд дійшов висновку, що ознайомлення зі змістом смартфона могло бути здійснено виключно на підставі судового ордера.

У вітчизняній правозастосовній практиці ця ідея натепер не достатньо сприймається. Цю тезу переконливо підтверджує позиція, викладена в ухвалі Апеляційної палати Вищого антикорупційного суду від 06 березня 2023 року: «ухвала слідчого судді про дозвіл на проведення обшуку з метою відшукання речей, у тому числі електронних носіїв інформації, які містять інформацію, що має

суттєве значення для встановлення важливих обставин у кримінальному провадженні, є не тільки дозволом на проникнення у житло чи інше володіння особи, але одночасно може бути і дозволом на втручання в приватне спілкування осіб, оскільки електронні носії інформації можуть містити одночасно і інформацію, дотичну до обставин кримінального провадження, іншу інформацію, неналежну до предмету доказування, в тому числі особистого характеру. Крім того, інформація особистого характеру, у тому числі приватного спілкування, може бути пов`язана із обставинами кримінального провадження, що розслідується. Надання дозволу слідчим суддею, судом на відшукання та вилучення електронних інформаційних систем чи їх частин презюмує необхідність ознайомлення слідчого з їх змістом для визначення належності чи неналежності такої інформації до обставин кримінального провадження» [7].

Така позиція суду фактично призводить до ототожнення фізичного та цифрового обшуку, в той час як останній є значно більш інтрузивним втручанням, що було достатньо переконливо обґрунтовано у рішення «Райлі проти Каліфорнії» Верховним Судом США. Різним є й контекст такого втручання. Якщо під час обшуку житла чи іншого володіння особи мова йде, здебільшого, про втручання у право недоторканості житла та право власності, у разі ознайомлення зі змістом мобільного телефона мова йде про втручання у приватне спілкування. Останнє передбачає необхідність здійснення судового контролю судом апеляційної інстанції та оцінки слідчим суддею винятковості такого заходу (що не охоплюється предметом доказування при розгляді клопотань про обшук).

Утім, чинна редакція ч.6 ст. 236 КПК України фактично надає слідчому, прокурору право здійснити пошук, виявлення та фіксацію комп’ютерних даних, що на них міститься, на місці проведення обшуку як без попереднього, так і без подальшого судового контролю, що є вкрай заниженим стандартом правомірності втручання у право на повагу до приватного життя.

Саме тому, процедури вилучення мобільного телефона та його ознайомлення з його змістом мають бути чітко розмежовані на таких засадах: 1) вилучення комп’ютерних систем або їх частин, мобільних терміналів систем зв’язку можливе лише на підставі ухвали слідчого судді; 2) вилучення без ухвали слідчого судді можливе лише у випадку якщо під безпосередньо під час обшуку виникла загроза знищення, спотворення доказів або небезпека для життя та здоров’я осіб, які беруть участь у відповідній слідчій (розшуковій) дії; 3) подальше ознайомлення з їх змістом повинно підлягати судовому контролю.

Важливою є й сама правова процедура, в межах якої здійснюватиметься ознайомлення зі змістом. А.В. Скрипник слушно зазначає, що повноцінної слідчої (розшукової) дії, яка б регламентувала пошукові дії сторони обвинувачення у цифровому просторі та межі допустимого втручання у сферу прав і свобод людини процесуальний закон не передбачає [3, с. 149]. Хоча, законодавство деяких країн Європи регламентує релевантні правові процедури. Найбільш концептуалізована модель цифрового обшуку передбачена КПК ФРН. Відповідна процесуальна дія

має назву онлайн–обшук (Online–Durchsuchung) і передбачає втручання за допомогою технічних засобів в інформаційно–технічну систему, якою користується така особа, а також отримання даних із неї (ст. 100 b КПК ФРН) [8]. Тобто мова йде фактично про дистанційне втручання у пристрій. Процесуальні дії, які були б максимально еквівалентні онлайн–обшуку за КПК ФРН у кримінальному процесуальному законодавстві України відсутні.

А.В. Скрипник пропонує визначати межі втручання не пристроєм, який дозволяється обшукувати, а цифровою інформацією, на пошук якої спрямований обшук. Автор зазначає, що у даному випадку застосовною є доктрина простого погляду, з якої випливає «право відкрити та дослідити зміст будь–якого файлу (незалежно від назви або формату) доти, доки невідповідність цифрової інформації з нього об'єкту пошуку не стане очевидною» [3, с. 149].

Безумовно, коли пристрій перебуває у володінні сторони обвинувачення, здійснити контроль меж і способу використання інформації, яка міститься на ньому складно. Втім, основна перевага пропонованої моделі полягає у можливості забезпечення допустимості доказів, які будуть отримані у ході такого втручання.

Але, водночас, виникає й інше питання: якщо в ході проведення такого обшуку будуть виявлені відомості, які свідчать про вчинення іншого кримінального правопорушення, чи правомірним буде їх використання у іншому кримінальному провадженні. У випадку проведення негласних слідчих (розшукових) дій, застосовними будуть положення ст. 257 КПК України. Втім, ККС ВС послідовно відстоює позицію про те, що огляд текстових повідомлень вилученого під час обшуку телефону, які в ньому знаходяться та доступ до яких не пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем, не є негласною слідчою (розшуковою) дією [9]. Логіка правозастосовника доволі проста: якщо втручання не здійснюється таємно, то вести мову про проведення негласних слідчих (розшукових) дій недоцільно. Але, відповідно, й гарантії, передбачені ч.1 ст. 257 КПК України щодо відомостей, які будуть отримані за результатами цієї процесуальної дії теж не поширюватимуться.

Це коло проблемних питань можна продовжувати, але й наведене свідчить про те, що нормативне забезпечення правомірності обмеження прав та свобод в ході проведення цифрового обшуку натепер не відповідає актуальному рівню цифровізації, сучасним уявленням про право на повагу до приватного життя та ступеню інтрузивності такого заходу. І хоча він існує де–факто у правозастосовній практиці вже давно, де–юре він лишається «замаскованим» під інші процесуальні дії, які дозволяють нівелювати належні процесуальні гарантії. Саме тому, перспективна модель цифрового обшуку має враховувати як вичерпне визначення його допустимих форм, так і необхідність ефективного судового контролю з чітко визначеним предметом перевірки.

Перелік використаних джерел:

1. Глинська Н.В. Щодо використання цифрової інформації у кримінальному провадженні: окремі аспекти. Використання цифрової інформації в розслідуванні кримінальних правопорушень: матеріали міжнар. наук.–практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Соколенко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. С. 18–21.

2. Пашковський М.І. Про колізійність приписів щодо процесуальної форми доступу до змісту відомостей, що містяться в мобільних терміналах систем зв'язку. Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково–практичного семінару (26 листопада 2021 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2021.С. 108–111.

3. Скрипник А.В. Цифровий обшук: бути чи не бути. Цифровізація кримінального провадження: стан та перспективи: матеріали наук.–практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н.В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України ; від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 148–151.

4. Філімонов М. В. Особливості доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі : дис. … д–ра філос. 081 «Право». Одеса, 2026. 215 с.

5. Federal rules of Criminal Procedure. URL: https://www.uscourts.gov/forms–rules/current–rules–practice–procedure/federal–rules–criminal–procedure

6. Riley v. California, 573 U.S. 373 (2014). Supreme Court of the United States. URL: https://supreme.justia.com/cases/federal/us/573/373/

7. Ухвала Апеляційної палати Вищого антикорупційного суду від 06 березня 2023 року, судова справа № 502/1960/17. URL: https://reyestr.court.gov.ua/Review/109479640

8. Strafprozeßordnung der Bundesrepublik Deutschland (StPO). URL: https://www.gesetze–im–internet.de/stpo/

9. Постанова Верховного Суду від 09 квітня 2020 року, судова справа № 727/6578/17. URL: https://reyestr.court.gov.ua/Review/88749345

DOI https://doi.org/10.32837/11300.33606

Загородній Ігор
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–0923–1887
e–mail: zagorodniyiv@ukr.net

АЛГОРИТМІЗАЦІЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ З МОЖЛИВОСТЯМИ ВИКОРИСТАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ОСНОВА ЕФЕКТИВНОГО РОЗКРИТТЯ ТЯЖКИХ ТА ОСОБЛИВО ТЯЖКИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У тезах досліджуються сучасні підходи до алгоритмізації досудового розслідування як одного з ключових напрямів підвищення ефективності діяльності органів досудового розслідування та прокурора при розкритті тяжких і особливо тяжких кримінальних правопорушень. Обґрунтовується необхідність впровадження структурованих алгоритмів прийняття процесуальних, тактичних і організаційних рішень на початковому та наступних етапах кримінального провадження.

З використанням інформаційних систем та елементів штучного інтелекту в процесі планування слідчих (розшукових) дій, аналізу доказової інформації та координації взаємодії між слідчим, детективом, прокурором і оперативними підрозділами.

Зазначено, що алгоритмізація сприяє стандартизації процесу розслідування, мінімізації процесуальних помилок, скороченню часу прийняття рішень, забезпеченню належного рівня доказування та підвищенню якості документування кримінальних правопорушень.

Робиться висновок, що створення та впровадження автоматизованих моделей підтримки досудового розслідування є перспективним напрямом розвитку криміналістики майбутнього та важливим елементом модернізації системи кримінальної юстиції України в умовах цифрової трансформації.

Ключові слова: алгоритмізація розслідування, досудове розслідування, криміналістика, автоматизоване робоче місце слідчого, цифрові технології, штучний інтелект, кримінальне провадження, доказування.

Zahorodnii Ihor
Candidate of Legal Sciences, Associate Professor,
Associate Professor at the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»
Odesa, Ukraine

ALGORITHMIZATION OF PRE–TRIAL INVESTIGATION WITH THE POSSIBILITY OF USING ELEMENTS OF ARTIFICIAL INTELLIGENCE AS A BASIS FOR THE EFFECTIVE DETECTION OF SERIOUS AND ESPECIALLY SERIOUS CRIMINAL OFFENCES

The theses examine modern approaches to the algorithmization of pre–trial investigation as one of the key areas for improving the effectiveness of pre–trial investigation bodies and prosecutors in detecting serious and especially serious criminal offences. The necessity of introducing structured algorithms for making procedural, tactical and organizational decisions at the initial and subsequent stages of criminal proceedings is substantiated.

Particular attention is paid to the possibilities of using information systems and elements of artificial intelligence in the process of planning investigative search actions, analyzing evidentiary information, identifying priority investigative versions, systematizing criminal proceedings materials and coordinating interaction between the investigator, detective, prosecutor and operational units. It is emphasized that digital tools can provide analytical support for decision–making; however, they should not replace the procedural independence of authorized subjects of criminal proceedings.

It is noted that algorithmization contributes to the standardization of the investigation process, minimization of procedural errors, reduction of decision–making time, ensuring an appropriate level of proving and improving the quality of documentation of criminal offences. The conclusion is drawn that the creation and implementation of automated models for supporting pre–trial investigation is a promising direction for the development of criminalistics of the future and an important element in the modernization of Ukraine's criminal justice system under conditions of digital transformation.

Key words: algorithmization of investigation, pre–trial investigation, criminalistics, automated workplace of an investigator, digital technologies, artificial intelligence, criminal proceedings, proving.

У сучасних умовах розвитку кримінальної юстиції України особливого значення набуває впровадження алгоритмізованих моделей організації досудового розслідування.

Зростання рівня організованої злочинності, використання злочинцями цифрових технологій, мобільного зв'язку, електронних платіжних систем та засобів конспірації потребує від правоохоронних органів нових підходів до організації слідчої діяльності.

Одним із найбільш перспективних напрямів удосконалення криміналістичного забезпечення досудового розслідування є алгоритмізація діяльності слідчого, детектива та прокурора, яка дозволяє забезпечити системність, послідовність та процесуальну правильність прийняття рішень на всіх стадіях кримінального провадження.

Особливої актуальності алгоритмізація набуває саме на початковому етапі розслідування тяжких та особливо тяжких злочинів, коли від швидкості, повноти та узгодженості дій залежить можливість:

- своєчасного виявлення та фіксації слідів кримінального правопорушення; встановлення механізму події;
- визначення напрямків пошуку злочинця;
- недопущення втрати доказової інформації;
- організації переслідування «по гарячих слідах»;
- формування належної доказової бази.

У зв'язку з цим алгоритмізація досудового розслідування повинна базуватись на чіткій системі взаємодії:

1. слідчого;
2. оперативних працівників;
3. спеціаліста–криміналіста;
4. судового експерта;
5. прокурора як процесуального керівника.

Саме міжвідомча та міжфункціональна координація дозволяє забезпечити комплексний підхід до документування злочину та оперативного отримання доказової інформації.

Особливе значення має алгоритмізований огляд місця події як ключова процесуальна дія початкового етапу розслідування. Саме якісний огляд забезпечує отримання первинної доказової інформації, виявлення матеріальних та цифрових слідів, визначення способу вчинення злочину, ознак інсценування, механізму приховування слідів та інших криміналістично значущих обставин.

Перспективним напрямом розвитку алгоритмізації є інтеграція елементів штучного інтелекту та криміналістичної аналітики у діяльність правоохоронних органів. Використання цифрових платформ дозволяє автоматизувати підготовку процесуальних документів, аналіз слідчих ситуацій, контроль виконання завдань та прогнозування напрямків розслідування.

Таким чином, алгоритмізація досудового розслідування виступає не лише інструментом оптимізації роботи слідчого, але є важливим елементом сучасного криміналістичного забезпечення боротьби з тяжкими та особливо тяжкими

злочинами. Її впровадження сприяє підвищенню ефективності взаємодії між слідчим, експертом та оперативними підрозділами, забезпечує процесуальну дисципліну, зменшує ризик помилок та підвищує результативність розкриття кримінальних правопорушень.

Практичні аспекти алгоритмізації початкового етапу досудового розслідування

Важливою складовою алгоритмізації досудового розслідування є використання стандартизованих електронних шаблонів процесуальних документів, які забезпечують: процесуальну правильність оформлення; скорочення часу підготовки документів; мінімізацію технічних помилок; уніфікацію слідчої практики; контроль повноти фіксації доказової інформації.

Використання автоматизованих форм документів у спеціалізованих інформаційних системах дозволяє забезпечити єдині стандарти документування та покращити процесуальний контроль з боку прокурора.

Сучасна криміналістика потребує активного впровадження цифрових технологій під час огляду місця події, особливо в умовах воєнного стану та розслідування масштабних злочинів.

Особливого значення набуває застосування:

- цифрової фото– та відеофіксації високої роздільної здатності;
- 3D–сканування місця події;
- геопросторової фіксації координат доказів;
- мобільних криміналістичних лабораторій;
- бодікамер слідчих та оперативних працівників;
- систем автоматичного збереження цифрових даних;
- безпілотних літальних апаратів (дронів).

Застосування дронів є особливо ефективним:

- під час огляду територій після ракетних ударів; документування наслідків бойових дій;
- огляду великих площ руйнувань;
- виявлення вибухонебезпечних предметів;
- пошуку слідів переміщення техніки;
- фіксації масових поховань;
- побудови цифрових моделей місця події.

Такі технології дозволяють забезпечити безпеку учасників слідчої дії, оперативність збору доказів та збереження обстановки місця події у цифровому форматі.

У сучасних умовах розвитку криміналістики та цифровізації кримінального провадження технології штучного інтелекту можуть виступати ефективним допоміжним інструментом для слідчого, детектива, прокурора, науковця та викладача юридичних дисциплін.

Практичне застосування ШІ є особливо актуальним під час:

- алгоритмізації слідчих (розшукових) дій;

- аналізу типових слідчих ситуацій;
- формування криміналістичних версій;
- підготовки методичних рекомендацій;
- створення уніфікованих шаблонів процесуальних документів;
- моделювання початкового етапу розслідування;
- систематизації криміналістичної інформації;
- підготовки навчальних матеріалів та наукових досліджень.

Особливу ефективність використання ШІ демонструє під час дослідження інсценувань самогубства, умисних вбивств із застосуванням вогнепальної зброї; приховування слідів злочину, організації огляду місця події та координації взаємодії слідчого, експерта та оперативних працівників.

Водночас ключовим елементом ефективної роботи зі штучним інтелектом є професійно сформульоване питання (запит). Саме якість, логічність та криміналістична грамотність поставленого завдання визначають рівень отриманого результату.

Штучний інтелект не замінює професійне мислення слідчого чи науковця, а систематизує інформацію, дозволяє аналізувати великі масиви даних, структурує нормативний та методичний матеріал, пропонує алгоритми дій, формує логічні моделі розслідування, допомагає виявляти взаємозв’язки між доказами та прискорює підготовку процесуальних і аналітичних документів.

Таким чином, штучний інтелект у криміналістиці слід розглядати як сучасний інструмент інтелектуальної підтримки діяльності правоохоронних органів.

Головною перевагою використання ШІ є можливість поєднання професійного досвіду слідчого або науковця з високою швидкістю аналітичної обробки інформації, що сприяє підвищенню ефективності розслідування тяжких та особливо тяжких злочинів.

Основна межа – ШІ не може замінити процесуальне рішення людини, адже штучний інтелект є допоміжним аналітичним інструментом, але: не є суб’єктом кримінального провадження; не має процесуального статусу; не несе юридичної відповідальності; не може оцінювати докази за внутрішнім переконанням у розумінні КПК України; не може приймати остаточні процесуальні рішення.

Кінцеве рішення завжди залишається за слідчим, детективом, прокурором, слідчим суддею чи судом.

Надмірне використання штучного інтелекту у кримінальному провадженні може спричинити низку суттєвих ризиків. Насамперед існує небезпека втрати професійного мислення слідчого, оскільки постійне покладання на алгоритми здатне формувати шаблонний підхід до розслідування. У таких умовах знижується рівень криміналістичної інтуїції, аналітичного мислення та уваги до нетипових слідів, деталей і обставин конкретного кримінального правопорушення. Використання технологій штучного інтелекту не повинно підміняти професійну

оцінку людини, адже саме слідчий здатний комплексно аналізувати фактичні дані та враховувати індивідуальні особливості кожного провадження.

Окрему проблему становить можливість формування помилкових висновків штучним інтелектом. Оскільки робота таких систем залежить від якості та повноти вхідних даних, ШІ може генерувати логічно обґрунтовані, проте фактично неправильні результати. Особливо небезпечним це є під час розслідування інсценувань, складних способів приховування злочину, аналізу поведінки осіб та оцінки психологічних аспектів. У подібних випадках автоматизований аналіз не завжди здатний врахувати всі приховані чи нестандартні обставини кримінального правопорушення.

Крім того, застосування штучного інтелекту пов’язане з процесуальними ризиками. Існує небезпека автоматичного копіювання текстів, шаблонного оформлення процесуальних документів та втрати індивідуалізації кримінального провадження. Такі недоліки можуть негативно впливати на допустимість доказів, законність проведення слідчих (розшукових) дій, а також на забезпечення прав учасників кримінального провадження.

Пропозиції щодо удосконалення кримінального процесуального законодавства України

Сучасні виклики зумовлюють необхідність подальшого розвитку кримінального процесуального законодавства України у напрямі цифровізації та впровадження новітніх технологій у діяльність органів досудового розслідування. В умовах стрімкого розвитку інформаційних технологій особливої актуальності набуває питання нормативного врегулювання використання автоматизованих систем підтримки прийняття процесуальних рішень, які можуть сприяти підвищенню ефективності аналізу інформації та оптимізації роботи слідчого.

Перспективним напрямом удосконалення кримінального процесуального законодавства є визначення процесуального статусу цифрових моделей місця події та результатів 3D–фіксації, що дозволить забезпечити належне використання сучасних засобів документування доказової інформації. Не менш важливим є врегулювання порядку застосування безпілотних літальних апаратів під час проведення слідчих (розшукових) дій, оскільки такі технічні засоби дедалі активніше використовуються для фіксації обстановки місця події, пошуку доказів та документування наслідків кримінальних правопорушень.

Подальшого вдосконалення потребує й система процесуального документообігу. Доцільним видається запровадження єдиних електронних стандартів процесуальних документів для органів досудового розслідування, що сприятиме уніфікації процесуальної практики та підвищенню оперативності кримінального провадження. Водночас актуальним є створення інтегрованої цифрової платформи взаємодії слідчого, прокурора, експерта та оперативних підрозділів з метою забезпечення швидкого обміну інформацією та координації процесуальної діяльності.

Окрему увагу необхідно приділити розширенню можливостей дистанційної участі спеціалістів та експертів у проведенні слідчих (розшукових) дій, що є особливо важливим в умовах воєнного стану та обмеженого доступу до окремих територій. Крім того, потребують удосконалення механізми фіксації, збереження та захисту електронних доказів, адже саме цифрова інформація дедалі частіше виступає важливим джерелом доказування у кримінальному провадженні.

Перелік використаних джерел:

1. Кримінальний процесуальний кодекс України // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651–17.

DOI https://doi.org/10.32837/11300.33605

Загородній Віктор
кандидат юридичних наук, доцент,
професор кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–1225–2814
e–mail: gponua@ukr.net

МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ПРОКУРОРА ЯК ПРОЦЕСУАЛЬНОГО КЕРІВНИКА НА ЗАВЕРШАЛЬНОМУ ЕТАПІ ДОСУДОВОГО РОЗСЛІДУВАННЯ

У тезах досліджуються можливості використання технологій штучного інтелекту в діяльності прокурора як процесуального керівника на завершальному етапі досудового розслідування. На підставі положень КПК України, судово–слідчої практики та сучасних тенденцій цифровізації кримінального провадження аналізуються питання перевірки доказової бази, правильності правової кваліфікації дій підозрюваного, дотримання процесуальних строків і законності проведення слідчих (розшукових) та негласних слідчих (розшукових) дій. Особлива увага приділяється використанню аналітичної підтримки штучного інтелекту для виявлення процесуальних порушень, оцінки допустимості доказів, забезпечення права на захист та контролю дотримання прав людини відповідно до вимог Кримінально процесуального кодексу України і практики Європейського суду з прав людини. Обґрунтовується значення інтеграції сучасних інформаційно–аналітичних систем у діяльність прокурора для підвищення ефективності процесуального керівництва та якості публічного обвинувачення.

Ключові слова: прокурор, процесуальне керівництво, обвинувальний акт, доказування, Кримінальний процесуальний кодекс України, права людини, допустимість доказів, штучний інтелект, досудове розслідування, Європейський суд з прав людини.

Zahorodnii Viktor
Candidate of Legal Sciences, Associate Professor,
Professor at the Department of Criminalistics, Forensic Examinations and Polygraphology
National University «Odesa Law Academy»
Odesa, Ukraine

POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF A PROSECUTOR AS A PROCEDURAL SUPERVISOR AT THE FINAL STAGE OF PRE–TRIAL INVESTIGATION

The theses examine the possibilities of using artificial intelligence technologies in the activities of a prosecutor as a procedural supervisor at the final stage of pre–trial investigation. The study considers the potential of modern information and analytical systems for verifying the completeness and relevance of the evidentiary base, the correctness of the legal qualification of the suspect's actions, compliance with procedural time limits, as well as the legality of investigative, search and covert investigative actions.

Particular attention is paid to the role of artificial intelligence as an auxiliary tool for analytical support of the prosecutor in identifying procedural violations, assessing the admissibility of evidence, verifying the compliance of the indictment with the requirements of criminal procedural legislation and ensuring the individual's right to defence. It is emphasized that the use of artificial intelligence in criminal proceedings cannot replace the procedural decision of the prosecutor; however, it can improve the quality of legal analysis, the timeliness of response to violations and the effectiveness of preparing materials for further public prosecution in court.

It is substantiated that the integration of digital technologies into prosecutorial activities should be carried out with due regard to the provisions of the Criminal Procedure Code of Ukraine, standards of admissibility of evidence, guarantees of human rights and the case law of the European Court of Human Rights. The conclusion is drawn that artificial intelligence may become an important means of increasing the effectiveness of procedural supervision, provided that the leading role of the prosecutor is preserved, algorithmic decisions remain transparent and automated decision–making on procedurally significant matters is not allowed without proper human control.

Key words: prosecutor, procedural supervision, indictment, proving, Criminal Procedure Code of Ukraine, human rights, admissibility of evidence, artificial intelligence, pre–trial investigation, European Court of Human Rights.

Сучасний розвиток цифрових технологій та впровадження систем штучного інтелекту формують нові підходи до організації досудового розслідування та процесуального керівництва. Особливого значення такі технології набувають на завершальному етапі досудового розслідування, коли прокурор здійснює перевірку повноти доказової бази, законності проведених процесуальних дій, правильності правової кваліфікації кримінального правопорушення та приймає рішення щодо затвердження обвинувального акта.

Відповідно до ст. 2 Кримінально процесуального кодексу України одним із завдань кримінального провадження є забезпечення швидкого, повного та неупередженого розслідування із дотриманням прав і свобод людини. У свою чергу, згідно зі ст. 36 Кримінально процесуального кодексу України прокурор здійснює процесуальне керівництво досудовим розслідуванням, забезпечує

додержання вимог закону, координує діяльність правоохоронних органів та підтримує публічне обвинувачення в суді.

Судово–слідча практика свідчить, що значна кількість процесуальних помилок виявляється саме на завершальному етапі досудового розслідування під час перевірки матеріалів кримінального провадження прокурором. До найбільш поширених належать:

неповнота доказової бази;

суперечності між доказами;

неналежне процесуальне оформлення слідчих (розшукових) дій; порушення вимог допустимості доказів;

помилки правової кваліфікації;

порушення права на захист;

недотримання процесуальних строків;

порушення порядку проведення негласних слідчих (розшукових) дій.

У таких умовах використання аналітичної підтримки штучного інтелекту може суттєво підвищити ефективність діяльності прокурора як процесуального керівника.

На завершальному етапі досудового розслідування системи штучного інтелекту можуть використовуватись для комплексного аналізу матеріалів кримінального провадження та автоматизованої перевірки відповідності процесуальних документів вимогам Кримінально процесуального кодексу України. Зокрема, ШІ може забезпечувати:

перевірку логічної узгодженості доказової бази;

виявлення суперечностей між показаннями учасників провадження;

аналіз достатності доказів для повідомлення про підозру та направлення обвинувального акта до суду;

контроль дотримання процесуальних строків;

виявлення ризиків визнання доказів недопустимими;

аналіз відповідності проведених слідчих дій вимогам Кримінально процесуального кодексу України.

Особливого значення набуває можливість використання систем штучного інтелекту для перевірки правильності правової кваліфікації дій підозрюваного. Аналітичні системи можуть здійснювати зіставлення фактичних обставин кримінального правопорушення з ознаками складу злочину, передбаченого Кримінальним кодексом України, аналізувати судову практику та виявляти типові помилки правозастосування.

Важливою складовою діяльності прокурора є забезпечення дотримання прав людини та гарантій сторони захисту. У цьому аспекті системи штучного інтелекту можуть використовуватись для:

контролю дотримання права на захист;

перевірки своєчасності вручення процесуальних документів;

аналізу законності застосування заходів забезпечення кримінального провадження;

перевірки дотримання вимог щодо проведення Негласних слідчих розшукових дій;

виявлення можливих порушень стандартів Європейської конвенції з прав людини та практики Європейського суду з прав людини.

Перспективним напрямом може стати створення автоматизованих робочих місць прокурора з інтегрованими модулями аналітичної підтримки ШІ. Такі системи можуть забезпечувати структуризацію матеріалів кримінального провадження, автоматизоване формування проектів процесуальних документів, побудову логічних схем доказування та аналітичне прогнозування судових ризиків.

Разом із тим використання штучного інтелекту у діяльності прокурора не повинно підміняти процесуальну самостійність та внутрішнє переконання прокурора. Остаточне рішення щодо затвердження обвинувального акта, оцінки доказів та визначення правової позиції повинно залишатися виключно за прокурором як суб’єктом кримінального процесу.

Таким чином, впровадження технологій штучного інтелекту у діяльність прокурора на завершальному етапі досудового розслідування створює нові можливості для підвищення якості процесуального керівництва, забезпечення законності, захисту прав людини та ефективного здійснення публічного обвинувачення. Комплексне поєднання кримінального процесу, криміналістики та сучасних інформаційно–аналітичних технологій формує перспективний напрям розвитку правоохоронної системи України в умовах цифровізації правосуддя.

Перелік використаних джерел:

1.Кримінальний процесуальний кодекс України // База даних «Законодавство України» / Верховна Рада України. URL: zakon.rada.gov.ua .

2.Про прокуратуру // База даних «Законодавство України» / Верховна Рада України. URL: zakon.rada.gov.ua.

DOI https://doi.org/10.32837/11300.33609

Згода Юлія
аспірантка кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0009–0001–3810–170X
e–mail: zgoda.yuliia@onua.edu.ua

ОБСТАНОВКА ВЧИНЕННЯ КОРИСЛИВИХ ЗЛОЧИНІВ В УМОВАХ ВОЄННОГО АБО НАДЗВИЧАЙНОГО СТАНУ

У тезах проаналізовано обстановку вчинення корисливих злочинів в умовах воєнного та надзвичайного стану. Розкрито вплив специфічних безпекових, соціальних та управлінських чинників на механізм злочинів. Обґрунтовано необхідність адаптації криміналістичних методик до сучасних реалій для ефективного розслідування.

Ключові слова: обстановка злочину, корисливі злочини, воєнний стан, надзвичайний стан, криміналістична характеристика, розслідування.

Zhoda Yuliia
postgraduate student of the Department of Criminalistics, Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

THE SETTING OF COMMITTING ACQUISITIVE CRIMES UNDER MARTIAL LAW OR STATE OF EMERGENCY

The theses analyze the setting of committing acquisitive crimes under martial law and a state of emergency. The influence of specific security, social, and administrative factors on the mechanism of crimes is revealed. The necessity of adapting forensic methodologies to modern realities for effective investigation is substantiated.

Keywords: crime setting, acquisitive crimes, martial law, state of emergency, forensic characterization, investigation.

Обстановка вчинення корисливих злочинів є багатогранним криміналістичним явищем, яке по–різному тлумачиться науковцями та включає різні складові елементи. Так, на думку В.А. Динту, вона формується під впливом матеріального, мікросоціального та морально–психологічного середовища, в якому відбувається підготовка, реалізація та приховування злочину [2]. Такий підхід дозволяє зрозуміти, що аналіз обстановки не може обмежуватися лише зовнішніми умовами, а має враховувати й психологічні чинники, які визначають поведінку суб’єктів злочину.

У контексті корисливих злочинів в умовах воєнного та надзвичайного стану аналіз обстановки набуває особливого значення. З одного боку, вона ускладнюється динамічними змінами безпекового середовища, правовими обмеженнями та соціально–економічними кризами. З іншого – саме ці фактори можуть виступати як сприятливим ґрунтом для вчинення злочину, так і стримуючим елементом у разі ефективного контролю. Тому криміналістичний аналіз обстановки корисливих злочинів у воєнних реаліях вимагає урахування не лише традиційних складових (часу, простору, матеріального середовища), але й специфічних умов, зумовлених війною: обмеження свободи пересування, посилені заходи охорони, психологічний тиск на населення та підвищений рівень недовіри в суспільстві.

У своїх дослідженнях В.Д. Берназ виокремлює структурні елементи обстановки вчинення кримінальних правопорушень, серед яких: матеріальне середовище (час, місце, об’єкт посягання, макро– та мікропогодні умови); організаційно–управлінське середовище (виробничо–функціональні об’єкти, діяльність правоохоронних структур); а також соціально–психологічне середовище (мікроклімат у трудовому колективі, система ціннісних орієнтацій, психологічна атмосфера у місці проживання) [1]. Такий підхід свідчить про багатофакторність обстановки злочину, де взаємодіють як об’єктивні, так і суб’єктивні чинники.

У наукових дискусіях простежується різноманіття позицій щодо наповнення цього поняття. Одні дослідники роблять акцент переважно на матеріальних елементах, інші вважають необхідним врахування не лише об’єктивних, а й суб’єктивних параметрів. Також існує підхід, згідно з яким обстановка охоплює соціологічні, політичні, географічні, природно–кліматичні, виробничі та інші фактори, що формують умови об’єктивної реальності [6, с. 99–112]. Водночас, у науковій літературі недостатньо досліджено питання взаємозв’язку між обстановкою злочину та умовами його вчинення.

Здійснюючи криміналістичний аналіз корисливих злочинів в умовах воєнного та надзвичайного стану обстановка набуває особливого значення. Війна чи надзвичайна ситуація змінюють матеріальне середовище (наприклад, руйнування інфраструктури, обмеження доступу до ресурсів), трансформують організаційно–управлінські механізми (зростання ролі військових адміністрацій, перевантаження правоохоронної системи), а також радикально впливають на соціально–психологічний клімат (підвищений рівень тривожності, зростання недовіри, деформація ціннісних орієнтацій).

Аналіз воєнного та надзвичайного стану у контексті розслідування корисливих злочинів доцільно здійснювати через три взаємопов’язані аспекти: правову регламентацію цих режимів, їх криміналістичне значення та особливості як специфічної обстановки вчинення і розслідування злочинів.

Насамперед воєнний та надзвичайний стан мають чітке нормативно–правове закріплення у законодавстві України. Правові засади запровадження та функціонування воєнного стану визначаються Конституцією України [3], Законом України «Про правовий режим воєнного стану» [4], а також низкою підзаконних актів, що регламентують діяльність органів державної влади, військового командування та правоохоронних органів у період збройної агресії або загрози нападу. Надзвичайний стан регулюється Законом України «Про правовий режим надзвичайного стану» [5] і запроваджується у випадках виникнення надзвичайних ситуацій природного або техногенного характеру, масових заворушень, спроб насильницької зміни конституційного ладу чи інших загроз державній безпеці. Обидва правові режими передбачають можливість тимчасового обмеження окремих прав і свобод громадян, встановлення спеціального порядку управління територіями, розширення повноважень органів державної влади та правоохоронних структур, а також залучення військових формувань до забезпечення правопорядку. Для кримінального провадження ці режими мають значення, оскільки вони впливають на організацію діяльності органів досудового розслідування, порядок взаємодії різних суб’єктів та умови реалізації процесуальних повноважень.

З криміналістичної точки зору воєнний і надзвичайний стан виступають специфічним фактором, що суттєво впливає на механізм злочинної діяльності та на процес її розслідування. У таких умовах відбувається трансформація криміногенної ситуації, що проявляється у зростанні кількості корисливих злочинів, появі нових способів їх вчинення та активізації організованих злочинних груп. Дестабілізація економічних процесів, переміщення населення, руйнування інфраструктури, дефіцит окремих ресурсів та послаблення контролю з боку державних інституцій створюють додаткові можливості для незаконного заволодіння майном, гуманітарною допомогою, бюджетними коштами, військовим майном або іншими матеріальними цінностями. У таких умовах криміналістичне значення воєнного чи надзвичайного стану полягає в тому, що він стає одним із елементів криміналістичної характеристики злочину, оскільки впливає на спосіб його підготовки, вчинення та приховування, а також на формування слідової картини.

Особливу роль зазначені правові режими відіграють як обстановка вчинення злочину. Як вже зазначалося вище, у криміналістиці обстановка традиційно розглядається як сукупність умов, у яких відбувається злочинна діяльність і здійснюється її розслідування. Воєнний або надзвичайний стан формує специфічну соціальну, організаційну та інформаційну ситуацію, яка безпосередньо впливає на поведінку злочинців і потерпілих, а також на можливості правоохоронних органів [7]. До характерних рис такої обстановки належать підвищений рівень соціальної напруженості, значні переміщення населення, зниження рівня контролю за окремими сферами господарської діяльності, використання воєнних або кризових умов для маскування злочинних

дій. Крім того, можуть виникати труднощі з доступом до місця події, фіксацією слідів, проведенням експертних досліджень, а також із забезпеченням належної взаємодії між різними правоохоронними структурами.

В умовах воєнного стану до зазначених факторів додаються бойові дії, небезпека для учасників кримінального провадження, руйнування транспортної та комунікаційної інфраструктури, тимчасова окупація окремих територій, що ускладнює збирання та перевірку доказів [8]. Надзвичайний стан також може створювати подібні ускладнення, особливо коли він запроваджується у зв'язку з масштабними катастрофами або масовими заворушеннями. У таких умовах особливого значення набувають гнучкість криміналістичних методик, використання сучасних технічних засобів фіксації доказів, активна взаємодія між правоохоронними органами, військовими формуваннями та іншими державними структурами.

Таким чином, воєнний та надзвичайний стан мають комплексне значення для криміналістики та практики розслідування корисливих злочинів. Вони виступають одночасно правовою категорією, що визначає особливий режим функціонування держави, фактором, який впливає на криміногенну ситуацію, і специфічною обстановкою вчинення та розслідування злочинів. Урахування цих особливостей є необхідною умовою формування ефективних криміналістичних методик та організації діяльності органів досудового розслідування в сучасних умовах.

Перелік використаних джерел:

1.Берназ В. Д. До питання про поняття обстановки вчинення крадіжок майна на морському транспорті. Криміналістика та судова експертиза. 1985. № 3. Київ: Вища школа, С. 44–47.

2.Динту В. А. Обстановка злочину як об'єкт пізнання. Актуальні проблеми держави і права. URL: http://www.apdp.in.ua/v69/62.pdf

3.Конституція України: Закон від 28.06.1996 № 254к/96–ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96–вр#doc_info

4.Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389–VIII. URL: https://zakon.rada.gov.ua/laws/show/389–19#doc_info

5.Про правовий режим надзвичайного стану: Закон України від 16.03.2000 № 1550–III. URL: https://zakon.rada.gov.ua/laws/show/1550–14#doc_info

6.Чучко С. В. Розслідування шахрайства при купівлі–продажу товарів через мережу Інтернет : дис. док–ра філософії. 081 – Право; Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 276 с.

7.Шрамко С. С., Калініна А. В., Злочинність в Україні: яка вона є під час війни і якою може бути у післявоєнний час? Питання боротьби зі злочинністю. № 44. 2022. С. 98–106

8.Янішевська К. Д. Деякі аспекти латентності кримінальних правопорушень, вчинених на тимчасово окупованих та деокупованих територіях. Юридичний науковий електронний журнал. № 11. 2022. С. 611–614

DOI https://doi.org/10.32837/11300.33610

Кіліміченко Сергій
аспірант кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0006–7862–8828
e–mail: skilimichenko@ukr.net

ОБСТАВИНИ, ЯКІ ПІДЛЯГАЮТЬ ВСТАНОВЛЕННЮ ПІД ЧАС ВИЯВЛЕННЯ ОЗНАК ПРОТИДІЇ РОЗСЛІДУВАННЮ

У тезах проаналізовано систему обставин, що підлягають встановленню під час виявлення протидії розслідуванню. Обґрунтовано криміналістичний підхід до реконструкції механізму протидії як цілісного явища. Визначено ключові групи факторів, що дозволяють ефективно діагностувати та нейтралізувати перешкоди.

Ключові слова: протидія розслідуванню, криміналістичний аналіз, доказова інформація, злочинна діяльність, слідча ситуація, нейтралізація.

Kilimichenko Serhii
postgraduate student of the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

CIRCUMSTANCES TO BE ESTABLISHED UPON DETECTION OF INVESTIGATION OBSTRUCTION

The theses analyze the system of circumstances to be established upon the detection of investigation obstruction. A forensic approach to reconstructing the mechanism of obstruction as a holistic phenomenon is substantiated. Key groups of factors that allow for effective diagnosis and neutralization of obstacles are identified.

Keywords: investigation obstruction, forensic analysis, evidentiary information, criminal activity, investigative situation, neutralization.

Обставини, які підлягають встановленню під час виявлення ознак протидії розслідуванню, утворюють самостійну та внутрішньо складну систему фактів, даних і зв’язків, без з’ясування яких неможливо ані коректно діагностувати сам феномен протидії, ані визначити її місце у системі злочинної діяльності, ані обґрунтовано вибудувати стратегію подальшого доказування. У криміналістичному розумінні протидія розслідуванню виступає не випадковою сукупністю перешкод, а особливим різновидом діяльності, що має власну логіку, інструментарій, суб’єктний склад, часово–просторові параметри, інформаційні

«мішені» та прогнозовані наслідки [1]. Відповідно, встановлювані обставини мають охоплювати не лише «що саме сталося» у площині окремого інциденту (наприклад, зник документ або свідок змінив показання), а і «чому саме так сталося», «кому це вигідно», «яким способом досягнуто результату», «як протидія інтегрована у злочинну діяльність» та «які системні умови забезпечили її ефективність». У цьому полягає принципова відмінність криміналістичного підходу від суто процесуального констатування перешкод: криміналістика прагне реконструювати механізм протидії як явища, а не лише відреагувати на окрему його ознаку.

Розглянемо детально коло обставин, які підлягають встановленню під час виявлення ознак протидії розслідуванню:

1. Обставини пов’язані зі встановленням факту протидії. Встановлення факту протидії повинно спиратися на аналіз наміру, контексту і наслідків: чи спричиняють відповідні дії непропорційне спотворення інформаційного середовища, чи мають вони ознаки координованості, чи спрямовані вони на ключові джерела доказової інформації, чи супроводжуються прихованим впливом на осіб та носії даних.

2. Обставини пов’язані з встановленням характеру та спрямованості протидії (тобто встановлення того, на який результат вона орієнтована).

У практичному вимірі можна виокремити протидію, спрямовану на: повний «підрив» розслідування (створення умов, за яких доказування стає неможливим або втрачає перспективу); суттєве затягування строків з метою «втомити» слідство, домогтися втрати актуальності доказів, зміни процесуальної ситуації чи застосування більш м’яких заходів; дискредитацію доказової бази через формування сумнівів у її достовірності та допустимості; вплив на суб’єктів доказування (свідків, потерпілих, експертів, понятих, службових осіб) шляхом тиску, підкупу, шантажу, психологічної маніпуляції; конструювання хибної картини події шляхом інсценування, підміни причинно–наслідкових зв’язків, «переприсвоєння» ролей учасників, створення легенди; дестабілізацію організаційної роботи слідчої групи, розпорошення зусиль та ресурсів через множинні інформаційні вкиди, паралельні повідомлення, штучні скарги та конфлікти [3]. Встановлення спрямованості протидії є принциповим, оскільки саме воно визначає подальші тактичні рішення: що саме треба захищати насамперед, які джерела інформації є «вразливими», де очікувати наступний удар, які процесуальні та організаційні заходи можуть забезпечити стійкість доказування.

3. Обставини пов’язані зі встановленням суб’єктного складу протидії та ідентифікація ролей учасників

Особливо складними є випадки, коли протидія здійснюється за участю посадових осіб або через використання службового становища. Тут обставинами, що підлягають встановленню, виступають: встановлення обставин щодо використання особами службових повноваженнь і реальний доступ до інформації

та носіїв доказів; встановлення обставин щодо наявності конфлікту інтересів; встановлення обставин щодо існування зв'язків посадової особи з підозрюваними або їх середовищем; встановлення обставин щодо способу використання службових процедур для створення перешкод; характер «легалізації» протидії у формах службових документів або формально правомірних дій [2].

У таких ситуаціях зростає значущість встановлення прихованих прийомів та методів впливу: неформальних домовленостей, обміну послугами, «взаємних зобов'язань», системи винагород і гарантій безпеки. При цьому криміналістичне встановлення обставин протидії повинно бути особливо уважним до доказового стандарту, оскільки будь–які твердження про корупційний компонент потребують чітких, перевірюваних даних, а не припущень.

4. Обставини пов'язані зі встановленням часових та просторових параметрів протидії

Такі обставини включають в себе визначення моменту її початку, тривалості, фазності та інтенсивності. Протидія може стартувати ще до вчинення основного злочину, коли суб'єкти планують «прикриття» майбутніх дій: створюють фіктивні документи, готують версії, облаштовують маршрути відходу, заздалегідь змінюють налаштування техніки, обмежують створення цифрових слідів, формують «сліпі зони» відеоспостереження. У такому разі обставини протидії тісно переплітаються з способами підготовки злочину і потребують встановлення того, які саме елементи підготовки мали подвійне призначення: забезпечити вчинення злочину і мінімізувати ризики викриття. Протидія може виникати безпосередньо після події, коли здійснюються «екстрені» дії з усунення слідів або формування первинної легенди. Вона може активізуватися при виникненні певних процесуальних загроз: після перших допитів, проведення обшуків, арешту майна, отримання доступу до даних. Вона може також мати хвилеподібний характер: періоди затишшя змінюються періодами активних атак на доказування, що часто корелює з ключовими процесуальними рішеннями у провадженні [4].

5. Обставини пов'язані з встановленням способів, засобів і прийомів протидії.

Саме вони формують «операційну тканину» цього явища. Встановлення способу протидії передбачає не просто опис того, що було зроблено, а реконструкцію послідовності дій, використаних ресурсів, контрольних точок і очікуваних ефектів. Способи протидії можна розглядати як такі, що спрямовані на матеріальні сліди, на людські джерела інформації, на процесуальну форму, на цифрове середовище та на соціально–інформаційний контекст. Матеріальний напрям включає приховування, знищення, підміну, переміщення предметів і документів, штучне створення або видалення слідів, модифікацію обстановки місця події. Установленню підлягає, які саме дії здійснювалися (очищення, заміна об'єктів, маніпуляція інструментами), чи мали вони професійні ознаки, чи

використовувалися спеціальні засоби, чи є сліди вторинного втручання. Людський напрям охоплює вплив на свідків, потерпілих, підозрюваних, експертів, а також на осіб, що можуть володіти інформацією про злочин. Тут важливо встановити форму впливу (переконання, тиск, підкуп, шантаж), його інтенсивність, наявність посередників, повторюваність контактів, а також психологічну уразливість об'єкта впливу.

6. Обставини пов'язані з встановленням об'єкта протидії (того, на що спрямовано вплив)

У криміналістичному сенсі таким об'єктом є доказова інформація як системна категорія, що охоплює матеріальні сліди, документи, цифрові дані, показання, експертні висновки, аналітичні продукти, а також процесуальну форму фіксації та використання цих відомостей. Підлягає встановленню, які конкретні елементи доказової системи стали мішенню, чому саме вони, чи є це вибірковою атакою на «слабку ланку», чи системним руйнуванням структури доказування. Важливим є з'ясування, чи спрямована протидія на первинні носії інформації (місце події, предмети, пристрої, бази даних) або на вторинні продукти (протоколи, звіти, експертні висновки), оскільки ці рівні мають різну вразливість і різні механізми відновлення.

7. Обставини пов'язані з встановленням конкретних механізмів впливу на учасників провадження

Варто зазначити, що саме через людей нерідко відбувається руйнування доказування без прямого «фізичного» знищення слідів. Підлягає встановленню, хто саме піддавався впливу, в якій формі і через які канали. Важливо з'ясувати, чи здійснювався контакт безпосередньо або через посередників; чи мав місце підкуп (у грошовій або негрошовій формі, включно з обіцянками послуг), чи була наявна загроза (пряма або завуальована), чи застосовувалася психологічна маніпуляція (апеляція до вини, сорому, страху за близьких, «раціоналізація» неправдивих показань).

8. Обставини пов'язані зі встановленням здійснення протидії у цифровому вимірі.

Виявляючи цифрову протидію, необхідно встановлювати не лише факт втручання, а й його авторство та контекст: хто мав доступ, коли здійснювалися дії, з яких пристроїв, чи співпадає це з іншими подіями у провадженні. Установленню підлягає і наявність «інсценованих» цифрових доказів, коли створюються фальшиві повідомлення, файли, фотографії, або коли справжні дані подаються у викривленому вигляді. У цьому аспекті криміналістична оцінка завжди має бути комплексною: цифрові дані аналізуються разом із матеріальними, поведінковими та процесуальними слідами, щоб уникнути як безпідставного довір'я до «цифри», так і необґрунтованого її заперечення.

9. Обставини пов'язані зі встановленням наслідків протидії.

Особливо важливо встановити, чи є наслідки протидії оборотними чи необоротними. Необоротність може полягати у фізичному знищенні унікальних

слідів, у втраті можливості відтворити первинний стан обстановки, у втраті короткоживучих цифрових журналів, у деградації пам'яті свідків з часом. Якщо наслідки є необоротними, це зумовлює необхідність максимального використання непрямих доказів, логічних реконструкцій, експертних моделей, а також підвищує значущість належної процесуальної фіксації залишкових даних. Якщо наслідки оборотні, ключовим стає питання темпу і правильної організації відновлювальних заходів.

10. Обставини пов'язані з встановленням умов та причин, що сприяли виникненню та реалізації протидії.

Вони формують «фон» і «інфраструктуру» для її успіху. До таких умов належать організаційні слабкості: недостатня координація між підрозділами, відсутність чітких протоколів захисту доказів, перевантаженість персоналу, обмеженість технічних ресурсів, нестача спеціалістів у цифровій сфері. До правових умов можуть належати прогалини у регулюванні, колізії, невизначеність процедур, що дозволяють суб'єктам протидії маневрувати. До соціальних умов – низька довіра до правоохоронних органів, страх свідків, соціальна напруженість, вплив кримінальних авторитетів. У контексті воєнного стану та безпекових загроз з'являються додаткові умови: обмежений доступ до територій, руйнування інфраструктури, переміщення населення, збільшення латентності злочинів, перебої зв'язку, що можуть використовуватися для маскування протидії.

Встановлення обставин під час виявлення ознак протидії розслідуванню є комплексним, багаторівневим процесом, що поєднує аналіз фактів, реконструкцію механізмів, оцінку інформаційних систем і прогнозування поведінки зацікавлених осіб. Тому криміналістичне осмислення та ретельне встановлення зазначених обставин має розглядатися як необхідна умова ефективності кримінального провадження, особливо у справах із підвищеним рівнем організованості злочинної діяльності, корупційними ризиками та значною часткою цифрової доказової інформації.

Перелік використаних джерел:

1.Криміналістика : підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Самодін та ін. ; за заг. ред. В. В. Пясковського. 2–ге вид., перероб. і допов. Київ : Філія вид–ва «Право», 2020. С. 262–263.

2.Павленко С. О. Деякі особливості протидії хабарництву, вчиненому службовими особами, які займають відповідальне становище. Боротьба з організованою злочинністю і корупцією (теорія і практика): наук.–практ. журн. 2013. № 2 (30). С. 279–288.

3.Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві : Закон України від 23.12.1993 № 3782–XII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/3782–12

4.Шепітько В. Ю. Криміналістична тактика (системно–структурний аналіз): монографія. Харків : Харків юридичний, 2007. 431 с.

DOI https://doi.org/10.32837/11300.33611

Кіліміченко Христина
аспірантка кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0002–7262–8828
e–mail: kristina.tcimbal@gmail.com

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТАКТИЧНИХ ОПЕРАЦІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ВЧИНЕНИХ ЖІНКАМИ

У тезах досліджено сутність типових тактичних операцій при розслідуванні злочинів проти національної безпеки, вчинених жінками. Визначено специфіку жіночої участі у таких злочинах та розмежовано поняття тактичної операції й комбінації. Запропоновано перелік операцій для підвищення ефективності досудового слідства.

Ключові слова: тактична операція, національна безпека, жінки, тактична комбінація, розслідування.

Kilimichenko Khrystyna
postgraduate student of the Department of Criminalistics,
Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

PECULIARITIES OF APPLYING TACTICAL OPERATIONS DURING THE INVESTIGATION OF CRIMES AGAINST NATIONAL SECURITY COMMITTED BY WOMEN

The theses explore the essence of typical tactical operations in the investigation of crimes against national security committed by women. The specifics of female participation in such crimes are identified, and the concepts of «tactical operation» and «tactical combination» are differentiated. A list of operations is proposed to improve the effectiveness of pre–trial investigation.

Keywords: tactical operation, national security, women, tactical combination, investigation.

Типова тактична операція під час розслідування злочинів проти основ національної безпеки, вчинених жінками, – це криміналістично обґрунтована програма комплексного, послідовного та узгодженого застосування слідчих (розшукових), негласних слідчих (розшукових), оперативно–розшукових,

інформаційно–аналітичних, експертних і організаційних заходів, спрямованих на вирішення конкретного тактичного завдання у типовій слідчій ситуації з урахуванням специфіки жіночої участі у механізмі антидержавної злочинної діяльності. У провадженнях досліджуваної категорії такими завданнями можуть бути, зокрема, встановлення особи фігурантки, документування її контактів із представниками держави–агресора, виявлення кураторів і посередників, фіксація факту передачі інформації, встановлення джерел фінансування, перевірка мотивів і ступеня усвідомлення злочинної мети, а також припинення подальшої протиправної діяльності.

Разом із тим типову тактичну операцію у межах розслідування злочинів зазначеної категорії слід розглядати як заздалегідь розроблену криміналістичну програму реалізації комплексу дій та заходів, спрямованих на вирішення конкретного тактичного завдання на певному етапі розслідування, коли досягнення відповідної мети шляхом проведення окремої слідчої (розшукової) чи негласної слідчої (розшукової) дії є недостатнім або неможливим.

Специфіка таких типових тактичних операцій полягає у тому, що вони повинні враховувати не лише загальні закономірності розслідування злочинів проти основ національної безпеки, але й особливості жіночої участі у відповідній протиправній діяльності. Йдеться, зокрема, про можливе виконання жінкою конкретних злочинних функцій; використання нею соціальних, родинних чи професійних зв’язків; цифрових каналів комунікації; а також імовірність її перебування під впливом куратора, вербувальника, близької особи, пропагандистського середовища або інших чинників зовнішнього впливу.

Досить часто у криміналістичній літературі поряд із поняттям тактичної операції згадується інший тактичний засіб – тактична комбінація. Слід підкреслити, що дані два поняття в жодному разі не є тотожними за змістом та значенням, хоча в деяких підручниках з криміналістики все ще можна зустріти формулювання «тактичні операції (комбінації)». Зокрема визначають, що тактична комбінація – це певне поєднання тактичних прийомів чи слідчих дій та інших заходів, що має на меті вирішити конкретне завдання розслідування та зумовлене цією метою і слідчою ситуацією [2, с. 267;6, с. 12]. В основі даного підходу до розуміння тактичної комбінації лежить традиція використання в теорії оперативно–розшукової діяльності поняття «оперативна комбінація». Деякі вчені визначають оперативну комбінацію як об’єднані спільною метою оперативно–розшукові заходи, методи і прийоми, спрямовані на вирішення певних тактичних задач оперативно–розшукової діяльності відповідно до оперативно–розшукової ситуації [5]. При цьому в теорії оперативно–розшукової діяльності поняття «оперативна комбінація» є ширшим за поняття «оперативна операція».

Проте з позиції науки криміналістики в поняття «операція» та «комбінація» закладається дещо інший зміст, обсяг та призначення даних тактичних засобів, аніж в теорії оперативно–розшукової діяльності. Тому, на нашу думку, в рамках положень криміналістичної тактики недоцільно об’єднувати в одному понятті дві

самостійні категорії – «поєднання тактичних прийомів» і «поєднання слідчих та інших заходів», адже зазначені тактичні засоби мають різну мету і не є рівнозначними між собою. Під тактичною комбінацією слід розуміти сукупність різних тактичних прийомів, об'єднаних однією метою для вирішення конкретного тактичного завдання в рамках однієї чи кількох слідчих дій [4, с. 248]. Тактичні комбінації можуть реалізовуватися задля: створення умов, необхідних для проведення процесуальної дії; забезпечення слідчої таємниці; здійснення тактичного впливу на слідчу ситуацію з метою її зміни або використання [3, с. 122]. Окрім того, з позиції складності організації та реалізації тактичні операції є більш високоорганізованими, адже їх реалізація передбачає здійснення взаємодії співробітників слідчих, оперативно–розшукових, ревізійних, контролюючих та інших органів, а також спеціалістів у певній галузі знань на шляху вирішення конкретного тактичного завдання [8, с.203].

Тож переходячи до визначення типових тактичних операцій та тактичних комбінацій, які можуть реалізовуватися під час розслідування злочинів проти основ національної безпеки, вчинених жінками, слід наголосити, що досить широка система досліджуваних злочинів не дозволяє визначитися із повним їх комплексом. Проте саме окремі складові механізму злочинної діяльності, пов'язані із участю жінок, переважним організованим характером такої протиправності, який не завжди вдається довести правоохоронним органам, та значним обсягом цифрової доказової інформації, дозволяють визначити ряд загальних типових тактичних операцій та комбінацій.

Як слушно відзначає В.С. Бондар, в умовах воєнної агресії і незахищеності кордонів України колабораційна діяльність, тероризм, державна зрада, екстремізм, сепаратизм набувають організованих форм, зумовлюють трансформацію організованої злочинності [1, с.112]. І до усіх названих науковцем антидержавних злочинів активно залучаються жінки у якості безпосередніх виконавиць, посередниць, зв'язкових, адміністраторок інформаційних ресурсів, фінансових операторок, учасниць злочинних схем, які збирають або передають відомості, координують комунікацію між учасниками, забезпечують поширення антидержавного контенту або виконують інші допоміжні функції. Це обумовлено тим фактом, що участь жінок може легко маскуватися під побутову, родинну, волонтерську, громадську, журналістську, інформаційну чи іншу зовні правомірну активність, що ускладнює своєчасне виявлення ознак злочинної діяльності та належне доказування фактичної ролі жінки у механізмі кримінального правопорушення.

З огляду на це ізольоване застосування окремих слідчих (розшукових), негласних слідчих (розшукових) дій, оперативно–розшукових чи інформаційно–аналітичних заходів не завжди здатне забезпечити досягнення мети досудового розслідування. У багатьох випадках встановлення механізму злочинної діяльності, каналів комунікації, зв'язків із представниками держави–агресора, джерел

фінансування, способів конспірації, мотивів та ступеня усвідомлення жінкою протиправного характеру власних дій потребує комплексного, узгодженого та послідовного використання різних криміналістичних засобів. Саме тому особливого значення набуває проведення тактичних операцій як форми складної та спільної високоорганізованої діяльності різних підрозділів правоохоронних органів.

Зміст тактичної операції у провадженнях досліджуваної категорії може охоплювати як різнойменні, так і однойменні слідчі (розшукові) дії, НС(Р)Д, оперативні заходи, аналітичну роботу з відкритими джерелами, фінансовий аналіз, залучення спеціалістів і експертів, взаємодію зі ЗМІ, громадськими об'єднаннями, психологами, прикордонними, кібернетичними, фінансово–аналітичними та іншими компетентними підрозділами. Їх поєднання має бути не механічним, а функціонально обумовленим конкретною слідчою ситуацією та спрямованим на вирішення певного тактичного завдання.

Тактичні операції можуть бути спрямовані на вирішення низки ключових завдань: встановлення факту причетності жінки до злочину проти основ національної безпеки; визначення її функціональної ролі у механізмі протиправної діяльності; виявлення кураторів, посередників, співучасників та інших осіб, із якими вона взаємодіє; документування фактів передачі інформації, виконання завдань, отримання винагороди або поширення антидержавного контенту; встановлення джерел фінансування; виявлення цифрових і матеріальних слідів; припинення злочинної діяльності та нейтралізація протидії розслідуванню.

В.М. Шевчук виокремлює систему типових тактичних операцій, які можуть бути реалізовані під час розслідування різних видів кримінальних правопорушень. Зокрема, до таких типових тактичних операцій він відносить «Встановлення характеру події кримінального правопорушення», «Встановлення місця і часу вчинення кримінального правопорушення», «Встановлення способу вчинення кримінального правопорушення», «Встановлення предмету злочинного посягання», «Встановлення мотивів вчинення злочину», «Встановлення особи злочинця», «Встановлення особи потерпілого (жертви)», «Встановлення провокуючої поведінки жертви», «Перевірка зв'язків потерпілого», «Встановлення співучасників злочину», «Затримання злочинця на місці злочину», «Розшук особи, яка зникла з місця події і переховується від слідства», «Перевірка алібі підозрюваного», «Встановлення свідків», «Перевірка обмови», «Перевірка самообмови», «Нейтралізація протидії розслідуванню з боку зацікавлених осіб», «Вивчення особи підозрюваного», «Усунення негативного впливу з боку підозрюваного», «Захист доказів», «Захист потерпілих», «Захист свідків», «Профілактика» [7, с.346–347]. Загалом слід погодитися із наведеним переліком тактичних операцій, адже їх універсальний характер пов'язаний із типовістю тактичних завдань, на вирішення яких вони спрямовані.

Разом із тим, злочини проти основ національної безпеки мають свою певну специфіку, обумовлену механізмом злочинної діяльності, предметом злочинного

посягання, рівнем організованості та конспірації протиправної діяльності. Тому на нашу думку, до найбільш типових тактичних операцій у межах розслідування зазначеної категорії кримінальних правопорушень можна віднести: «Встановлення ролі жінки у механізмі антидержавної діяльності»; «Виявлення куратора та каналів комунікації»; «Документування передачі інформації представникам держави–агресора»; «Виявлення фінансового забезпечення протиправної діяльності»; «Затримання фігурантки під час реалізації контрольованої злочинної дії» («Затримання на гарячому»).

Таким чином, тактична операція у кримінальних провадженнях щодо злочинів проти основ національної безпеки, вчинених жінками, є не лише засобом поєднання окремих слідчих (розшукових) і негласних слідчих (розшукових) дій, оперативно–розшукових та інших заходів, а складною криміналістичною програмою, що забезпечує системне вирішення ключових завдань розслідування. Її застосування дозволяє вирішити складні тактичні завдання, процесуально закріпити виявлену інформацію та попередити завдання шкоди інтересам національної безпеки. Саме тому розроблення типових тактичних операцій для зазначеної категорії кримінальних проваджень слід розглядати як один із перспективних напрямів удосконалення криміналістичної методики розслідування злочинів проти основ національної безпеки, вчинених жінками.

Перелік використаних джерел:

1.Бондар В.С. Тактична операція як криміналістична категорія: сутність та зміст застосування під час розслідування злочинів, учинених злочинними спільнотами. Прикарпатський юридичний вісник. 2023. № 4 (51). С. 112–122.

2.Пчолкін В. Д., Федосова О. В. Тактичні операції при розслідуванні злочинів економічної спрямованості. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренко. 2019. № 4 (88). С. 265–277.

3.Копча В. В., Копча Н. В. Криміналістична техніка, тактика і методика : навчальний посібник. Одеса : Видавничий дім «Гельветика», 2022. 286 с.

4.Криміналістика. Академічний курс: підручник / Т.В.Варфоломеєва, В.Г. Гончаренко, В.І. Бояров та ін. Київ:Юрінком Інтер, 2011. 504 с.

5.Оперативно–розшукова діяльність органів внутрішніх справ: Загальна частина: підручник / кол. авт.: Е. О. Дідоренко, І. П. Козаченко, Я. Ю. Кондратьєв та ін. ; за ред. Л.В. Бородича. Луганськ: РВВ ЛІВС, 1999. Т. 1. 390 с.

6.Чаплинський К.О. Тактика проведення окремих слідчих дій: монографія. Дніпропетровськ, 2006. 416 с.

7.Шевчук В.М. Тактичні операції у криміналістиці: теоретичні засади формування та практика реалізації: монографія. Харків: Видавнича агенція «Апостіль», 2013. 440 с.

8.Шевчук В.М. Тактичні операції в системі тактико–криміналістичних комплексів. Право і Безпека. 2012. № 4 (46). С. 199–205.

DOI https://doi.org/10.32837/11300.33614

Ковиршин Віктор
аспірант кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0007–4733–4656
e–mail:adv.vkvs@gmail.com

СПЕЦИФІКА ЗАТРИМАННЯ АДВОКАТА У КРИМІНАЛЬНОМУ ПРОЦЕСІ

У тезах досліджено особливості затримання адвоката відповідно до чинного кримінального процесуального законодавства України та проаналізовано співвідношення положень КПК України і Закону України «Про адвокатуру та адвокатську діяльність» у частині гарантій захисту прав адвокатів під час застосування заходів процесуального примусу. Зроблено висновок, що відсутність у КПК України спеціальної процедури затримання адвоката призводить до практичних проблем у забезпеченні прав адвокатів.

Ключові слова: кримінальний процес, адвокат, затримання, процесуальні гарантії

Kovyrshyn Viktor
Postgraduate Student of the Department of Criminal Procedure at
National University «Odesa Law Academy»,
Odesa, Ukraine

SPECIFICS OF DETENTION OF AN ATTORNEY IN CRIMINAL PROCEEDINGS

The theses examine the peculiarities of the detention of a lawyer in accordance with the current criminal procedural legislation of Ukraine and analyze the correlation between the provisions of the Criminal Procedure Code of Ukraine and the Law of Ukraine «On the Bar and Practice of Law» regarding guarantees for the protection of lawyers' rights during the application of procedural coercive measures. It is concluded that the absence of a special procedure for the detention of a lawyer in the Criminal Procedure Code of Ukraine leads to practical difficulties in ensuring the rights of lawyers.

Keywords: criminal procedure, lawyer, detention, procedural guarantees.

Однією з важливих гарантій здійснення адвокатської діяльності є встановлення спеціального порядку кримінального провадження щодо адвокатів, зокрема під час застосування заходів процесуального примусу. Особливого значення у цьому контексті набуває затримання адвоката, яке безпосередньо

пов'язане з обмеженням конституційного права на свободу та особисту недоторканність, а також може впливати на незалежність адвокатської діяльності та реалізацію права особи на професійну правничу допомогу. У зв'язку з цим кримінальне процесуальне законодавство України передбачає додаткові гарантії та спеціальні вимоги щодо порядку затримання адвоката.

Одразу необхідно підкреслити, що чинне кримінальне процесуальне законодавство не містить жодних особливостей щодо затримання адвоката, проте такі особливості передбачені в профільному законі. Так, відповідно до п. 12 ч. 1 ст. 23 ЗУ «Про адвокатуру та адвокатську діяльність», орган або посадові особи, які затримали адвоката або застосували до нього запобіжний захід, зобов'язані негайно повідомити про це відповідну раду адвокатів регіону [1]. В такий спосіб законодавець намагається надати адвокату додаткові процесуальні гарантії проти незаконного затримання. Однак проблема в даному випадку полягає у тому, що в КПК України відповідні зміни внесені не були, що на практиці стає причиною ігнорування таких вимог.

Так, відповідно до ч. 3 ст. 9 КПК України, «закони та інші нормативно–правові акти України, положення яких стосуються кримінального провадження, повинні відповідати цьому Кодексу. При здійсненні кримінального провадження не може застосовуватися закон, який суперечить цьому Кодексу» [2]. Саме через це деякі представники правоохоронних органів відмовляються виконувати вимоги, які передбачені ЗУ «Про адвокатуру та адвокатську діяльність», адже така процедура чинним кримінальним процесуальним законодавством не передбачена.

Асоціація адвокатів України розробила маніфест, в якому, крім іншого, зазначено, що «гарантії адвокатської діяльності повинні бути розширені шляхом законодавчого закріплення норм про неможливість затримання адвоката без згоди ради адвокатів регіону, проведення щодо нього слідчих дій тільки за ухвалою апеляційного суду за клопотанням Генпрокурора, заборону на вилучення належних йому засобів зв'язку і комп'ютерної техніки» [3]. Хоча пропозиції, які містяться в даному маніфесті, дійсно підвищили би процесуальні гарантії професійного захисту адвокатів у кримінальному провадженні, реалістичність запровадження таких змін виглядає дещо сумнівною. Очевидно, що рада адвокатів регіону повинна бути обізнана з фактом затримання та можливістю захисту свого колеги, проте отримання згоди на затримання означає, що такі процесуальні дії неможливо буде вчинити в момент вчинення кримінального правопорушення, а аналогічні гарантії були ліквідовані по відношенню навіть до народних депутатів.

Наразі гарантії захисту прав адвокатів містяться лише в ЗУ «Про адвокатуру та адвокатську діяльність», тому самі ради адвокатів регіонів надають наступні рекомендації щодо дій у випадку затримання: «наполягайте на здійсненні дзвінка до регіональної ради адвокатів з метою повідомлення про факт затримання для виїзду її представників (п. 12 ч. 1 ст. 23 Закону України «Про адвокатуру та адвокатську діяльність»). Сприяння захисту та представництву інтересів адвоката

за таких обставин – право та обов'язок органів адвокатського самоврядування. Зокрема, Радою адвокатів Київської області для оперативного реагування на подібні питання створений та успішно діє Комітет захисту професійних прав адвокатів та реалізації гарантій адвокатської діяльності» [4].

Таким чином наразі можна констатувати досить слабкі процесуальні гарантії захисту прав адвокатів під час затримання, у зв'язку з чим доцільно вести мову про внесення змін до чинного кримінального процесуального законодавства.

Перелік використаних джерел:

1. Закон України «Про адвокатуру та адвокатську діяльність». Відомості Верховної Ради (ВВР), 2013, № 27, ст.282. URL: https://zakon.rada.gov.ua/laws/show/5076–17#Text

2. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України (ВВР), 2013, № 9–10, № 11–12, № 13, ст.88. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text

3. Затримання адвоката повинно відбуватися тільки за згоди ради адвокатів регіону – маніфест ААУ. URL: http://kdkako.com.ua/zatrymannya–advokata–povynno–vidbuvatysya–til′ky–za–z·hody–rady–advokativ–rehionu–manifest–aau/

4. Затримання адвоката: алгоритм протидій. Національна асоціація адвокатів України: веб сайт. URL: https://unba.org.ua/publications/1804–zatrimannya–advokata–algoritm–protidij.html

DOI https://doi.org/10.32837/11300.33616

Денис Колодін
доктор юридичних наук, професор,
декан факультету прокуратури та слідства (кримінальної юстиції)
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–6368–0849
e–mail:kolodinodessa@gmail.com

Анна Колодіна
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–7097–0155
e–mail:padeyanya@gmail.com

ДО ПИТАННЯ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ НА СИСТЕМУ ЗАСОБІВ КРИМІНАЛІСТИЧНОЇ ТАКТИКИ

У тезах розглянуто актуальні питання впливу цифровізації, яка трансформує криміналістичну тактику, а саме змінюючи як зміст окремих тактичних засобів, так і механізм їх реалізації у процесі розслідування кримінальних правопорушень. Акцентовано увагу на тому, що сьогодні сучасні цифрові технології стають не лише джерелом доказової інформації, а й потужним інструментом організації, планування та проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій.

Ключові слова: криміналістична тактика, цифрова криміналістика, цифрові технології, засоби криміналістичної тактики, цифровізація, криміналістика.

Kolodin Denys
Doctor of Law, Professor, Dean of the Faculty of Prosecution and Investigation (Criminal Justice) National University «Odesa Law Academy»
Odesa, Ukraine

Kolodina Anna
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminslistics, Forensic Examinations and Polygraphology National University «Odesa Law Academy»
Odesa, Ukraine

ON THE ISSUE OF THE IMPACT OF DIGITAL TECHNOLOGIES ON THE SYSTEM OF FORENSIC TACTICS TOOLS

The theses consider the current issues of the impact of digitalization, which transforms forensic tactics, namely by changing both the content of individual tactical means and the mechanism of their implementation in the process of investigating criminal offenses. Attention is focused on the fact that today modern digital technologies are becoming not only a source of evidentiary information, but also a powerful tool for organizing, planning and conducting investigative (search) actions and covert investigative (search) actions.

Key words: forensic tactics, digital forensics, digital technologies, forensic tactics tools, digitalization, forensics.

Стрімкий розвиток діджиталізації та вплив цифровізації на усі сфери людської діяльності сьогодні набуває неабиякого значення та потребує змін і адаптації, не винятком у цих процесах є також криміналістика, яка становить важливе значення для діяльності розслідування кримінальних правопорушень. Трансформація криміналістичної діяльності сьогодні відбувається саме через зміну інструментарію (засобів та методів), які є ефективними в процесі практичної діяльності з розслідування, а також інтеграції та диференціації наукових знань, що обумовлено розвитком цифрових технологій, спрямованих на вирішення завдань протидії злочинності.

Наслідки діджиталізації є передумовою розширення предмету сучасної криміналістики та появи нових видів кримінальних правопорушень, змінення способів їх вчиненя, та злочинних технологій зокрема, тому все це потребує застосування нових інформаційних технологій при розслідуванні. Якщо говорити в науковому напрямку, варто зазначити про появу нових галузей (судових наук), а саме: «Цифрової криміналістики», воєнної криміналістика, ядерної криміналістика та ін. Ці галузі є наслідком технологічного прогресу та еволюції суспільства та повинні відображати світові тенденції та можливості впровадження інноваційних підходів у практику протидії злочинності.[1]

Тому, інновації в криміналістиці сьогодні охоплюють всю систему криміналістичних знань, і виходячи з розширення предмету науки, до інноваційних продуктів сьогодні відносять інноваційні розробки та нові підходи у галузях криміналістичної техніки, тактики та методики розслідування окремих видів кримінальних правопорушень.

Предметом дослідження наразі є засоби криміналістичної тактики в умовах цифровізації, яким притаманний динамічний характер. Як вже зазначалось вище, злочинні технології змінюються та ускладняються, підлаштовуються до нових умов, тому й ефективність застосування засобів криміналістичної тактики передбачає їх удосконалення, упровадження новітніх розробок, наукового обґрунтування [2, С.172].

В традиційному розумінні, засоби криміналістичної тактики це – певні інструменти тактико–криміналістичного спрямування, якими користується слідчий, детектив, прокурор, оперативний працівник, адвокат, суддя (суд), застосування яких дає їм змогу успішно вирішувати тактичні завдання, які виникають на кожному з етапів кримінального провадження з урахуванням особливостей події кримінального правопорушення, що розслідується або розглядається в суді, слідчих і судових ситуаціях, чинників–детермінантів, що впливають на вибір та доцільність застосування тих чи інших різновидів тактичних засобів і їх систем [3, с. 545].

Відповідно, у цифрову епоху відбувається трансформація засобів криміналістичної тактики, їх технічна складова переважає та стає домінуючою, як наслідок зростає та підвищується роль аналітичних та цифрових інструментів, які сьогодні є інструментом організації, планування та проведення слідчих (розшукових дій).

Традиційно в криміналістичній науці систему засобів криміналістичної тактики утворюють наступні елементи: тактичний прийом, тактична рекомендація, тактична комбінація, тактична операція, тактика слідчої (розшукової) дії, тактика негласної слідчої (розшукової) дії, тактика взаємодії слідчого та інших учасників провадження, які спрямовані підвищувати ефективність тактичного планування та прийняття процесуальних рішень.

Виходячи з предмету нашого дослідження, можна виділити такі основні напрями впливу цифрових технологій на систему засобів криміналістичної тактики:

Трансформація інформаційної основи криміналістичної тактики – говорить про те, що значний обсяг криміналістично значущої інформації сьогодні існує у цифровій формі, а саме: листування у месенджерах, метадані файлів, геолокаційні дані, записи камер відеоспостереження, інформація із соціальних мереж і т.д.;

Використання технологій штучного інтелекту та аналітичних систем – застосовуються сьогодні в багатьох інституціях і в діяльності з розслідування зокрема, де алгоритми штучного інтелекту (ШІ) та системи Big Data дозволяють: аналізувати великі масиви даних, встановлювати зв’язки між особами, автоматизувати пошук доказової інформації та інше;

Модернізація тактики слідчих (розшукових) дій, адже весь типовий тактичний комплекс цифрові технології сьогодні доповнюють та трансформують, наприклад при допиті використання відеофіксації, дистанційних комунікацій, якщо говорити про обшук – пошук цифрових носіїв, хмарних сховищ, мобільних пристроїв, при огляді місця події – 3D– фіксація на місці події, застосування дронів, цифрового моделювання, тощо;

Розширення можливостей тактичних комбінацій – а саме інтеграція OSINT–технологій, цифрової аналітики та автоматизованих баз даних сприяє формуванню нових комплексів тактичних засобів;

Зміна характеру кримінальної протидії – полягає в тому, що характер злочинних технологій з впливом цифровізації суспільства теж зазнає змін, сьогодні злочинці активно використовують: шифрування даних, анонімізацію, VPN та TOR, – мережі, самознищуванні повідомлення та інше. Всі ці аспекти потребують розроблення нових тактичних рішень щодо подолання цифрової протидії розслідуванню.

Посилення ролі міждисциплінарної взаємодії – обумовлена тим, що реалізація сучасних тактичних засобів дедалі більше залежить від співпраці слідчого зі спеціалістами у сфері: цифрової криміналістики, кібербезпеки, комп'ютерно – технічної експертизи, телекомунікацій та інших інституцій.

Таким чином, вплив цифрових технологій на систему засобів криміналістичної тактики має комплексний характер і проявляється у трансформації традиційних тактичних прийомів, формуванні нових цифрово орієнтованих засобів. У сучасних умовах ефективність засобів криміналістичної значною мірою визначається здатністю інтегрувати цифрові технології у практику досудового розслідування з дотриманням процесуальних гарантій та вимог допустимості доказів.

Перелік використаних джерел:

1.Шепітько В.Ю. Інноваційні методи та технології цифрової криміналістики в розслідуванні воєнних злочинів. Criminalistics and Forensic Exspertology: Science, Studies, Practice. Vilnius, Brno, 2023. P. 67.

2.Шепітько В.Ю. Засоби криміналістичної тактики в діяльності органів досудового слідства (проблеми ефективності застосування). Правові засади підвищення ефективності боротьби зі злочинністю в Україні: матеріали наук. конф., 15 трав..2008 р. Харків, 2008. С. 172–174.

3.Криміналістика: підручник / [В.М.Шевчук, В.А. Журавель, В.Ю. Шепітько та ін.]; за ред. В.М. Шевчука; Нац. Юрид. ун–т ім. Ярослава Мудруго. – Харків: Право, 2024. – 1008 с.

DOI https://doi.org/10.32837/11300.33619

Кузнецова Людмила
аспірант кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0001–1782–8264
e–mail: kuznetsova@onua.edu.ua

ЩОДО ДОЦІЛЬНОСТІ ЗГАДКИ ЕКОНОМІЧНОГО ДОБРОБУТУ У ВИПАДКАХ ВИНЕСЕННЯ РІШЕННЯ ПРО СКЛАДАННЯ ДОСУДОВОЇ ДОПОВІДІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У тезах досліджуються проблеми нормативного закріплення категорії «економічний добробут» як підстави для складення досудової доповіді відповідно до ч. 5 ст. 314 КПК України, а також аналізуються практичні аспекти її застосування судами. Обґрунтовується висновок про декларативний характер відповідної законодавчої конструкції та пропонується виключити із ч. 5 ст. 314 КПК України вказівку на «національну безпеку» та «економічний добробут», залишивши орієнтацію на забезпечення прав людини як основну мету складення досудової доповіді.

Ключові слова: кримінальне провадження, досудове доповідь, економічний добробут, суд, підготовче провадження

Kuznetsova Liudmyla
Postgraduate student of the Department of Criminal Procedure,
National University «Odesa Law Academy»,
Odesa, Ukraine

ON THE EXPEDIENCY OF MENTIONING ECONOMIC WELL–BEING IN CASES OF MAKING A DECISION TO DRAW UP A PRE–TRIAL REPORT IN CRIMINAL PROCEEDINGS

The theses examine the problems of normative consolidation of the category of «economic well–being» as a basis for drawing up a pre–trial report in accordance with Part 5 of Article 314 of the Code of Criminal Procedure of Ukraine, and also analyze practical aspects of its application by courts. The conclusion about the declarative nature of the relevant legislative construction is substantiated and it is proposed to exclude from Part 5 of Article 314 of the Code of Criminal Procedure of Ukraine the indication of «national security» and «economic well–being», leaving the orientation on ensuring human rights as the main goal of drawing up a pre–trial report.

Keywords: criminal proceedings, pre–trial report, economic welfare, court, preparatory proceedings

Відповідно до ч. 5 ст. 314 КПК України, «у підготовчому судовому засіданні суд у випадках, передбачених цим Кодексом, за власною ініціативою або за клопотанням обвинуваченого, його захисника чи законного представника, чи за клопотанням прокурора і лише в інтересах національної безпеки, економічного добробуту та прав людини вирішує питання щодо складання досудової доповіді, про що постановляє ухвалу із зазначенням строку підготовки такої доповіді» [1]. Хоча згадка про економічний інтерес в цьому випадку виглядає дещо дивно, адже ні в цій, ні в інших статтях не конкретизується, про чий саме економічний добробут ведеться мова та як його необхідно оцінювати. Більше того, формулювання «економічний добробут» згадується між «національною безпекою» та «правами людини», при цьому в ст. 314 КПК України ці категорії перелічуються через кому, що змушує зробити висновок про однорідність цих понять в даному конкретному контексті, хоча однорідність в даному випадку є вкрай умовною, адже ці поняття можливо і перетинаються між собою, проте однозначно не є синонімічними. Це дає змогу зробити висновок, що хоча законодавець і вирішив зробити акцент на економічному добробуті, проте таке уточнення є досить узагальненим.

Представник персоналу органу пробації, складаючи доповідь, дійсно оцінює майновий стан обвинуваченого, проте лише в аспекті оцінки умов життєдіяльності та розвитку. Власне економічні інтереси обвинуваченого не є предметом оцінки, а дослідження майнового стану пов’язано лише з оцінкою можливості виправлення такої особи без застосування до неї покарання. Чи можна стверджувати, що в даному випадку мова йде про економічній добробут (навіть хоча й в масштабах однієї людини – обвинуваченого)? Очевидно що ні. Суд в подальшому буде оцінювати не майнові наслідки призначення покарання для особи, а умови його життя (в тому числі фінансові), які будуть вказувати на можливість в майбутньому вчиняти нові кримінальні правопорушення. Економічній добробут особи точно не буде досліджуватись судом, а тому з впевненістю можемо стверджувати, що в ч. 5 ст. 314 КПК України йде мова про економічний добробут суспільства та держави. Такий саме висновок виходить і з того, що перед цим йде вказівка про національні інтереси, а отже і економічний добробут тут має оцінюватись в масштабах всієї країни.

Проте законодавець не уточнює, що і як саме має оцінюватись. Судді часто використовують дану категорію у своїх рішеннях, проте в переважній більшості випадків вони це роблять тоді, коли цитують ч. 5 ст. 314 КПК України. Реальних прикладів, коли судді оцінюють економічну доцільність складання досудової доповіді, ми не побачили. З однієї сторони можна стверджувати, що це системне порушення з боку суддів, адже вони лише формально виконують вимоги ч. 5 ст. 314 КПК України. Проте такі результати дослідження можуть свідчити про реальну неможливість виконання цих вимог. Нагадаємо, що економічний добробут в даному випадку буде оцінюватись не при заслуховуванні досудової

доповіді і не на етапі прийняття кінцевого судового рішення та призначення покарання. Чи може суддя реально вплинути на економічний добробут держави, призначаючи або не призначаючи складання досудової доповіді? Очевидно що ні. Дійсно, можливо в даному випадку доцільно вести мову про кінцевий результат – можливість призначити особі менше покарання – тобто рішення, яке може бути прийняте в тому числі і за рахунок досудової доповіді. Чи впливає в такому випадку рішення судді на економічний добробут держави? Очевидно що ні. Відповідно до ч. 2 ст. 314–1 КПК України, досудова доповідь складається щодо особи, обвинуваченої у вчиненні нетяжкого або тяжкого злочину, нижня межа санкції якого не перевищує п’яти років позбавлення волі (досудова доповідь щодо неповнолітнього обвинуваченого віком від 14 до 18 років складається незалежно від тяжкості вчиненого злочину, крім випадків, передбачених КПК України). Чи можна стверджувати, що нетяжкі злочини реально впливають на економічний добробут цілої держави? Можливо лише в своїй сукупності, проте така сукупність має бути фантастична за обсягом та кількістю. Дослідження свідчать, що в 25% випадків досудова доповідь взагалі не складається через обставини, які передбачені ч. 4 ст. 314–1 КПК України, з них в 40% випадків доповідь не складається через те, що до моменту її складення суд вже виносить вирок [2]. Таким чином навіть самі судді розуміють, що з метою підвищення ефективності судового розгляду та його пришвидшення краще винести кінцеве рішення, ніж чекати складання досудової доповіді. В такому випадку гарантуються не лише інтереси держави, але і самого обвинуваченого (в тому числі економічні), адже судовий розгляд буде проведено в межах розумного строку, що є нормативною вимогою.

Отже вказівка на економічний добробут як на підставу складення досудової доповіді є зайвою. Можливо на момент внесення змін до КПК України в частині застосування пробації законодавець вважав за потрібне вписати в ст. 314 КПК України мету не стільки досудової доповіді, скільки всієї служби пробації, підкреслюючи її значення як для окремої особи, так і для всієї держави. Ми не маємо права стверджувати, що якісна система пробації не матиме позитивний вплив на національну безпеку та економічний добробут, проте вважаємо, що ці положення радше є декларативними, ніж регулятивними. Тому, задля спрощення КПК України та забезпечення лаконічності та грамотності юридичного тексту пропонуємо прибрати вказівку про те, що досудова доповідь складається «лише в інтересах національної безпеки, економічного добробуту та прав людини», особливо з урахуванням використання імперативного слова «лише», яке є точно зайвим, адже навіть права людини охоплюють фактично всі аспекти здійснення кримінального провадження, а тому фраза «лише в інтересах прав людини» є логічно некоректною. В той же час ми пропонуємо залишити вказівку на права людини, адже це дозволяє підкреслювати значення досудової доповіді, при цьому не обтяжуючи сам юридичний текст.

Перелік використаних джерел:

1. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України. 2013. № 9–10, № 11–12, № 13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651–17

2. Кримінальний процесуальний кодекс України : науково–практичний коментар. Навчальні матеріали онлайн : вебсайт. URL: http://pidruchniki.com/1233090949171/pravo/kriminalniy_protsesualniy_kodeks_ukrayini_naukovo–praktichniy_komentar

DOI https://doi.org/10.32837/11300.33617

Кривда Людмила
доктор філософії (PhD), доцент кафедри кримінального процесу та криміналістики Одеського державного університету внутрішніх справ, Одеса, Україна
ORCID: https://orcid.org/0000–0001–9193–3823
e–mail: liudmyla.kryvda@oduvs.edu.ua

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У РОЗСЛІДУВАННІ НАСИЛЬНИЦЬКИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У тезах розглянуто теоретичні та практичні аспекти застосування спеціальних знань у розслідуванні насильницьких кримінальних правопорушень в Україні. Охарактеризовано основні види судових експертиз та окреслено проблеми їх використання у кримінальному провадженні.

Ключові слова: спеціальні знання, насильницькі кримінальні правопорушення, судова експертиза, досудове розслідування, криміналістика.

Kryvda Liudmyla
Doctor of Philosophy (PhD),
Associate Professor at the Department of Criminal Procedure and Criminalistics
of Odesa State University of Internal Affairs,
Odesa, Ukraine

THE USE OF SPECIAL KNOWLEDGE IN THE INVESTIGATION OF VIOLENT CRIMES: CURRENT STATE AND PROSPECTS FOR DEVELOPMENT

The theses examine theoretical and practical aspects of using special knowledge in the investigation of violent criminal offenses in Ukraine. The main types of forensic examinations are characterized and the problems of their use in criminal proceedings are outlined.

Keywords: special knowledge, violent criminal offenses, forensic examination, pre–trial investigation, criminology.

Розслідування насильницьких кримінальних правопорушень є одним із найскладніших напрямів діяльності правоохоронних органів. Ефективне встановлення обставин таких злочинів неможливе без залучення фахівців різних галузей знань та проведення судових експертиз. Як зазначають Бондар В., Горєлкіна К. та ін., практично кожне кримінальне провадження щодо

насильницьких кримінальних правопорушень здійснюється із застосуванням спеціальних знань [1].

Спеціальні знання у кримінальному процесі – це знання, що не є загальновідомими і якими володіє обмежене коло фахівців. Їх використання у досудовому розслідуванні ґрунтується передусім на залученні до процесу розслідування спеціаліста та експерта – осіб, які є носіями таких спеціальних знань та навичок. Зазначені знання визначають процесуальний та правовий статус учасників кримінального провадження, впливають на формування їхніх прав і обов'язків, систему гарантій та умов діяльності під час розслідування кримінальних правопорушень.

Серед основних форм використання спеціальних знань у кримінальному провадженні провідне місце посідає судова експертиза. Відповідно до Закону України «Про судову експертизу», судова експертиза – це дослідження, яке проводиться експертом на підставі спеціальних знань матеріальних об'єктів, явищ і процесів, що містять інформацію про обставини справи, яка перебуває у провадженні органів досудового розслідування або суду.

У ході розслідування насильницьких кримінальних правопорушень може призначатися широкий спектр судових експертиз. Провідне місце серед них займає судово–медична експертиза, яка проводиться у 92% кримінальних проваджень зазначеної категорії. Вона дозволяє встановити характер і ступінь тяжкості тілесних ушкоджень, вік та механізм їх заподіяння, вид і тип зброї, що застосовувалась. Крім того, у відповідних ситуаціях призначаються: судово–психіатрична та судово–психологічна (у 27% проваджень); судово–біологічна; трасологічна та дактилоскопічна; балістична; експертиза холодної зброї; генотипоскопічна (ДНК–аналіз).

Особливої уваги заслуговує молекулярно–генетична експертиза, можливості якої постійно розширюються. Метод ДНК–аналізу дозволяє ідентифікувати особу на рівні індивідуально–специфічної тотожності, що є надзвичайно цінним при розслідуванні серійних кримінальних правопорушень та у випадках, коли інші докази є недостатніми. Подальший розвиток генотипоскопічної експертизи пов'язаний із вдосконаленням методу ДНК–аналізу для діагностики властивостей і стану людини за її слідами.

Незважаючи на широкі можливості сучасних судових експертиз, практика свідчить про їх недостатнє використання. За результатами опитування, 78% слідчих і експертів вказують на неповне застосування досягнень науки й техніки при розслідуванні кримінальних правопорушень. Зокрема, судово–біологічна експертиза, яка дозволяє вирішити велику кількість спірних питань при наявності фізичного контакту злочинця з жертвою, призначається лише у 8% проваджень. Це пояснюється недооцінкою її можливостей та специфікою виявлення, вилучення й фіксації речових доказів відповідної категорії.

Таким чином, ефективне розслідування насильницьких кримінальних правопорушень потребує комплексного застосування різних видів судових

експертиз. Теоретичні й методологічні основи таких досліджень потребують постійного оновлення та адаптації до новітніх технологій і кращого світового досвіду. Підвищення рівня обізнаності слідчих та прокурорів щодо можливостей сучасних судово–експертних досліджень є необхідною умовою підвищення ефективності досудового розслідування насильницьких кримінальних правопорушень в Україні.

Перелік використаних джерел:

1.Бондар В. О., Горєлкіна К. В., Кривда Л. М., Назарук О. М., Матюшкова Т. П. Використання спеціальних знань у розслідуванні насильницьких кримінальних правопорушень. Cuestiones Políticas. 2023. Vol. 41, № 76. С. 241–258. DOI: https://doi.org/10.46398/cuestpol.4176.13

2.Закон України «Про судову експертизу» від 25.02.1994 № 4038–XII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon2.rada.gov.ua/laws/show/4038–12

3.Кримінальний процесуальний кодекс України від 13.04.2012 № 4651–VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon3.rada.gov.ua/laws/show/4651–17

4.Кривда Л. М., Кривда Р. С. Генезис криміналістичних знань та напрями їх використання при розслідуванні насильницьких кримінальних правопорушень і злочинів з корисливих мотивів. Юридичний вісник. 2021. № 2. С. 133–145.

DOI https://doi.org/10.32837/11300.33620

Максимчук Іван
доктор філософії, викладач кафедри криміналістики та судової медицини
Національної академії внутрішніх справ,
м. Київ, Україна
ORCID: https://orcid.org/0009–0002–5246–6315
e–mail: maksymum@ukr.net

ВПЛИВ ПРЕДМЕТУ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ НА ФОРМУВАННЯ СТАТИСТИЧНИХ ПОКАЗНИКІВ ЗА ОКРЕМИМИ ВИДАМИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У тезах розглянуто комплексну теоретико–правову проблему реагування та протидії кримінальним правопорушенням, які пов’язані з незаконним обігом небезпечних хімічних (отруйних) речовин в Україні. Проаналізовано статистичні дані, які відображають фактичний стан протидії таким правопорушенням та акцентовано увагу на удосконаленні судово–експертної діяльності за даним напрямком, взаємодії правоохоронних органів і запровадженні сучасних криміналістичних методів, спрямованих на документування окремих видів злочинів, які становлять реальні загрози для здоров’я та життя.

Ключові слова: отруйна речовина, небезпечна хімічна речовина, отруйна хімічна речовина, криміналістична експертиза сильнодіючих речовин, судова експертиза.

Maksymchuk Ivan
PhD, Lecturer of the Department of Criminalistics and Forensic Medicine,
National Academy of Internal Affairs,
Kyiv, Ukraine

THE INFLUENCE OF THE SUBJECT OF FORENSIC RESEARCH ON THE FORMATION OF STATISTICAL INDICATORS FOR CERTAIN TYPES OF CRIMINAL OFFENSES

The theses examine a comprehensive theoretical and legal issue of response to and counteraction against criminal offenses related to the illicit trafficking of dangerous chemical (poisonous) substances in Ukraine. Statistical data reflecting the actual state of combating such offenses are analyzed, and attention is focused on improving forensic expert activity in this field, enhancing cooperation among law enforcement agencies, and implementing modern forensic methods aimed at documenting certain types of crimes that pose real threats to human health and life.

Keywords: poisonous substance, dangerous chemical substance, poisonous chemical substance, forensic examination of potent substances, forensic expertise.

Так, норми статті 321 Кримінального кодексу України передбачають відповідальність за незаконне виробництво, виготовлення, придбання, перевезення, пересилання, зберігання з метою збуту або збут отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів.

За статистичними даними Офісу Генерального прокурора України за 2025 рік обліковано 411 злочинів, передбачених статтею 321 КК України, за 2024 – 575, за 2023 рік – 393 злочини, протягом 2022 – 247, за 2021 рік обліковано таких злочинів – 474, за 2020 рік – 335, за 2019 рік – 328 та за 2018 рік – 267 [1].

Однак, як нами раніше зазначалося, скасування Переліку отруйних речовин та відсутність нормативно–правового закріплення їх поняття призвело до того, що органи досудового розслідування вносять до Єдиного реєстру досудових розслідувань (далі – ЄРДР) відомості про злочини, пов'язані з незаконним обігом отруйних речовин не завжди з кримінально–правовою кваліфікацією за статтею 321 КК України в частині визначення предметом злочину саме отруйних речовин [2, с. 316 – 324].

Так, за даними Національної поліції України, протягом 2018 року зареєстровано сім кримінальних проваджень, де предметом посягання стали отруйні речовини, протягом 2019 та 2020 років – по дев'ять таких фактів, у 2021 році – шість, за 2022 рік – п'ять кримінальних проваджень, у 2023 – сім, протягом 2024 року – п'ять, а за 2025 рік, увага – на території держави Україна не зареєстровано жодного кримінального правопорушення, де предметом посягання стали отруйні речовини [3].

На наше переконання, такі статистичні дані можуть свідчити лише про недостатній рівень криміналістичного забезпечення досудового розслідування кримінальних правопорушень згаданої категорії, чому сприяють, зокрема, розбіжності та суперечності між юридичними термінами та нормативно–правовими актами. А в загальному розумінні, при об'єктивній оцінці злочинної діяльності, яка проявляється у незаконному поводженні з отруйними речовинами та, безперечно, має ризик подвійного трактування одних і тих самих термінів, такий стан можна оцінювати як правовий дисбаланс у сфері поводження з отруйними хімічними речовинами.

Визначення терміну «отруйні речовини», як це вказано у статті 321 КК України [4], наведено в Інструкції про розгляд заявок та надання дозволів на виробництво, зберігання, транспортування, використання, захоронення, знищення та утилізацію отруйних речовин, у тому числі продуктів біотехнології та інших біологічних агентів, яка затверджена Наказом Міністерства екології та природних ресурсів України від 30.07.2002 за № 294 (далі – Наказ № 294), де зазначено, що отруйні речовини – це небезпечні хімічні речовини та сполуки індивідуальні за своїм складом, суміші хімічних речовин та сполук, продукти їх розкладу та розпаду, які за сукупністю притаманних їм властивостей створюють або можуть створити небезпеку для довкілля, тварин та здоров'я людей, що може привести до

загибелі об'єктів довкілля, тварин та людей, і, які потребують спеціальних методів, умов і засобів поводження з ними [5].

У даному випадку слід звернути увагу, що Наказ № 294 визначає отруйні речовини саме як «хімічні», тому фактор небезпеки нами розглядається з позиції саме хімічних речовин.

Натомість, Закон України «Про забезпечення хімічної безпеки та управління хімічною продукцією» від 01.12.2022 пропонує досить ширше коло з визначенням термінів, які більш детальніше, об'єктивніше розкривають, тлумачать та розмежовують поняття небезпечності «отруйних» (небезпечних хімічних) речовин» де, наприклад, зазначено, що: небезпечна хімічна речовина (хімічна продукція) – хімічна речовина (хімічна продукція), що потенційно може завдати шкоду здоров'ю людини та/або довкіллю; отруйна хімічна речовина – небезпечна хімічна речовина, яка може спричинити виникнення гострого або відстроченого тяжкого отруєння, яке призводить до хвороб, порушення роботи систем організму або його загибелі, у разі її перорального надходження, потрапляння на шкіру або під час вдихання; особливо небезпечна хімічна речовина – небезпечна хімічна речовина, яка має мутагенні та/або канцерогенні властивості, та/або є токсичною для репродуктивної системи людини, та/або має здатність до руйнування ендокринної системи людини, та/або є стійкою, біоакумулятивною і токсичною для довкілля [6].

Врахування зазначених особливостей законодавства повинне відіграти визначальну роль під час розгляду питання про внесення змін, які, на нашу думку, вже давно назріли та прямо підштовхують до активних дій законодавця, як до Кримінального кодексу України, зокрема до статті 321, так і до основного в даному питанні наказу Міністерства юстиції України від 08.10.1998 № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково–методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень», зокрема у частині визначення такого підвиду криміналістичної експертизи, як «криміналістична експертиза сильнодіючих і отруйних речовин», де однозначним, на нашу думку, є, перш за все, виокремлення такої експертизи в окремі підвиди, тобто окремо має бути криміналістична експертиза сильнодіючих речовин, до яких переважно відносяться сильнодіючі лікарські засоби, та, окремо, криміналістична експертиза «отруйних речовин».

Однак при цьому, зважаючи на положення Закону України «Про забезпечення хімічної безпеки та управління хімічною продукцією» [6], пропонується розглянути питання щодо запровадження абсолютно нового підвиду криміналістичної експертизи матеріалів, речовин та виробів, а саме, наприклад, такого її підвиду як «криміналістична експертиза отруйних хімічних речовин».

У даному випадку слід враховувати, що термін «отруйна хімічна речовина» поглинає у своєму розумінні такі визначення (терміни) як: небезпечна хімічна

речовина (хімічна продукція) та особливо небезпечна хімічна речовина, на яких зосереджено увагу вище.

Водночас слід брати до уваги фактор небезпечності, який у даному випадку розглядається у призмі негативного впливу саме на організм людини, завдання йому шкоди та спричинення непрогнозованих наслідків у подальшому, у т.ч. і для наступних поколінь (токсичність для репродуктивної системи людини).

Разом з цим, зважаючи на положення Постанови Кабінету Міністрів України від 2 липня 2008 р. № 595 «Про затвердження Порядку атестації та державної реєстрації методик проведення судових експертиз» [7], виникають підстави для розроблення та впровадження абсолютно нових та, без перебільшення, новітніх методик проведення судових експертиз, у тому числі і з застосуванням цифрових інновацій, штучного інтелекту, що сприятиме об’єктивному встановленню істини при розслідуваннях кримінальних правопорушень, пов’язаних з незаконним обігом небезпечних хімічних (отруйних) речовин.

Перелік використаних джерел:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: Офіс Генерального прокурора: [сайт]. URL: https://new.gp.gov.ua/ua/posts/statistika.

2. Максимчук І.М. Отруйні речовини як елемент криміналістичної характеристики окремих кримінальних правопорушень. Науковий вісник публічного та приватного права. Вип. 4, том 1, 2019. С. 316 – 324. URL: https://nvppp.in.ua/vip/2019/4/tom_1/54.pdf.

3. Звіт про окремі види злочинів, пов’язаних із небезпечними матеріалами за 12 місяців 2018 – 2025 років (форма № 1–НМ) : Наказ Національної поліції України від 19.06.2019 р. № 589.

4. Кримінальний кодекс України від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text (дата звернення: 22.05.2026).

5. Наказ Міністерства екології та природних ресурсів України від 30.07.2002 за № 294 «Про затвердження Інструкції про розгляд заявок та надання дозволів на виробництво, зберігання, транспортування, використання, захоронення, знищення та утилізацію отруйних речовин, у тому числі продуктів біотехнології та інших біологічних агентів». URL: https://zakon.rada.gov.ua/laws/show/z0781–02/ed20020925/find?text=%CE%F2%F0%F3%E9%ED%B3+%F0%E5%F7%EE%E2%E8%ED%E8#Text

6. Закон України «Про забезпечення хімічної безпеки та управління хімічною продукцією» від 01.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2804–20#Text (дата звернення: 22.05.2026).

7. Постанова Кабінету Міністрів України від 2 липня 2008 р. № 595 «Про затвердження Порядку атестації та державної реєстрації методик проведення судових експертиз». URL: https://zakon.rada.gov.ua/laws/show/595–2008–%D0%BF#n11

DOI https://doi.org/10.32837/11300.33621

Мунтяну Юліан
аспірант кафедри криміналістики, судових експертиз та поліграфології,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна, ORCID: 0009-0005-0684-2481,
e–mail: muntianu.yulian@gmail.com

АНАЛІЗ ВІДКРИТИХ ДЖЕРЕЛ У ДІЯЛЬНОСТІ З РОЗСЛІДУВАННЯ ЗАХОПЛЕННЯ ТА УМИСНОГО ВБИВСТВА ЗАРУЧНИКІВ

У тезах розглянуто використання аналізу відкритих джерел інформації та методів OSINT під час розслідування захоплення та умисного вбивства заручників. Наведено можливості використання інформації відкритих джерел для встановлення обставин вчинення злочину.

Ключові слова: відкриті джерела, розслідування, захоплення заручників, умисне вбивство, OSINT, цифрові сліди.

Muntianu Yulian
Postgraduate Student of the Department of Criminalistics, Forensic Examinations, and Polygraphology, National University «Odesa Law Academy», Odesa, Ukraine

OPEN SOURCE INTELLIGENCE IN THE INVESTIGATION OF HOSTAGE-TAKING AND INTENTIONAL MURDER

The abstract explores the use of open-source information analysis and OSINT methods in the investigation of hostage-taking and the intentional killing of hostages. It outlines the potential of using information from open sources to establish the circumstances of the committed crime.

Key words: open sources, investigation, hostage-taking, intentional killing, OSINT, digital traces.

Сучасні умови суцільної цифровізації вимагають від правоохоронних органів використання інноваційних методів розслідування кримінальних правопорушень. Водночас, захоплення заручників та їх подальше умисне вбивство часто супроводжується значним суспільним резонансом та широким медійним розголосом. У цьому контексті аналіз відкритих джерел із використанням методології OSINT стає критично важливим інструментом криміналістичного забезпечення розслідування такої категорії злочинів та їх швидкого розкриття.

Відомості щодо обставин вчинення особливо резонансного злочину можуть поширюватись соціальними мережами та засобами масової інформації з перших хвилин його вчинення, а профіль злочинця та його дописи є основою для

складання психологічного портрету, встановлення зв'язків з іншими співучасниками, аналізу та доведення мотивів і мети вчинення правопорушення тощо.

Одним з прикладів стрімкого розповсюдження у відкритих джерелах інформації щодо вчинення злочину є події 18 квітня 2026 року у Голосіївському районі м. Києва. Нападник відкрив вогонь з карабіна по перехожих, після чого забарикадувався в супермаркеті із заручниками, а в подальшому був ліквідований спецпризначенцями після вбивства ним одного з заручників [1].

Ще до початку поліцейської операції, новинними каналами у мессенджері Telegram поширювались дописи та відеозаписи цих подій, зафіксовані очевидцями, в тому числі із зображенням особи злочинця.

В подальшому також і сторінки та дописи нападника у соціальних мережах стали окремим предметом дослідження правоохоронних органів для встановлення мотивів вчинення злочину [2].

За таких обставин, саме з відкритих джерел інформації на початкових етапах розслідування злочину слідчі та оперативні органи мають можливість отримати первинні дані для встановлення обставин злочину, особи злочинця, та засобів які використовуються для його вчинення.

Таким чином, використання методології OSINT під час розслідування злочинів є майже обов'язковим елементом роботи слідчо-оперативної групи.

OSINT (open source intelligence – розвідка відкритих баз даних) у світовій спільноті визначається як розвідка інформації, отриманої із загальнодоступних джерел, яка не потребує таємних методів збору, а також включає в себе обробку даних та оцінку їх надійності. Аналіз отриманої з відкритих джерел інформації є ключовим етапом розвідки відкритих джерел і полягає у поглибленому дослідженні значення та суттєвих характеристик наявної інформації [3, с. 9-11].

Методи розвідки та аналізу відкритих джерел вже ефективно використовуються іноземними правоохоронними органами для забезпечення досягнення результатів у розслідувані злочинів [4].

Ефективність розслідування злочинів, пов'язаних із захопленням та умисним вбивством заручників, в першу чергу залежить від швидкості ідентифікації суб'єктів його вчинення та визначення локації перебування потерпілих. Використання методів штучного інтелекту для аналізу відеозаписів, фотознімків та повідомлень у месенджерах та засобах масової інформації дозволяє отримати відомості як безспосередньо щодо обставин злочину, так і виявити приховані метадані (геолокацію, час зйомки, параметри пристрою), що може бути цифровим ключем для ідентифікації особистості очевидця, потерпілого та злочинця.

Також напрямами використання відкритих джерел у розслідуванні захоплення заручників можуть бути:

- моніторинг соціальних мереж для встановлення зв'язків між імовірними злочинцями та вивчення їхньої психологічної характеристики;

- геопросторовий аналіз, що включає співставлення візуальних маркерів із відеоматеріалів та фотоматеріалів із супутниковими знімками місцевості;
- аналіз цифрових слідів, залишених у мережі Інтернет під час висування вимог– як інструмент додаткової ідентифікації особи злочинця.

Слід зазначити, що документування злочинів у цифровий час з використанням розвідки та аналізу відкритих джерел потребує дотримання суворих протоколів збереження цілісності даних. В свою чергу, інтеграція OSINT-технологій у традиційну методику розслідування дозволяє не лише ефективно забезпечувати виконання завдань кримінального провадження, а й попереджати фатальні наслідки для заручників за рахунок випереджального аналізу дій злочинців.

Перелік використаних джерел:

1. У Києві озброєний чоловік захопив заручників у житловому будинку: що відомо. Українська правда. 2026. 18 квіт. URL: https://www.pravda.com.ua/news/2026/04/18/8030739/
2. Теракт у Києві 18 квітня: побутовий конфлікт міг стати причиною трагедії. NV.ua. 2026. 18 квіт. URL: https://nv.ua/ukr/ukraine/events/terakt-u-kiyevi-18-kvitnya-pobutoviy-konflikt-mig-stati-prichinoyu-tragediji-50602406.html
3. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса: Видавництво «Юридика», 2024. 180 с.
4. Каландирець Я. М., Тітко І. А. Використання методик OSINT у межах розслідування кримінальних правопорушень: успішні кейси у практиці іноземних правоохоронних органів та інститутів громадянського суспільства. *Аналітично-порівняльне правознавство*. 2026. Вип. 2. Ч. 3. С. 95-101. URL: https://journal-app.uzhnu.edu.ua/article/view/358390/344258

DOI https://doi.org/10.32837/11300.33553

Нечипорук Володимир
аспірант кафедри кримінального процесу
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID: https://orcid.org/0009–0009–2232–8983
e–mail:criminal_process@onua.edu.ua

ДИСТАНЦІЙНІ ДОПИТИ УЧАСНИКІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ У ФОКУСІ ПРАВОВИХ ПОЗИЦІЙ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

Тези присвячено питанням відповідності дистанційних допитів учасників кримінального провадження стандартам ст. 6 Конвенції про захист прав людини та основоположних свобод. Проаналізовано низку рішень ЄСПЛ з релевантним контекстом. Сформульовано загальні критерії відповідності дистанційних допитів стандартам права на справедливий суд.

Ключові слова: кримінальне провадження, дистанційний допит, судове провадження, рішення ЄСПЛ.

Nechyporuk Volodymyr
Postgraduate Student of the Department of Criminal Process,
National University «Odesa Law Academy»,
Odesa, Ukraine

REMOTE EXAMINATION OF PARTICIPANTS IN CRIMINAL PROCEEDINGS IN THE FOCUS OF THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

The theses are devoted to the issues of compliance of remote examinations of participants in criminal proceedings with the standards of Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms. A number of judgments of the European Court of Human Rights within the relevant context have been analysed. General criteria for the compliance of remote examinations with the standards of the right to a fair trial have been formulated.

Keywords: criminal proceedings, remote examination, judicial proceedings, judgments of the European Court of Human Rights.

Стрімка цифровізація кримінального провадження закономірно обумовлює розширення практики використання дистанційних форм здійснення процесуальних дій, серед яких особливе місце займають дистанційні допити осіб. У сучасних умовах саме такі процедури дедалі частіше розглядаються як необхідний інструмент забезпечення оперативності кримінального провадження, процесуальної економії та безперервності здійснення правосуддя. Їх

затребуваність істотно зросла внаслідок пандемії COVID–19, однак особливої актуальності відповідна проблематика набула після запровадження в Україні правового режиму воєнного стану.

Повномасштабна збройна агресія проти України суттєво ускладнила можливість безпосередньої участі учасників кримінального провадження у проведенні слідчих (розшукових) та судових дій. Перебування осіб на тимчасово окупованих територіях, їх вимушене переміщення як за кордон, так і в межах країни, постійні ризики для життя і здоров'я та необхідність забезпечення безпеки учасників процесу обумовили об'єктивну потребу у ширшому застосуванні дистанційних допитів із використанням відеоконференцзв'язку та інших цифрових технологій.

Законодавець вживав спеціальних заходів щодо унормування цього аспекту. Зокрема, ч.1 ст. 336 КПК України окремо було доповнено пунктом 4–1, відповідно до якого судове провадження може здійснюватися у режимі відеоконференції під час трансляції з іншого приміщення, у тому числі яке знаходиться поза межами приміщення суду (дистанційне судове провадження), у разі введення воєнного стану або під час карантину, встановленого Кабінетом Міністрів України. Водночас, розширення можливостей використання таких процедур актуалізує питання їх відповідності фундаментальним гарантіям справедливого судового розгляду.

Насамперед йдеться про стандарти ст. 6 Конвенції про захист прав людини і основоположних свобод, сфера якої охоплює право особи на ефективну участь у провадження, право на захист, а також можливість безпосереднього допиту свідків. Саме тому, особливого значення у цьому контексті набуває практика ЄСПЛ, у якій поступово формуються критерії відповідності дистанційних процедур зазначеним стандартам.

ЄСПЛ розглядав релевантні питання у низці справ.

Так, наприклад, у рішенні Marcello Viola v. Italy заявник стверджував, що його участь у кримінальному провадженні через відеоконференцію порушила гарантії справедливого судового розгляду, оскільки дистанційний формат створив труднощі для реалізації права на захист. ЄСПЛ звернув увагу на те, що використання відеоконференції прямо передбачалося італійським законодавством, переслідувало легітимні цілі, пов'язані із забезпеченням громадської безпеки, протидією мафії, захистом свідків та дотриманням розумних строків кримінального провадження. Суд також підкреслив, що заявник мав можливість бачити й чути всіх учасників процесу, робити заяви суду та конфіденційно спілкуватися із захисником. У підсумку ЄСПЛ не констатував порушення ст. 6 Конвенції, оскільки дистанційний формат участі не поставив сторону захисту у суттєво невигідне становище та не позбавив заявника можливості ефективно брати участь у провадженні [1].

У рішенні Sakhnovskiy v. russia заявник також стверджував, що його участь у касаційному розгляді через відеоконференцію у поєднанні з неналежною правовою допомогою позбавила його можливості ефективно захищати себе. ЄСПЛ звернув увагу на те, що заявнику було призначено адвоката безпосередньо перед слуханням, а час для конфіденційного спілкування із захисником був явно недостатнім з огляду на складність справи. Суд наголосив на тому, що система відеоконференції не гарантувала належного рівня конфіденційності комунікації між заявником та адвокатом, а держава не вжила компенсаторних заходів для мінімізації обмежень дистанційного формату провадження. У результаті ЄСПЛ констатував порушення ст. 6 § 1 та ст. 6 § 3 (c) Конвенції, оскільки заявник фактично був позбавлений ефективної правової допомоги [2].

У рішенні Yevdokimov and Others v. russia заявники стверджували, що їхня неможливість особисто брати участь у судових засіданнях позбавила їх права на справедливий судовий розгляд. ЄСПЛ звернув увагу на те, що національні суди формально відмовили заявникам в участі у провадженні, посилаючись на положення внутрішнього законодавства, однак не оцінили, чи вимагав характер спору їхньої особистої присутності та чи могли бути застосовані альтернативні процесуальні механізми, зокрема відеоконференція, судове доручення або представництво. Суд зазначив, що держава зобов'язана забезпечити такі процесуальні гарантії, які дозволять особі ефективно представляти свою позицію у суді. У підсумку ЄСПЛ констатував порушення ст. 6 Конвенції, оскільки заявників фактично позбавили можливості ефективної участі у провадженні, а національні суди не забезпечили належних компенсаційних процесуальних гарантій. Аналізоване рішення Суду є доволі знаковим, оскільки закладає вкрай важливий стандарт у розглядуваному контексті: чим більше показання ґрунтуються на власному досвіді заявника, тим більше зростає необхідність його усної та безпосередньої участі у провадженні [3].

Таким чином, практика ЄСПЛ свідчить про те, що дистанційний судовий розгляд сам по собі не розглядається як несумісний зі стандартами ст. 6 Конвенції. Вирішальне значення для Суду має не стільки сам формат дистанційної участі, скільки те, чи забезпечує він ефективну участь особи у провадженні та чи не ставить сторону захисту у суттєво невигідне становище. При оцінці сумісності дистанційного провадження із гарантіями справедливого судового розгляду ЄСПЛ звертає увагу на наявність легітимної мети використання відеоконференції, можливість особи повноцінно бачити та чути учасників процесу, конфіденційно спілкуватися із захисником та належним чином представляти свою позицію. Водночас, Суд наголошує, що держави зобов'язані забезпечувати належні компенсаційні процесуальні гарантії, особливо у випадках, коли показання особи значною мірою ґрунтуються на її власному досвіді та потребують безпосереднього усного сприйняття судом.

Перелік використаних джерел:

1. Case of Marcello Viola v. Italy (Application № 45106/04): Judgment of the European Court of Human Rights, 5 October 2006. URL: https://hudoc.echr.coe.int/eng?i=001–77246

2. Case of Sakhnovskiy v. russia (Application № 21272/03): Judgment of the Grand Chamber of the European Court of Human Rights, 2 November 2010. URL: https://hudoc.echr.coe.int/eng?i=001–101568.

3. Case of Yevdokimov and Others v. russia (Applications № 27236/05, 44223/05, 53304/07, 40232/11, 60052/11, 76438/11, 14919/12, 19929/12, 42389/12, 57043/12 and 67481/12): Judgment of the European Court of Human Rights, 16 February 2016. URL: https://hudoc.echr.coe.int/eng?i=001–160620

DOI https://doi.org/10.32837/11300.33555

Павзюк Анатолій
доктор філософії в галузі права, доцент кафедри психології,
директор Центру організації освітньої підготовки
та інформаційно–аналітичної роботи
Національного університету «Одеська юридична академія»
м. Одеса, Україна
ORCID ID: https://orcid.org/0009–0008–0924–1333
e–mail: pavzukk@onua.edu.ua

ПСИХОЛОГІЧНИЙ ПРОФІЛЬ ОСОБИ, ЯКА ВЧИНИЛА ПРОТИПРАВНЕ ДІЯННЯ: МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛІСТИЧНОМУ АНАЛІЗІ ПОВЕДІНКИ

У тезах досліджено можливості використання технологій штучного інтелекту для формування психологічного профілю особи, яка вчинила протиправне діяння. Розглянуто значення цифрових слідів, поведінкових моделей, комунікативних ознак та інформаційно–аналітичних систем у криміналістичному аналізі особистості правопорушника. Акцентовано увагу на тому, що штучний інтелект може використовуватися як допоміжний інструмент для виявлення закономірностей поведінки, прогнозування можливих дій особи та оптимізації розслідування кримінальних правопорушень. Підкреслено необхідність поєднання цифрових технологій із професійною оцінкою психолога, криміналіста та слідчого.

Ключові слова: психологічний профіль, штучний інтелект, криміналістичний аналіз, поведінка правопорушника, цифрові сліди, профайлінг, кримінальне провадження.

Pavziuk Anatolii
PhD in Law, Associate Professor of the Department of Psychology,
Director of the Center for Educational Training Organization
and Information–Analytical Activities
National University «Odesa Law Academy»
Odesa, Ukraine

PSYCHOLOGICAL PROFILE OF A PERSON WHO COMMITTED AN UNLAWFUL ACT: POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN FORENSIC BEHAVIORAL ANALYSIS

The theses examine the possibilities of using artificial intelligence technologies to form a psychological profile of a person who has committed an unlawful act. The importance of digital traces, behavioral models, communicative features and

information–analytical systems in forensic personality analysis is considered. It is emphasized that artificial intelligence can be used as an auxiliary tool for identifying behavioral patterns, predicting possible actions of a person and optimizing the investigation of criminal offenses. The need to combine digital technologies with the professional assessment of a psychologist, criminalist and investigator is emphasized.

Keywords: psychological profile, artificial intelligence, forensic analysis, offender behavior, digital traces, profiling, criminal proceedings.

Сучасний розвиток криміналістики, юридичної психології та інформаційно–аналітичної діяльності зумовлює необхідність переосмислення традиційних підходів до вивчення особи, яка вчинила протиправне діяння. Якщо раніше психологічний профіль правопорушника формувався переважно на підставі матеріалів кримінального провадження, результатів допитів, характеристик особи та аналізу слідової картини, то сьогодні значна частина інформації про поведінку людини міститься у цифровому середовищі. Це створює нові можливості для криміналістичного аналізу поведінки, однак водночас потребує обережного та науково обґрунтованого використання технологій штучного інтелекту.

Психологічний профіль особи, яка вчинила протиправне діяння, можна розглядати як систему відомостей про її індивідуально–психологічні риси, мотивацію, емоційні реакції, стиль комунікації, соціальні зв’язки та типові моделі поведінки. У юридичній психології особлива увага приділяється дослідженню девіантної і делінквентної поведінки, а також психології особистості злочинця та злочинних груп [1, с. 94]. Саме ці елементи мають значення для встановлення мотиву протиправної поведінки, способу вчинення діяння та можливих подальших дій особи.

У криміналістичному аспекті психологічний профіль має не лише описове, а й пошукове значення. Він може використовуватися для звуження кола осіб, які могли бути причетними до правопорушення, визначення ймовірної поведінки правопорушника після вчинення діяння, прогнозування його реакції на слідчі дії та побудови тактичної лінії розслідування. Особливо важливим це є у справах, пов’язаних із серійними злочинами, насильницькими правопорушеннями, кіберзлочинністю, організованою злочинністю та діяннями, що мають ознаки ретельної підготовки.

В умовах цифровізації суспільства поведінка особи дедалі частіше залишає інформаційні сліди. До них можна віднести повідомлення в месенджерах, дописи у соціальних мережах, історію пошукових запитів, електронне листування, геолокаційні дані, цифрові транзакції, фото– та відеоматеріали, а також іншу інформацію, яка відображає спосіб життя, коло спілкування та психологічні особливості особи. Як зазначають О. П. Метелев та Є. В. Коваленко, цифрові доказові відомості можуть містити інформацію не лише про осіб, причетних до злочину, а й про зв’язки підозрюваних, місця переховування, предмети та

документи, пов'язані з протиправною діяльністю [2, с. 178]. Отже, цифрові сліди можуть бути важливим джерелом не тільки доказової, а й поведінково–психологічної інформації.

Особливого значення у цьому контексті набуває використання штучного інтелекту. Алгоритми машинного навчання здатні обробляти великі масиви інформації, виявляти повторювані моделі поведінки, встановлювати приховані взаємозв'язки між подіями, особами та комунікаціями. В. М. Шевчук наголошує, що розвиток штучного інтелекту в правоохоронній діяльності пов'язаний із цифровізацією, технологізацією та появою нових завдань криміналістики, спрямованих на підвищення ефективності протидії злочинності [3, с. 356]. Саме тому застосування таких технологій у поведінковому аналізі може стати одним із перспективних напрямів сучасної криміналістики.

У практичному вимірі штучний інтелект може використовуватися під час аналізу текстових повідомлень, дописів у соціальних мережах, аудіовізуальної інформації та моделей онлайн–поведінки. Наприклад, аналіз мовлення і тексту може допомогти виявити ознаки агресивності, тривожності, маніпулятивності, імпульсивності або схильності до ризикованих дій. Аналіз соціальних зв'язків дозволяє визначити роль особи у групі, характер її комунікацій, можливий вплив інших учасників та рівень організованості протиправної діяльності. У цьому аспекті штучний інтелект не формує остаточний висновок про винуватість особи, а лише допомагає виокремити важливі аналітичні ознаки, які потребують подальшої перевірки.

Водночас необхідно враховувати, що використання штучного інтелекту у криміналістичному аналізі поведінки має певні межі. Н. В. Нестор, досліджуючи використання штучного інтелекту у судовій експертизі, звертає увагу на те, що такі технології мають як перспективи, так і ризики, пов'язані з достовірністю результатів, методологічною перевіркою та можливістю помилкової інтерпретації даних [4, с. 86]. Це положення є актуальним і для формування психологічного профілю особи, оскільки алгоритм може помилково оцінити поведінкові ознаки без урахування контексту, соціального середовища, психоемоційного стану та індивідуальних особливостей людини.

Окремої уваги потребує питання використання штучного інтелекту під час досудового розслідування. У наукових тезах, присвячених проблемам застосування штучного інтелекту у кримінальному провадженні, слушно зазначається, що автоматизовані системи доцільно використовувати для обробки великих обсягів даних, розпізнавання образів та аналізу текстів, однак у складних або спірних ситуаціях їх результати мають обов'язково перевірятися людиною [5, с. 42]. Такий підхід є принципово важливим, оскільки психологічний профіль не може бути повністю автоматизованим продуктом. Він повинен формуватися на основі поєднання цифрового аналізу, криміналістичних знань, психологічної оцінки та процесуальних вимог.

Перспективним напрямом є використання штучного інтелекту для криміналістичного прогнозування. Йдеться про можливість аналізу попередньої поведінки особи, її комунікацій, реакцій на зовнішні події, способу підготовки та приховування протиправного діяння. На основі таких даних можуть моделюватися ймовірні подальші дії правопорушника, зокрема спроби уникнути відповідальності, змінити місце перебування, вплинути на свідків, знищити докази або продовжити злочинну діяльність. Однак такі прогнози не можуть мати самостійного доказового значення, а повинні використовуватися лише як орієнтуюча інформація для планування слідчих та розшукових заходів.

Важливим аспектом є також етична сторона застосування штучного інтелекту. Формування психологічного профілю особи на основі цифрових слідів може зачіпати право на приватність, захист персональних даних та презумпцію невинуватості. У монографічних дослідженнях цифровізації кримінального провадження наголошується, що використання цифрових технологій потребує належної правової процедури, гарантій безпеки, конфіденційності та захисту персональних даних [6, с. 64]. Тому використання штучного інтелекту у криміналістичному аналізі поведінки має супроводжуватися чіткими правилами доступу до даних, перевірки результатів та недопущення необґрунтованого втручання у приватне життя особи.

Водночас застосування штучного інтелекту не повинно призводити до підміни професійного мислення фахівця автоматизованими висновками. ШІ може бути корисним інструментом для обробки великих масивів даних, але остаточна оцінка психологічних характеристик особи має здійснюватися людиною. Саме поєднання цифрової аналітики, криміналістичної методики та психологічної компетентності забезпечує найбільш обґрунтований результат.

Таким чином, психологічний профіль особи, яка вчинила протиправне діяння, в умовах цифрової трансформації набуває нового змісту. Він формується не лише на основі традиційних джерел інформації, а й із урахуванням цифрової поведінки, інформаційних слідів та аналітичних можливостей штучного інтелекту. Використання таких технологій може підвищити ефективність криміналістичного аналізу, однак потребує належного правового регулювання, етичного контролю та обов’язкової участі фахівця у перевірці результатів. Штучний інтелект у цій сфері має розглядатися не як заміна психолога, криміналіста чи слідчого, а як інструмент посилення їх професійної діяльності.

Перелік використаних джерел:

1.Демиденко Н. М. Юридична психологія : навчальний посібник. Харків : Харківський національний університет внутрішніх справ, 2025.

2.Метелев О. П., Коваленко Є. В. До питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та

оперативно–розшукової діяльності. Науковий вісник Ужгородського Національного Університету. Серія Право. 2023. Вип. 80. Ч. 2. С. 177–182.

3.Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. Юридичний науковий електронний журнал. 2024. № 6. С. 356–361.

4.Нестор Н. В. Штучний інтелект у судовій експертизі: загроза чи перспектива? Криміналістика і судова експертиза. 2024. № 69. С. 85–88.

5.Алексик Н. Проблемні питання використання штучного інтелекту під час досудового розслідування. Використання цифрових технологій у криміналістиці та судовій експертизі : матеріали науково–практичної конференції. Харків : НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, 2024. С. 40–43.

6.Цифровізація кримінального провадження: стан та перспективи : монографія. Харків : НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, 2024. 174 с.

DOI https://doi.org/10.32837/11300.33558

Паламарчук Олексій
аспірант кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–3354–3215
e–mail:palclifclaimer@gmail.com

ОБСТАНОВКА ВЧИНЕННЯ КВАРТИРНИХ КРАДІЖОК, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ УГРУПОВАННЯМИ

Досліджено особливості обстановки вчинення квартирних крадіжок, учинених організованими злочинними угрупованнями, та її значення для формування криміналістичної характеристики злочину. Визначено основні фактори, що впливають на підготовку, вчинення й приховування крадіжок.

Ключові слова: квартирні крадіжки, організовані злочинні угруповання, обстановка вчинення злочину, криміналістична характеристика, слідова картина.

Palamarchuk Oleksii
postgraduate student of the Department of Criminalistics,
Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

THE SITUATION REGARDING BURGLARIES COMMITTED BY ORGANISED CRIMINAL GANGS

This study examines the specific circumstances surrounding burglaries committed by organized criminal groups and their significance for establishing the forensic profile of the crime. It identifies the key factors influencing the planning, commission and concealment of such burglaries.

Key words: burglaries, organised criminal groups, the circumstances of the offence, forensic profile, evidence at the scene.

Обстановка вчинення квартирних крадіжок, учинених організованими злочинними угрупованнями, є одним із ключових елементів криміналістичної характеристики цього виду кримінальних правопорушень, оскільки саме вона визначає особливості підготовки, реалізації та приховування злочинної діяльності, впливає на механізм утворення слідів, поведінку учасників угруповання та вибір засобів протидії правоохоронним органам. На відміну від поодиноких крадіжок, які часто мають ситуативний або імпульсивний характер, діяльність організованих злочинних угруповань у сфері квартирних крадіжок характеризується

системністю, чітким розподілом ролей, попереднім плануванням та використанням комплексу заходів щодо забезпечення конспірації. У зв'язку з цим обстановка вчинення таких злочинів формується не випадково, а як результат ретельного аналізу злочинцями території, часу, режиму життєдіяльності потерпілих, рівня технічної захищеності житла та можливих ризиків викриття.

У криміналістичному аспекті обстановка вчинення квартирної крадіжки охоплює систему взаємопов'язаних умов і факторів, у межах яких відбувається підготовка, проникнення до житла, викрадення майна та подальше приховування злочину. До таких факторів належать місце вчинення кримінального правопорушення, часові характеристики, соціально–побутові умови, особливості забудови території, технічний стан об'єкта посягання, поведінка мешканців та оточення, наявність охоронних систем, відеоспостереження, консьєржів, сигналізації, а також криміногенна ситуація в конкретному регіоні. Для організованих злочинних угруповань характерним є свідоме використання сприятливих елементів обстановки та нейтралізація факторів, які можуть ускладнювати реалізацію злочинного наміру.

Однією з найбільш характерних ознак обстановки квартирних крадіжок, учинених організованими групами, є ретельний вибір місця вчинення злочину [1]. Найчастіше об'єктами посягання стають квартири заможних осіб, власників бізнесу, громадян, які тривалий час перебувають за межами місця проживання, або осіб, інформація про матеріальне становище яких була попередньо отримана злочинцями. Значну роль у формуванні такої обстановки відіграє проведення попередньої розвідки. Учасники злочинного угруповання вивчають графік перебування мешканців, кількість осіб у квартирі, маршрути їх пересування, наявність охоронних систем, поведінку сусідів, режим роботи камер відеоспостереження та інші фактори, що можуть впливати на успішність проникнення.

Особливу увагу організовані злочинні угруповання приділяють територіальним особливостям району, де планується вчинення крадіжки. Практика свідчить, що злочинці нерідко обирають райони з високою щільністю населення, де постійний рух людей дозволяє маскувати присутність сторонніх осіб. Водночас значна кількість багатоквартирних будинків створює умови для швидкого залишення місця злочину та ускладнює встановлення очевидців. У деяких випадках перевага надається новобудовам, де мешканці ще недостатньо знайомі між собою, що знижує ризик викриття сторонніх осіб у під'їзді. Інколи злочинці, навпаки, обирають старі будинки з низьким рівнем технічного захисту, несправними домофонами або відсутністю відеоспостереження.

Обстановка вчинення квартирних крадіжок також тісно пов'язана з часовими характеристиками. Організовані злочинні угруповання зазвичай обирають періоди, коли ймовірність присутності власників житла є мінімальною. Найчастіше злочини вчиняються у денний час у робочі дні, коли більшість мешканців перебувають на роботі або навчанні. Водночас у святкові та відпускні

періоди поширеними є крадіжки з квартир осіб, які тимчасово виїхали за межі населеного пункту. Для отримання такої інформації злочинці можуть використовувати соціальні мережі, спостереження, контакти у сфері обслуговування або навіть корумповані зв'язки.

Суттєвим елементом обстановки є спосіб проникнення до житла, який безпосередньо залежить від технічних характеристик об'єкта посягання. Організовані групи часто використовують спеціальні інструменти для відкриття замків, дублікати ключів, електронні пристрої для обходу охоронних систем, засоби зв'язку та техніку для блокування сигналізації. У випадках підвищеного ризику застосовуються методи, спрямовані на маскування злочинної діяльності під роботу комунальних служб, кур'єрів або ремонтних бригад. Це створює додаткові умови для безперешкодного проникнення до під'їзду та зменшує підозру з боку мешканців будинку.

Обстановка вчинення квартирних крадіжок організованими угрупованнями нерідко включає використання декількох учасників, які одночасно виконують різні функції. Одні учасники здійснюють безпосереднє проникнення до квартири, інші спостерігають за навколишньою обстановкою, контролюють можливу появу правоохоронців або власників житла, забезпечують транспорт та маршрути відходу. Такий розподіл ролей істотно впливає на слідову картину та дозволяє злочинцям швидко реагувати на зміну ситуації. У криміналістичному аспекті це означає, що обстановка злочину формується не лише умовами місця події, а й організаційною структурою самого угруповання.

Важливою складовою обстановки є використання транспортних засобів. Організовані злочинні угруповання зазвичай використовують автомобілі для оперативного прибуття та швидкого залишення місця вчинення злочину. Нерідко транспортні засоби мають підроблені номерні знаки, орендовані на підставних осіб або належать третім особам, не пов'язаним безпосередньо зі злочинною діяльністю. У деяких випадках застосовуються декілька автомобілів із метою зміни маршруту та ускладнення переслідування. Відповідно, транспортна складова обстановки створює додаткові джерела криміналістично значущої інформації, пов'язаної з камерами відеоспостереження, маршрутами руху, слідами шин та цифровими даними навігаційних систем.

Не менш важливим елементом обстановки є використання сучасних інформаційних технологій. Організовані злочинні угруповання активно застосовують мобільний зв'язок, месенджери, навігаційні сервіси, засоби дистанційного спостереження та інші цифрові інструменти. У деяких випадках злочинці отримують інформацію про потенційних потерпілих через соціальні мережі, фотографії з відпочинку, оголошення про продаж майна або інші відкриті джерела. Це суттєво змінює обстановку підготовки та вчинення злочину, оскільки частина злочинної діяльності переноситься у цифровий простір.

Особливості обстановки квартирних крадіжок, учинених організованими злочинними угрупованнями, також проявляються у способах приховування злочину. Після викрадення майна злочинці нерідко змінюють місце його зберігання, використовують посередників для реалізації викрадених речей, переправляють цінності в інші регіони або за кордон. Для легалізації майна можуть використовуватись ломбарди, інтернет–платформи, фіктивні документи та підконтрольні особи. В окремих випадках злочинці навмисно створюють хибну слідову картину, імітують дії випадкових крадіїв або використовують методи інсценування для ускладнення розслідування.

На формування обстановки вчинення квартирних крадіжок значно впливають умови воєнного стану та загальна криміногенна ситуація. Переміщення населення, евакуація громадян, тимчасове залишення житла без нагляду, перевантаження правоохоронної системи та збільшення кількості зброї в незаконному обігу створюють додаткові можливості для організованих злочинних угруповань. У таких умовах злочинці можуть використовувати хаотичність соціальних процесів, недостатній контроль за пересуванням осіб та зниження рівня суспільної пильності. Водночас зростає рівень конспірації та мобільності злочинних груп, які нерідко змінюють регіони діяльності та використовують міжрегіональні зв’язки [2].

Криміналістичне значення обстановки вчинення квартирних крадіжок полягає у тому, що її аналіз дозволяє встановити характер злочинної діяльності, рівень організованості угруповання, можливий склад учасників, способи підготовки та приховування злочину, а також прогнозувати подальші дії злочинців. Вивчення обстановки дає можливість формувати типові слідчі версії, визначати найбільш імовірні джерела доказової інформації, встановлювати маршрути переміщення учасників та викраденого майна, а також визначати напрями взаємодії слідчих і оперативних підрозділів.

Отже, обстановка вчинення квартирних крадіжок, учинених організованими злочинними угрупованнями, є складною системою взаємопов’язаних умов, факторів та обставин, які відображають високий рівень підготовки, організації та конспірації злочинної діяльності. Її формування залежить від територіальних, часових, соціальних, технічних та інформаційних характеристик середовища, а також від структури й професійного рівня самого злочинного угруповання. Комплексний аналіз обстановки має важливе значення для побудови ефективної методики розслідування квартирних крадіжок, своєчасного виявлення злочинних зв’язків та встановлення всіх учасників організованої злочинної діяльності.

Перелік використаних джерел:

1. Методика розслідування крадіжок з автотранспортних засобів: проблеми теорії та практики : монографія / В. Ю. Дрозд. К. О. Чаплинський, Одеса : Видавництво «Юридика», 2023. 306 с.

2. Копча В.В. Криміналістична характеристика щодо розслідування крадіжок під час воєнного стану. Аналітично–порівняльне правознавство. 2025. № 4, ч. 3. С. 224–228.

DOI https://doi.org/10.32837/11300.33562

Патрелюк Дмитро
кандидат юридичних наук,
докторант Донецького державного університету внутрішніх справ
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–7300–4905
e–mail:d.a.patreluk@ukr.net

ЩОДО ЗАСОБІВ КРИМІНАЛЬНОГО ПЕРЕСЛІДУВАННЯ

Проаналізовано засоби кримінального переслідування на стадії досудового кримінального провадження. Відмічено, що засоби кримінального переслідування спрямовані на отримання та перевірку доказової інформації про обставини вчиненого кримінального правопорушення. Наголошено, що система засобів кримінального переслідування складається з різноманітних процесуальних (оперативно–розшукових) засобів одержання та перевірки доказової інформації про подію та склад кримінального правопорушення. Акцентовано, що до засобів кримінального переслідування необхідно віднести: оперативно–розшукові заходи, слідчі (розшукові) дії, негласні слідчі (розшукові) дії, заходи забезпечення кримінального провадження, інші процесуальні дії.

Ключові слова: кримінальне провадження, кримінальне переслідування, засоби кримінального переслідування, слідчі (розшукові) дії.

Patreluk Dmytro
candidate of Juridical Sciences,
doctoral Candidate of Law, Donetsk State University of Internal Affairs
Odesa, Ukraine

REGARDING MEANS OF CRIMINAL PROSECUTION

The means of criminal prosecution at the stage of pre–trial criminal proceedings are analyzed. It is noted that the means of criminal prosecution are aimed at obtaining and verifying evidentiary information about the circumstances of the committed criminal offense. It is emphasized that the system of means of criminal prosecution consists of various procedural (operational and investigative) means of obtaining and verifying evidentiary information about the event and the composition of the criminal offense. It is emphasized that such means should include: operational and investigative measures, investigative (investigative) actions, covert investigative (investigative) actions, measures to ensure criminal proceedings, other procedural actions.

Keywords: criminal proceedings, criminal prosecution, means of criminal prosecution, investigative (search) actions.

Кримінальне переслідування як діяльність з встановлення події та складу кримінального правопорушення може здійснюватися шляхом реалізації різноманітних засобів. Останні спрямовані на отримання та перевірка доказової інформації про обставини вчиненого кримінального правопорушення.

Система засобів кримінального переслідування складається з різноманітних процесуальних (оперативно–розшукових) засобів одержання та перевірки доказової інформації про подію та склад кримінального правопорушення. До таких засобів необхідно віднести: оперативно–розшукові заходи, слідчі (розшукові) дії, негласні слідчі (розшукові) дії, заходи забезпечення кримінального провадження, інші процесуальні дії.

Всі перераховані вище пізнавальні засоби належать до засобів кримінального переслідування незважаючи на їхнє неоднакове функціональне призначення у відповідності до норм кримінального процесуального законодавства. Якщо не виникає сумнівів щодо віднесення слідчих (розшукових) дій (ч. 1 ст. 223 КПК України) та негласних слідчих (розшукових) дій (ч.ч. 1, 2 ст. 246 КПК України) до засобів кримінального переслідування, то стосовно оперативно–розшукових заходів, заходів забезпечення кримінального провадження та інших процесуальних дій логічно постають деякі питання щодо їх включення до системи засобів кримінального переслідування.

Попри те, що оперативно–розшукові заходи не охоплюються предметом правового регулювання КПК України та спрямовані на отримання та перевірку оперативно–розшукової інформації, такі заходи слід відносити до засобів кримінального переслідування. Оскільки оперативно–розшукові заходи є аналогами негласних слідчих (розшукових) дій, результати оперативно–розшукової діяльності використовуються у доказуванні обставин вчиненого кримінального правопорушення. З урахуванням змісту Закону України «Про оперативно–розшукову діяльність» (ст. 6) та положень КПК України (ст. 214) можна зазначити, що стосовно кримінальних правопорушень, що готуються, та щодо осіб, які готують скоєння кримінальних правопорушень, до внесення відомостей до Єдиного реєстру досудових розслідувань, оперативно–розшукові заходи є єдиними засобами кримінального переслідування. За таких обставин шляхом здійснення оперативно–розшукових засобів здобувається процесуально значима інформація, що надалі використовується для підтвердження факту вчинення кримінального правопорушення та встановлення причетності певної особи до вчинення кримінального правопорушення.

Заходи забезпечення кримінального провадження регулюються змістом КПК України, проте прямо не належать за засобів одержання та перевірки доказів (ч. 1 ст. 131 КПК України). Через застосування окремих заходів забезпечення кримінального провадження (наприклад, тимчасовий доступ до речей і документів) можна здобути доказову інформацію про подію і склад кримінального

правопорушення. Саме тому заходи забезпечення кримінального провадження потрібно включати до різновидів засобів кримінального переслідування.

Разом з тим, в частині отримання та перевірки доказових даних нормативне регулювання заходів забезпечення кримінального провадження є недосконалим щодо ефективного забезпечення прав і свобод людини. Це створює ризик визнання одержаних доказів недопустимими внаслідок істотного порушення прав і свобод людини у кримінальному провадженні. У зв'язку з цим, правова регламентація деяких заходів забезпечення кримінального провадження як засобів кримінального переслідування потребує удосконалення.

Серед інших процесуальних дій, які є засобами кримінального переслідування доцільно виокремити витребування та отримання речей, документів та відомостей (ч. 2 ст. 93 КПК України), що можуть підтверджувати обставини скоєного кримінального правопорушення. Незважаючи на те, що «витребування та отримання» має недостатній ступінь урегульованості щодо порядку реалізації та дотримання правових гарантій, вказані процесуальні дії безумовно за своєю пізнавальною природою мають ототожнюватися із засобами кримінального переслідування.

Окреслений широкий підхід до системи засобів кримінального переслідування передбачає включення до останніх інших процесуальних (поза процесуальних) засобів, в результаті яких може здобуватися доказова інформація про обставини вчиненого кримінального правопорушення.

DOI https://doi.org/10.32837/11300.33563

Петросян Айк
здобувач кафедри оперативно–розшукової діяльності та національної безпеки Національної академії внутрішніх справ,
м. Київ, Україна
ORCID: https://orcid.org/0009–0000–3841–8179
e–mail: kafedra_ord@navs.edu.ua

РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, УЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ ГРУПАМИ У СФЕРІ ІНВЕСТИЦІЙНОЇ ДІЯЛЬНОСТІ: ТЕОРЕТИКО–ПРАВОВІ ЗАСАДИ

Наголошено на розробленні наукового та навчально–методичного забезпечення проблематики, задля підґрунтя ефективного виявлення, припинення, розкриття, розслідування та запобігання кримінальним правопорушенням у сфері інвестиційної діяльності.

Ключові слова: кримінальне правопорушення; інвестиційна діяльність; криміналістична характеристика.

Petrosian Aik
candidate of the Department of Operational Investigation and National Security of the National Academy of Internal Affairs,
Kyiv, Ukraine

INVESTIGATION OF CRIMINAL OFFENSES COMMITTED BY ORGANIZED CRIME GROUPS IN THE SPHERE OF INVESTMENT ACTIVITIES: THEORETICAL AND LEGAL PRINCIPLES

Emphasis is placed on the development of scientific and educational and methodological support for the issue, in order to provide a basis for effective detection, suppression, disclosure, investigation and prevention of criminal offenses in the field of investment activities.

Keywords: criminal offense; investment activities; forensic characteristics.

Питання виявлення та забезпечення досягнення завдань кримінального провадження щодо кримінальних правопорушень, учинених організованими злочинними групами у сфері інвестиційної діяльності, є пріоритетними у діяльності правоохоронних органів.

Для зниження рівня економічної злочинності та правопорушень у сфері інвестиційної діяльності Міністерством внутрішніх справ України проводиться робота за такими напрямами, як: а) організація виявлення, попередження, припинення та розкриття економічних злочинів та адміністративних проступків в

органах виконавчої влади, які здійснюють ведення питань економіки та фінансів, володіння, користування, розпорядження, що перебувають у державній власності, та природними ресурсами; б) організація профілактичних та оперативно–розшукових заходів щодо захисту всіх форм власності від злочинних посягань з метою забезпечення сприятливих умов для розвитку підприємництва та інвестиційної діяльності. До зазначеного комплексу заходів належать забезпечення захисту реалізації інвестиційних проєктів від економічних та інших загроз, протидія криміналізації інвестиційної діяльності з боку правоохоронних органів. МВС України на постійній основі проводиться комплекс організаційних та практичних заходів, спрямованих на виявлення та припинення злочинів та адміністративних правопорушень, що негативно впливають на інвестиційний клімат в Україні [1, с. 166].

Виходячи із аналізу джерел, розслідування кримінальних правопорушень у сфері інвестиційної діяльності є одним із пріоритетних напрямів у діяльності правоохоронних органів, а за умови вчинення організованими злочинними групами – мають ще більш суспільно небезпечний і масштабний характер, набувають транснаціональних форм, що лише загострює проблематику.

Важливим завданням є висвітлення теоретико–правових основ дослідження кримінальних правопорушень у сфері інвестиційної діяльності як щодо їх комплексної нормативно–правової характеристики, так і під кутом зору науки криміналістики, з метою виявлення закономірних зв’язків протиправної діяльності, що є запорукою успішного виявлення, розкриття та розслідування кримінальних правопорушень.

Передусім слід окреслити нормативно–правову основу дослідження, й у даному аспекті важливими є Стандарти діяльності прокурорів у сфері захисту інвестицій під час досудового розслідування, затверджені Наказом Генерального прокурора від 24 квітня 2024 року №84 [2].

Вказані Стандарти діяльності прокурорів у сфері захисту інвестицій під час досудового розслідування (Стандарти) є комплексом основних характеристик і моделлю реалізації повноважень прокурора у кримінальному провадженні, розробленою на підставі загальної кримінальної процесуальної форми, передбаченої кримінальним процесуальним законодавством України, чинних міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, рішень Європейського суду з прав людини, правових позицій Конституційного Суду України та Верховного Суду (Верховного Суду України та Вищого спеціалізованого суду з розгляду цивільних та кримінальних справ) (п. 1 Стандартів) [2].

Стандарти ґрунтуються на засадах діяльності прокуратури, встановлених ст. 3 Закону України «Про прокуратуру», загальних засадах кримінального провадження, визначених ст. 7 КПК України (п. 2 Стандартів).

Метою розроблення і впровадження вказаних Стандартів є:

– забезпечення однакового застосування норм законодавства України під час реалізації повноважень прокурора у кримінальному провадженні;

– забезпечення ефективної організації та процесуального керівництва досудовим розслідуванням при виконанні завдань і дотримання загальних засад кримінального провадження;

– визначення найбільш ефективного механізму реалізації прокурорами повноважень щодо організації і процесуального керівництва досудовим розслідуванням;

– недопущення незаконного втручання прокуратури та органів досудового розслідування у господарську та інвестиційну діяльність;

– підвищення професійного рівня прокурорів, які реалізують свої повноваження у кримінальному провадженні;

– оцінювання якості діяльності прокурорів щодо організації та процесуального керівництва досудовим розслідуванням у кримінальних провадженнях стосовно суб'єктів інвестиційної діяльності, а також щодо протиправного втручання в господарську та інвестиційну діяльність (п. 3 Стандартів) [2].

Стандарти діяльності прокурорів у сфері захисту інвестицій окреслюють визначення поняття «кримінальні правопорушення у сфері інвестиційної діяльності» як передбачені нормами Особливої частини Кримінального кодексу України суспільно небезпечні винні діяння (дія або бездіяльність), спрямовані на протиправне втручання в інвестиційну діяльність, вчинені суб'єктом кримінального правопорушення [2].

Поняття інвестиційної діяльності визначено у ст. 2 Закону України «Про інвестиційну діяльність» від 18 вересня 1991 року, а саме що «інвестиційною діяльністю є сукупність практичних дій громадян, юридичних осіб і держави щодо реалізації інвестицій» [3].

У свою чергу інвестиціями, згідно ч. 1–2 ст. 1 Закону України «Про інвестиційну діяльність», є всі види майнових та інтелектуальних цінностей, що вкладаються в об'єкти підприємницької та інших видів діяльності, в результаті якої створюється прибуток (доход) та/або досягається соціальний та екологічний ефект. Такими цінностями можуть бути: 1) кошти, цільові банківські вклади, паї, акції та інші цінні папери (крім векселів); 2) рухоме та нерухоме майно (будинки, споруди, устаткування та інші матеріальні цінності); 3) майнові права інтелектуальної власності; 4) сукупність технічних, технологічних, комерційних та інших знань, оформлених у вигляді технічної документації, навиків та виробничого досвіду, необхідних для організації того чи іншого виду виробництва, але не запатентованих («ноу–хау»); 5) права користування землею, водою, ресурсами, будинками, спорудами, обладнанням, а також інші майнові права; 6) інші цінності [3].

Вказані Стандарти наводять визначення, що «кримінальне провадження щодо протиправного втручання в господарську та інвестиційну діяльність – досудове розслідування і судове провадження, процесуальні дії у зв'язку із вчиненням діяння, передбаченого законом України про кримінальну відповідальність, щодо посягання на порядок інвестиційної та господарської діяльності, права і законні інтереси суб'єктів інвестиційної та господарської діяльності, та/або у яких вони залучені як потерпілі або є особами, права та інтереси яких порушені чи можуть бути порушені внаслідок вчинення кримінального правопорушення» (п. 4 Стандартів) [2].

Важливо, що зміст Стандартів деталізується за змістом аналізованого нормативно–правового акту, а саме наводяться основні джерела, на яких ґрунтується стандарт та закріплюються основні джерела перевірки стандарту.

Поряд із вказаним, слід зауважити, що сфера інвестиційної діяльності є досить широка і регламентується різними галузями права, а також пов'язана із реалізацією господарської діяльності суб'єктів.

З криміналістичного підходу, усталеним, перевіреним наукою і практикою є підхід до формування криміналістичної характеристики кримінального правопорушення.

Криміналістичну характеристику варто тлумачити як інформаційну модель, що складається із системи ознак певного виду (групи) злочинів, що визначає алгоритм дій слідчого щодо встановлення її елементів: предмету посягання, обстановки та способу вчинення злочину, слідової картини події, особи злочинця та особи потерпілого, з метою використання отриманих даних у процесі розслідування злочину. Основними елементами є: предмет посягання; спосіб підготовки, безпосереднього вчинення та приховування злочину; слідова картина; обстановка вчинення злочину; особа злочинця; особа потерпілого [4, с. 10].

Вважаємо доцільним наголосити на необхідності створення науково та навчально–методичного забезпечення, що буде підґрунтям удосконалення як нормативно–правового регулювання вказаної діяльності, так і запорукою ефективного виявлення, припинення, розкриття, розслідування та запобігання кримінальним правопорушенням у сфері інвестиційної діяльності.

Перелік використаних джерел:

1. Фесенко О.М. Компетенція та повноваження правоохоронних органів у сфері захисту інвестицій в Україні. Науковий вісник публічного та приватного права. Випуск 4, 2020. С. 161–167. DOI https://doi.org/10.32844/2618–1258.2020.4.28

2. Стандарти діяльності прокурорів у сфері захисту інвестицій під час досудового розслідування : Наказ Генерального прокурора від 24 квітня 2024 року №84. https://zakon.rada.gov.ua/laws/show/v0084905–24#n6

3. Про інвестиційну діяльність : Закон України від 18 вересня 1991 року № 1560–XII. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1560–12#Text

4. Чорноус Ю.М., Жовтюк О.В. Воєнні злочини: криміналістична характеристика та психологічні особливості реалізації злочинної діяльності. Юридична психологія : наук. журн. 2024. № 2 (35). С. 7–17. DOI: 10.33270/03243502.07

DOI https://doi.org/10.32837/11300.33569

Пишненко Ірина
асистент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0009–0004–4380–7071
e–mail:irinapysnenko986@gmail.com

ІНСЦЕНУВАННЯ ЯК ЗАСІБ МАСКУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ: МЕТОДИ МОДЕЛЮВАННЯ ТА ВИЯВЛЕННЯ

У тезах досліджено інсценування як спосіб маскування злочинної діяльності, розкрито методи моделювання штучної обстановки події та особливості її виявлення засобами криміналістики. Проаналізовано типові ознаки інсценування та способи їх викриття.

Ключові слова: інсценування, маскування злочину, слідова картина, криміналістика, моделювання події, виявлення злочину.

Pyshnenko Iryna
Assistant of the Department of Criminalistics, Forensic Examinations, and Polygraphology, National University «Odesa Law Academy», Odesa, Ukraine

STAGING AS A MEANS OF CONCEALING CRIMINAL ACTIVITY: METHODS OF MODELLING AND DETECTION

This paper examines staging as a means of concealing criminal activity, explores methods of fabricating the scene of an incident, and outlines the specific features of its detection using forensic techniques. It analyses the typical characteristics of staging and the methods used to expose it.

Key words: staging, concealing a crime, crime scene evidence, forensic science, reconstructing the incident, detecting a crime.

Інсценування як засіб маскування злочинної діяльності є одним із найбільш складних і багатогранних об’єктів криміналістичного дослідження, оскільки поєднує у собі елементи приховування злочину, психологічного впливу на учасників кримінального провадження, маніпулювання доказовою інформацією та створення хибної картини події. В умовах сучасної злочинності інсценування дедалі частіше використовується не лише для уникнення кримінальної відповідальності, а й для дезорієнтації правоохоронних органів, формування помилкових слідчих версій, створення штучних доказів або імітації обставин, які свідчать про відсутність кримінального правопорушення. Особливої актуальності ця проблема набуває в умовах воєнного стану, активізації організованої

злочинності, широкого використання цифрових технологій та ускладнення способів приховування протиправної діяльності.

Інсценування у криміналістичному аспекті доцільно розглядати як умисне створення або зміну обстановки події з метою формування неправдивого уявлення про характер, механізм, мотиви, учасників чи наслідки кримінального правопорушення. Основною ознакою інсценування є цілеспрямоване викривлення фактичної картини події шляхом створення штучних слідів, знищення або приховування справжніх слідів, зміни положення об’єктів, фальсифікації доказів чи моделювання іншої події [1]. На відміну від звичайного приховування злочину, інсценування характеризується активним формуванням альтернативної інформаційної моделі події, яка повинна переконати слідство у правдивості вигаданої версії.

Найбільш поширеними є інсценування самогубства, нещасного випадку, природної смерті, пожежі, зникнення особи, крадіжки зі зломом, дорожньо–транспортної пригоди, необхідної оборони чи раптового конфлікту. При цьому злочинці нерідко використовують знання про типові дії правоохоронних органів, особливості огляду місця події, характер слідоутворення та поширені слідчі версії. Саме тому сучасне інсценування часто має складний комбінований характер і передбачає не лише фізичне моделювання обстановки, а й інформаційний вплив через свідків, цифрові комунікації, соціальні мережі та електронні документи.

Одним із ключових елементів інсценування є моделювання обстановки події. У криміналістиці моделювання розглядається як процес створення певної системи ознак, яка повинна імітувати реальні обставини іншої події. Злочинець намагається відтворити типову слідову картину, характерну для певного виду події, однак через обмеженість знань, психологічний стан, дефіцит часу або помилки у відтворенні механізму події між справжньою та інсценованою картиною виникають суперечності. Саме ці суперечності мають ключове значення для виявлення інсценування.

Методи моделювання інсценування можуть бути класифіковані за кількома напрямами. Першу групу становлять матеріально–обстановочні методи, які полягають у зміні фізичної обстановки місця події. До них належать переміщення трупа, імітація боротьби, пошкодження замків, вікон чи дверей, розкидання речей, створення слідів проникнення, підпал приміщення, розміщення предметів у певному порядку або створення штучних слідів крові. Наприклад, при інсценуванні квартирної крадіжки злочинці можуть пошкоджувати замки вже після законного проникнення до приміщення, а при інсценуванні самогубства – створювати неприродне положення тіла, залишати фальшиві передсмертні записки або розміщувати знаряддя смерті у спосіб, який не відповідає механізму травмування.

Другу групу становлять інформаційні методи моделювання, пов’язані зі створенням неправдивої інформації про подію. Вони можуть проявлятися у

поданні неправдивих заяв, узгодженні показань між співучасниками, створенні фальшивого алібі, підробленні документів, маніпулюванні відеозаписами чи цифровими повідомленнями. У сучасних умовах значного поширення набули випадки цифрового інсценування, коли злочинці видаляють електронні сліди, створюють підроблені листування, використовують відкладені повідомлення або штучно формують геолокаційні дані для підтвердження неправдивої версії.

Третю групу становлять поведінкові методи моделювання, що пов'язані з імітацією певної психологічної або емоційної реакції. Особи, які здійснили злочин, можуть демонструвати надмірне хвилювання, штучну розгубленість, агресію або, навпаки, неприродний спокій. Іноді інсценування супроводжується активною участю у пошуку потерпілого, демонстративною співпрацею зі слідством або навмисним поширенням окремих версій серед свідків та знайомих. Аналіз поведінки учасників події нерідко дозволяє виявити невідповідність між їх емоційними реакціями та реальним характером події.

Виявлення інсценування базується на встановленні суперечностей між реальною механікою події та штучно створеною картиною. Основне значення у цьому процесі має криміналістичний аналіз слідової картини. Будь–яке інсценування залишає комплекс невідповідностей, які можуть проявлятися у локалізації слідів, механізмі їх утворення, часових параметрах, взаємному розташуванні об'єктів або фізичних характеристиках ушкоджень. Наприклад, при інсценуванні самогубства шляхом повішення можуть бути відсутні характерні ознаки механічної асфіксії, а при інсценуванні пограбування – не відповідати механізму злому характер пошкоджень дверей чи вікон.

Одним із найбільш ефективних методів виявлення інсценування є ситуаційне моделювання події. Слідчий аналізує можливість розвитку події за версією, яку намагається створити злочинець, та порівнює її з об'єктивними даними. Якщо механізм події суперечить законам фізики, біомеханіки, логіці поведінки чи особливостям слідоутворення, виникають підстави для висунення версії про інсценування. У таких випадках важливе значення мають судово–медичні, трасологічні, балістичні, біологічні та психологічні експертизи.

Суттєву роль у викритті інсценування відіграє комплексний підхід до оцінки доказової інформації. Окремий слід або окрема обставина можуть виглядати правдоподібно, однак у сукупності виникають суперечності, які свідчать про штучність створеної картини. Наприклад, при інсценуванні дорожньо–транспортної пригоди пошкодження транспортного засобу можуть не відповідати характеру травм потерпілого, а траєкторія руху автомобіля – розташуванню уламків чи гальмівного шляху.

Важливе значення для виявлення інсценування має також аналіз негативних обставин. Негативними вважаються факти, які повинні були існувати за певних умов, однак відсутні на місці події. Наприклад, відсутність слідів крові при значних тілесних ушкодженнях, відсутність слідів боротьби у випадку насильницького злочину або відсутність характерних пошкоджень при

заявленому механізмі проникнення до приміщення можуть свідчити про штучне створення обстановки. Саме негативні обставини нерідко стають першими ознаками інсценування.

Сучасна криміналістика дедалі більше використовує цифрові технології для викриття інсценувань. Аналіз метаданих фотографій, відеозаписів, геолокації, телефонної активності, цифрових листувань та електронних транзакцій дозволяє встановити реальний механізм події та виявити спроби фальсифікації інформації. Особливого значення це набуває при розслідуванні злочинів, пов’язаних із використанням соціальних мереж, месенджерів та електронних документів. У багатьох випадках саме цифрові сліди дозволяють встановити, що певні повідомлення були створені вже після смерті особи або з іншого пристрою, ніж той, який належав потерпілому.

Окремої уваги потребує інсценування у діяльності організованих злочинних угруповань. Для таких випадків характерний високий рівень підготовки, розподіл ролей між учасниками, використання корумпованих зв’язків та професійне маскування слідів. Одні учасники можуть безпосередньо створювати штучну обстановку, інші – забезпечувати фальшиве алібі, впливати на свідків або організовувати інформаційне прикриття. Саме тому розслідування таких злочинів вимагає проведення комплексних тактичних операцій, одночасного документування дій різних учасників та активного використання негласних слідчих (розшукових) дій [2].

Психологічний аспект інсценування також має важливе значення. Особи, які створюють інсценування, часто концентрують увагу на найбільш помітних деталях, залишаючи поза увагою другорядні елементи, які можуть викривати штучність події. Крім того, злочинці нерідко переоцінюють власні знання у сфері криміналістики, що призводить до надмірної деталізації або створення неприродно ідеальної картини події. Саме надлишкова демонстративність, логічна завершеність або штучна впорядкованість місця події можуть свідчити про намагання приховати реальний механізм злочину.

Отже, інсценування є складною формою приховування злочинної діяльності, що передбачає цілеспрямоване моделювання неправдивої картини події шляхом зміни обстановки, створення штучних слідів та маніпулювання доказовою інформацією. Його виявлення потребує комплексного криміналістичного аналізу, використання спеціальних знань, ситуаційного моделювання, аналізу негативних обставин та сучасних цифрових технологій. Ефективне викриття інсценування можливе лише за умови системного дослідження усіх елементів слідової картини, критичної оцінки доказів та встановлення суперечностей між реальною механікою події і створеною злочинцем моделлю.

Перелік використаних джерел:

1. Аксьонов В. В., Кожевніков В. В. До проблеми встановлення факту інсценування злочинів. Криміналістичний вісник. 2017. № 1 (27). С. 117–123.

2. Лисиченко В.К., Шехавцов Р.М. Проблеми теорії та практики подолання протидії розслідуванню окремих різновидів кримінальних правопорушень, вчинених організованими групами, злочинними організаціями : монографія. Вид. 2–е, перероб. та доп. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 343 с.

DOI https://doi.org/10.32837/11300.33571

Пожар Вадим
кандидат юридичних наук,
доцент кафедри криміналістики, судових експертиз та поліграфології,
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000-0003-2029-1581
e–mail: pvg.profy03@gmail.com

ПРОБЛЕМАТИКА ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ПРАВ І ЗАКОННИХ ІНТЕРЕСІВ ПОТЕРПІЛОГО ПІД ЧАС ЗАСТОСУВАННЯ ДО ОСОБИ ТРИМАННЯ ПІД ВАРТОЮ

У тезах досліджено проблематику забезпечення прав і законних інтересів потерпілого під час вирішення питання про застосування до підозрюваного чи обвинуваченого запобіжного заходу у вигляді тримання під вартою. На підставі положень Конституції України, Кримінального процесуального кодексу України та практики Європейського суду з прав людини обґрунтовано необхідність переосмислення процесуальної ролі потерпілого у кримінальному провадженні.

Ключові слова: потерпілий, засади кримінального провадження, запобіжні заходи, тримання під вартою, забезпечення прав учасників кримінального провадження.

Pozhar Vadym
Candidate of Legal Sciences,
Associate Professor at the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»
Odesa, Ukraine

ISSUES OF THE PRINCIPLE OF ENSURING THE RIGHTS AND LEGITIMATE INTERESTS OF THE VICTIM WHEN APPLYING DETENTION TO A PERSON

The theses examine the issue of ensuring the rights and legitimate interests of the victim when deciding on the application of detention as a preventive measure to a suspect or accused person. Based on the provisions of the Constitution of Ukraine, the Criminal Procedure Code of Ukraine and the case law of the European Court of Human Rights, the need to reconsider the procedural role of the victim in criminal proceedings is substantiated. Particular attention is paid to the need to strengthen the procedural guarantees of the victim, ensure their right to be heard during the consideration of issues

concerning preventive measures and maintain a balance of interests among the participants in criminal proceedings.

Key words: victim, principles of criminal proceedings, preventive measures, detention, ensuring the rights of participants in criminal proceedings..

Відповідно до ст. 2 КПК України, завдання кримінального провадження охоплюють не лише забезпечення охорони прав, свобод і законних інтересів підозрюваного чи обвинуваченого, але й захист особи, суспільства та держави від кримінальних правопорушень. У цьому контексті потерпілий виступає безпосереднім носієм порушеного кримінальним правопорушенням блага, а тому належне забезпечення його процесуального статусу є необхідною передумовою досягнення цілей кримінального провадження. Відсутність належного акценту на правах та законних інтересах потерпілого у системі кримінально–процесуальних гарантій обумовлює виникнення дисбалансу між учасниками кримінального провадження та негативно впливає на реалізацію принципу рівності прав й справедливості.

Сталим є той факт, що у доктрині кримінального процесу пріоритетна увага приділялася гарантуванню прав підозрюваного та обвинуваченого, що було об’єктивно зумовлено необхідністю утвердження стандартів демократичної правової держави та запобігання можливим проявам свавілля з боку органів державної влади. Однак сучасний етап розвитку кримінального процесуального законодавства та правозастосовної практики актуалізує потребу у переосмисленні ролі потерпілого у кримінальному провадженні. На практиці саме потерпілий нерідко залишається найбільш уразливим учасником кримінального процесу, права та законні інтереси якого потребують не лише формального визнання, а й ефективного механізму відновлення та захисту.

Отже, положення ст. 55 Конституції України, інтерпретовані крізь призму практики Європейський суд з прав людини, формують не лише декларативне право потерпілого на звернення до суду, а й покладають на державу позитивний обов’язок щодо створення ефективного механізму реалізації та захисту такого права. У зазначеному аспекті право на судовий захист набуває змістовного наповнення через систему процесуальних гарантій, спрямованих на забезпечення реальної можливості потерпілого брати участь у кримінальному провадженні, відстоювати власні інтереси та домагатися відновлення порушених прав. За таких умов забезпечення прав і законних інтересів потерпілого слід розглядати як самостійну галузеву засаду кримінального провадження, що має фундаментальне значення для функціонування всієї системи кримінальної юстиції.

У зв’язку з цим, доцільно виокремити низку аргументів на користь нормативного закріплення відповідної засади у кримінальному процесуальному законодавстві. По–перше, її існування сприятиме забезпеченню належного балансу між сторонами кримінального провадження, оскільки сучасна модель кримінального процесу не може обмежуватися виключно посиленими гарантіями

сторони захисту без належного врахування прав та інтересів потерпілого. Закріплення окремої засади дозволить досягти процесуальної рівноваги між потерпілим та обвинуваченим, що відповідає принципу справедливого судочинства.

По–друге, належне забезпечення прав потерпілого безпосередньо пов'язане з реалізацією завдань кримінального провадження, визначених ст. 2 КПК України. Ефективне кримінальне судочинство є неможливим без гарантування належного захисту особи, яка зазнала шкоди внаслідок кримінального правопорушення, оскільки саме відновлення її порушених прав виступає одним із ключових критеріїв ефективності механізму кримінальної юстиції.

По–третє, нормативне закріплення засади забезпечення прав і законних інтересів потерпілого має важливе значення у контексті запобігання вторинній віктимізації. Недостатність процесуальних гарантій, складність процедур та відсутність ефективних механізмів захисту нерідко призводять до повторного психологічного та правового травмування потерпілої особи вже в межах самого кримінального провадження. У зв'язку з цим формування належної системи гарантій захисту потерпілого є необхідною умовою гуманізації кримінального процесу та забезпечення його людиноцентричного характеру.

Аналіз сучасної правозастосовної практики свідчить, що потерпілий часто не залучається до розгляду клопотання про запобіжний захід, хоча закон прямо не забороняє йому брати участь. Така практика веде до обмеження його права бути почутим та висловити свою думку щодо ризиків, які несе підозрюваний. Навіть коли вони беруть у цьому участь, інтереси потерпілого не завжди враховуються судом при ухваленні рішення. Це суперечить принципам змагальності та рівності сторін, які закріплені в Конституції України та КПК України. Крім того. потерпілі часто не інформуються про зміну або скасування запобіжного заходу, що ставить під загрозу їх безпеку та законні інтереси.

З огляду на це, вважаю, що у випадках, коли під час вирішення питання про застосування запобіжного заходу зачіпаються права чи законні інтереси потерпілого, зокрема у зв'язку з необхідністю забезпечення його особистої безпеки від можливих посягань або погроз з боку підозрюваного, а також з метою гарантування відшкодування завданої злочином матеріальної шкоди, потерпілий, його представник чи законний представник повинні мати право висловити свою позицію щодо обрання, продовження, зміни чи скасування відповідного запобіжного заходу. Крім того, вони також повинні бути наділеними правом оскаржити рішення, прийняте за результатами розгляду цього питання, до вищестоящого суду. Його позиція може стосуватися необхідності застосування до підозрюваного тримання під вартою у зв'язку з ризиками тиску, залякування або іншими формами впливу на потерпілого.

Задля реального забезпечення прав потерпілого, його законного представника та представника на цьому етапі провадження необхідно вносити

зміни до КПК України, які б чітко регламентували право потерпілого, законного представника, представника, по–перше, бути повідомленим про розгляд клопотання про застосування запобіжного заходу, брати участь у судовому засіданні, виступати в судовому засіданні, викладаючи свою позицію та аргументи, висловлювати свою думку щодо необхідності застосування певного заходу та його виду, зокрема наполягати на триманні під вартою підозрюваного, обвинуваченого. По–друге, у випадках коли слідчий, прокурор взагалі не ініціюють застосування до підозрюваного, обвинуваченого запобіжного заходу, потерпілий, його законний представник, представник повинні мати право самостійно звертатися до слідчого судді, суду з відповідним клопотанням про застосування запобіжного заходу. Також потерпілий, його представник повинен мати право самостійно звертатися до слідчого судді, суду з клопотаннями про зміну запобіжного заходу у вигляді тримання під вартою на інший і навпаки, а також про скасування тримання під вартою, якщо це буде відповідати його законним інтересам. І по–третє, потерпілий, його представник повинен мати безперешкодне право на оскарження ухвали слідчого судді про застосування запобіжного заходу або про відмову у цьому до суду апеляційної інстанції незалежно від їх участі у судовому розгляді цього питання в суді. Це сприятиме не лише дотриманню балансу інтересів сторін, але й підвищенню довіри потерпілих до системи кримінального правосуддя.

Таким чином, засада забезпечення прав і законних інтересів потерпілого в кримінальному провадженні повинна зайняти окрему важливу сходинку у системі галузевих засад кримінального провадження. Для цього необхідно забезпечити всебічний її розвиток та дослідження, зокрема й в аспекті її реалізації під час застосування до підозрюваного, обвинуваченого запобіжних заходів. Особливо гостро це питання постає при застосуванні найбільш суворого запобіжного заходу – тримання під вартою.

DOI https://doi.org/10.32837/11300.33573

Рубець Катерина
старший судовий експерт лабораторії почеркознавчих та технічних досліджень Львівського–науково дослідного інституту судових експертиз Міністерства юстиції України ,
м.Львів, Україна
ORCID: https://orcid.org/0009–0000–3587–0522
e–mail:katirubets@ukr.net

КРИМІНАЛЬНО–ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ ЗАСАДИ ВИКОРИСТАННЯ ПОЧЕРКОЗНАВЧОЇ ЕКСПЕРТИЗИ ПІД ЧАС ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

Розглянуто кримінально–процесуальні та криміналістичні засади використання почеркознавчої експертизи у цифрову епоху. Проаналізовано значення оригіналів документів, проблеми копій та вплив цифровізації на доказування у кримінальному провадженні.

Ключові слова: почеркознавча експертиза, кримінальне провадження, документування злочинів, цифровізація, докази, оригінал документа.

Rubets Kateryna
senior forensic expert laboratories of handwriting and technical research of documents Lviv Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine,
Lviv, Ukraine

CRIMINAL PROCEDURAL AND FORENSIC PRINCIPLES OF THE USE OF HANDWRITING EXAMINATION IN THE DOCUMENTATION OF CRIMES IN THE CONDITIONS OF DIGITALIZATION

The theses examine the criminal procedural and forensic foundations of the use of handwriting examination in the digital era. The significance of original documents, issues related to copies, and the impact of digitalization on evidence in criminal proceedings are analyzed.

Key words: handwriting examination, criminal proceedings; crime documentation; digitalization; evidence; original document.

У сучасних умовах цифровізації суспільних відносин суттєво трансформуються способи вчинення, приховування та документування кримінальних правопорушень. Активне використання цифрових технологій, засобів копіювання та обробки документів створює нові виклики для органів досудового розслідування та судово–експертної діяльності. У зв’язку з цим

особливого значення набуває застосування спеціальних криміналістичних знань, зокрема можливостей почеркознавчої експертизи як важливого засобу доказування у кримінальному провадженні.

Почеркознавча експертиза традиційно є одним із ключових видів судових експертиз, що використовується для встановлення виконавця рукописних текстів або підписів, а також виявлення ознак їх підроблення. Водночас особливістю даного виду дослідження є те, що його об'єктами виступають оригінали документів, які містять повний комплекс індивідуальних ознак письма. Застосування копій документів або їх цифрових відтворень у почеркознавчому дослідженні є недопустимим, оскільки вони не забезпечують необхідної повноти ознак для експертного аналізу та й це суперечить вимогам Науково – методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень згідно з якими для проведення почеркознавчих досліджень рукописних записів та підписів надаються оригінали документів [1].

Актуальність теми зумовлена необхідністю дослідження кримінально–процесуальних та криміналістичних засад використання почеркознавчої експертизи в умовах цифровізації, а також визначення особливостей документування злочинів, пов'язаних із використанням цифрових носіїв інформації, ускладненням фіксації та збереженням оригінальних документів, поширенням їх копій та ризиками цифрового підроблення.

Розвиток цифрових технологій істотно вплинув на процес документування кримінальних правопорушень та особливості роботи з доказовою інформацією. У кримінальному провадженні дедалі частіше використовуються копії документів, скановані матеріали та цифрові зображення, що вимагає чіткого дотримання процесуальних вимог щодо допустимості та достовірності доказів.

Почеркознавча експертиза є одним із найпоширеніших видів криміналістичних експертиз, що застосовується під час розслідування злочинів, пов'язаних із підробленням документів, шахрайством, службовими злочинами та іншими кримінальними правопорушеннями. Її основним завданням є ідентифікація виконавця рукописного тексту або підпису шляхом аналізу індивідуальних ознак письма.

Специфіка почеркознавчої експертизи полягає у необхідності дослідження саме оригіналів документів, оскільки лише вони містять повний комплекс ознак письма, зокрема особливості натиску, темпу виконання та послідовності рухів. Копії документів не дозволяють у повному обсязі дослідити ці характеристики, що може призвести до обмеженості або ймовірнісного характеру експертного висновку.

Важливим елементом є належне процесуальне оформлення призначення експертизи та отримання порівняльних зразків письма. Порушення вимог кримінального процесуального законодавства під час збирання матеріалів може вплинути на допустимість висновку експерта як доказу.

Окрему проблему становить поширення технічних способів підроблення документів, зокрема шляхом копіювання, монтажу або цифрової імітації підписів, що значно ускладнює процес виявлення фальсифікацій на етапі досудового розслідування. Такі способи підроблення дозволяють створювати візуально переконливі документи, які на перший погляд не викликають сумнівів у їх автентичності, проте не містять або спотворюють криміналістично значущі ознаки оригінального виконання. У результаті ускладнюється не лише ідентифікація виконавця рукописних елементів, але й встановлення способу виготовлення документа, часу та умов його створення.

Це, у свою чергу, потребує комплексного застосування криміналістичних знань та залучення різних видів судових експертиз. Зокрема, ефективним є поєднання почеркознавчої експертизи, спрямованої на встановлення виконавця рукописних записів або підписів, із технічною експертизою документів, яка дозволяє виявляти ознаки монтажу, дописок, підчисток, а також використання різних технічних засобів для виготовлення або зміни документа. Лише комплексний підхід дає можливість всебічно дослідити об’єкт, встановити механізм його створення та забезпечити належну доказову оцінку отриманих результатів у кримінальному провадженні.

У зв’язку з цим важливого значення набуває адаптація криміналістичних методик до умов цифровізації. Ефективність використання почеркознавчої експертизи залежить від правильного процесуального підходу, якості зібраних матеріалів та дотримання вимог щодо роботи з оригіналами документів.

Таким чином, почеркознавча експертиза залишається важливим засобом доказування у кримінальному провадженні навіть в умовах активної цифровізації суспільства. Вона забезпечує можливість встановлення виконавця рукописних записів та виявлення фактів підроблення документів. Незважаючи на поширення цифрових технологій та зменшення частки рукописних документів у діловому обігу, значна кількість юридично значущих документів і надалі містить рукописні елементи, зокрема підписи та рукописні записи, які потребують спеціального дослідження.

Ефективність застосування почеркознавчої експертизи значною мірою залежить від дотримання кримінально–процесуальних вимог щодо збирання та оформлення доказів, а також від використання саме оригіналів документів як основних об’єктів дослідження. Водночас сучасні способи цифрової обробки та фальсифікації документів ускладнюють процес доказування, що зумовлює необхідність комплексного підходу із залученням різних видів криміналістичних експертиз.

Узагальнюючи викладене, слід зазначити, що почеркознавча експертиза в сучасному кримінальному провадженні зберігає своє вагоме доказове значення, однак її застосування ускладнюється впливом цифровізації та трансформацією способів створення й обігу документів. У таких умовах підвищуються вимоги до

належного процесуального забезпечення експертних досліджень, зокрема щодо роботи з первинними матеріалами та дотримання правил збирання доказів.

Практика свідчить, що ефективність використання почеркознавчих досліджень значною мірою залежить від якості наданих матеріалів та комплексного підходу до їх оцінки у взаємозв'язку з іншими видами криміналістичних експертиз. Це дозволяє компенсувати обмеження, пов'язані з поширенням технічних способів підроблення документів та використанням їх копій у доказуванні.

Отже, розвиток сучасних технологій не зменшує значення почеркознавчої експертизи, а лише змінює умови її застосування, що потребує подальшого удосконалення криміналістичної методології та процесуальних підходів до використання спеціальних знань у кримінальному провадженні.

Перелік використаних джерел:

1.Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково – методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 08.10.1998 №53/5. URL :https://zakon.rada.gov.ua/laws/show/z0705–98.

DOI https://doi.org/10.32837/11300.33576

Самойленко Олена
доктор юридичних наук, професор,
професор кафедри оперативно–розшукової та поліцейської діяльності,
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–8925–4116
e–mail: samoilenko_elena@ukr.net

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ЕЛЕМЕНТ СУЧАСНИХ КРИМІНАЛІСТИЧНИХ МЕТОДИК

У тезах доповіді досліджено сучасні напрями інтеграції кримінального аналізу в систему криміналістичного забезпечення розслідування кримінальних правопорушень в умовах цифрового суспільства та воєнного стану. Проаналізовано можливості застосування оперативного аналізу, OSINT–технологій, аналізу зв'язків і геопросторового моделювання для підвищення ефективності слідчої діяльності, швидкого прийняття тактичних рішень та виявлення прихованих закономірностей злочинної діяльності.

Ключові слова: кримінальний аналіз, кримінальне правопорушення, криміналістична методика, цифрові сліди, алгоритм

Samoilenko Olena
Doctor of Law, Professor,
Professor of the Department of Operational–Search and Policing Activity,
National University «Odesa Law Academy»,
Odesa, Ukraine

CRIMINAL ANALYSIS AS AN ELEMENT OF MODERN CRIMINALISTIC METHODOLOGIES

These conference papers explore contemporary trends in integrating criminal analysis into the system of criminalistic support for investigating criminal offenses within the context of a digital society and martial law. The study analyzes the potential applications of operational analysis, OSINT (Open Source Intelligence) technologies, link analysis, and geospatial modeling to enhance the efficiency of investigative activities, facilitate rapid tactical decision–making, and identify hidden patterns of criminal activity.

Keywords: criminal analysis, criminal offense, criminalistic methodology, digital traces, algorithm.

Сучасна архітектура безпеки України вимагає переходу від реактивного моделювання (реагування на факт) до проактивного, стратегічного аналізу загроз. В умовах воєнного стану кримінальний аналіз поступово трансформувався з допоміжної, оперативно–розшукової функції у базовий елемент криміналістичної тактики, що дозволяє слідчому приймати рішення в умовах дефіциту часу та наявності великого обсягу неструктурованих даних (так званих Big Data).

На підставі аналізу матеріалів судово–слідчої практики можна виділити наступні основні напрями застосування методик кримінального аналізу у поєднанні із :

1. Інтеграція кримінального аналізу в криміналістичну структуру слідчої діяльності Оперативний аналіз (Operational Analysis) під час реагування на резонансні злочини полягає у миттєвій обробці великих потоків інформації. Використання інтегрованих систем відеонагляду та розпізнавання облич (на основі AI) для побудови маршрутів руху підозрюваних осіб або транспортних засобів у режимі реального часу стала одним з ключових елементів алгоритму дій, спрямованого на розслідування кримінального правопорушення. Аналітик забезпечує слідчого не просто довідкою, а динамічною картою події, що дозволяє коригувати слідчому алгоритм та тактику подальших слідчих (розшокових) дій.

Логічний зв’язок тут полягає у безперервному циклі: слідчий надає аналітику первинні відомості з місця події, а кримінальний аналітик у режимі реального часу перетворює їх на тактичну перевагу, ідентифікуючи зв’язки, які не є очевидними при візуальному огляді. Методика розслідування при такому підході збагачується інструментами автоматизованого пошуку кореляцій між способом вчинення злочину та наявними базами даних (від інформації про попередні правопорушень до результатів фільтрації цифрових слідів, логів мобільного зв’язку та даних систем відеомоніторингу, що у перші години після події злочину суттєво збільшує можливість затримання злочинця у найкоротчий термін після вчинення злочину. Також мінімізується ризик втрати доказової інформації, що в цілому дозволяє ефективно протидіяти професійній злочинності, яка використовує технологічні засоби конспірації.

2. Використання OSINT–технологій у розслідуванні злочинів проти національної безпеки та воєнних злочинів. Значна частина доказової бази сьогодні знаходиться у відкритому цифровому просторі (соціальні мережі, месенджери, супутникові знімки). Тактика та методика аналізу відкритих джерел була сьогодні предметом увага багатьох науковців [1; 2] саме через те, що Open Source Intelligence передбачає верифікацію контенту, встановлення геолокації за метаданими та ідентифікацію осіб через цифрові сліди. В умовах неможливості доступу до окупованих територій та територій бойових дій здійснення аналітичного опрацювання відеоматеріалів із месенджерів та соціальних мереж у поєднанні з ретроспективним аналізом супутникових знімків дозволяє ідентифікувати окремих фізичних осіб, встановити ієрархію підрозділів ворога, зафіксувати факт руйнувань, визначити точний час події чи траєкторію обстрілу.

Також методика розслідування при цьому збагачується алгоритмами цифрової автентифікації, які дозволяють відокремити дезінформацію від достовірних даних, забезпечуючи допустимість доказів для національних та міжнародних судових інстанцій.

3. Аналіз зв'язків (Link Analysis) та візуалізація злочинних мереж Сьогодні складні схеми незаконного обігу зброї чи наркотиків потребують методик розкриття прихованих взаємозв'язків. Застосування спеціалізованого прогманого забезпечення дозволяє створення мережевих діаграм, які якісно демонструють «вузлових учасників» організованої групи, які часто залишаються поза увагою при лінійному підході до розслідування діяльності організованої групи. Слідчий отримує візуалізовану схему ієрархії, що дозволяє визначати черговість проведення обшуків та допитів для досягнення максимального ефекту «раптовості».

4. Геопросторовий аналіз (Crime Mapping) та прогнозування Фактично цей напрям поєднює математичні точні розрахунки та засади математичної статистики з тактикою слідчої діяльності – на карту місцевості з урахуванням часу та зовнішніх чинників можуть бути нанесені раціонально розподілені сили і засоби поліції, місця вчинення нових правопорушень, маршрути руху та логіка діяльності злочинця, місця контакти жертви та злочинця тощо.

Отже, оптимізація методики розслідування кримінального правопорушення сьогодні неможлива без впровадження моделей діяльності слідчого керованих аналітикою. Кримінальний аналіз забезпечує методику розслідування необхідною швидкістю та точністю, перетворюючи розрізнені факти на цілісну картину кримінальної події. Зрештою, це дозволяє слідчому діяти превентивно, перехоплюючи ініціативу у правопорушника ще до моменту вчинення нового епізоду злочину чи знищення ним речових доказі. Таким чином, кримінальний аналіз де–факто стає новітнім елементом структури окремих криміналістичних методик, адаптованих до умов цифрового суспільства та воєнного стану.

Перелік використаних джерел:

1.Технологія OSINT: інструменти та методи для захисту інформаційної безпеки: практ. посіб. / Т. Ю. Ткачук, Н. І. Ткачук, І. М. Ничитайло А. І. Старосєк. Київ: НА СБУ, 2023. 180 с.

2.Реалізація філософії «Intelligence–led Policing» в системі кримінального аналізу Національної поліції України : монографія / [О. Користін, Д. Швець, Б. Бутко та ін.] ; за заг. ред. О. Є. Користіна. Київ : ВАІТЕ, 2024. 444 с.

DOI https://doi.org/10.32837/11300.33577

Стародубов Олександр
аспірант кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0007–6266–4813
e–mail:criminalistic@onua.edu.ua

ОСОБЛИВОСТІ ВИКОРИСТАННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС ПРОВЕДЕННЯ ТАКТИЧНИХ ОПЕРАЦІЙ З УРАХУВАННЯМ СУЧАСНИХ УМОВ

Досліджено особливості використання негласних слідчих (розшукових) дій під час проведення тактичних операцій у сучасних умовах. Визначено їх значення для документування організованої злочинної діяльності, протидії конспірації та забезпечення ефективності розслідування.

Ключові слова: негласні слідчі (розшукові) дії, тактична операція, досудове розслідування, організована злочинність, воєнний стан, криміналістика.

Starodubov Oleksandr
Postgraduate student of the Department of Criminalistics,
Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

FEATURES OF THE USE OF COVERT INVESTIGATIVE (INTELLIGENCE–GATHERING) MEASURES DURING TACTICAL OPERATIONS, TAKING CURRENT CONDITIONS INTO ACCOUNT

This study examines the specific features of the use of covert investigative (surveillance) measures during tactical operations in the modern context. It identifies their significance in documenting organized criminal activity, countering secrecy, and ensuring the effectiveness of investigations.

Key words: covert investigative (surveillance) activities, tactical operations, pre–trial investigations, organized crime, martial law, forensic science.

Сучасний етап розвитку кримінальної процесуальної діяльності характеризується суттєвим ускладненням форм і способів вчинення кримінальних правопорушень, активним використанням цифрових технологій злочинними угрупованнями, підвищеним рівнем конспірації, мобільністю кримінальних структур та адаптацією злочинців до діяльності правоохоронних органів. В умовах воєнного стану, поширення транснаціональної організованої злочинності, незаконного обігу зброї, наркотичних засобів, кіберзлочинності та корупційних

схем особливого значення набуває ефективне використання негласних слідчих (розшукових) дій у системі тактичних операцій. Саме поєднання комплексу процесуальних, оперативно–розшукових та організаційно–тактичних заходів дозволяє отримувати доказову інформацію в умовах прихованої злочинної діяльності, протидії розслідуванню та інформаційної ізоляції окремих кримінальних середовищ.

Негласні слідчі (розшукові) дії є одним із найбільш складних та інформаційно насичених інструментів кримінального провадження, оскільки забезпечують можливість отримання відомостей про підготовку, вчинення та приховування кримінальних правопорушень без розкриття факту здійснення процесуального контролю з боку правоохоронних органів. Їх значення особливо зростає у випадках документування діяльності організованих злочинних угруповань, терористичних структур, злочинів у сфері незаконного обігу зброї, наркотичних засобів, контрабанди, корупційних правопорушень та злочинів, що вчиняються із застосуванням сучасних засобів комунікації.

Тактична операція у криміналістиці розглядається як система взаємопов’язаних слідчих, негласних слідчих, оперативно–розшукових, організаційних та інших заходів, об’єднаних єдиною метою та реалізованих відповідно до конкретної слідчої ситуації для вирішення проміжних або кінцевих завдань розслідування [1]. У сучасних умовах проведення тактичних операцій дедалі частіше пов’язане із необхідністю комплексного використання негласного інструментарію, оскільки відкриті форми фіксації доказової інформації нерідко виявляються неефективними через високий рівень конспірації злочинців, використання ними захищених каналів зв’язку, спеціальних заходів контрспостереження, а також корумпованих зв’язків.

Особливістю використання негласних слідчих (розшукових) дій у сучасних умовах є їх інтеграція у багаторівневі тактичні операції, спрямовані не лише на фіксацію окремого епізоду злочинної діяльності, а й на встановлення структури злочинного угруповання, ролей його учасників, джерел фінансування, каналів постачання, способів легалізації доходів та механізмів внутрішньої взаємодії. У зв’язку з цим негласні дії дедалі частіше мають тривалий, системний і поетапний характер.

Однією з ключових сучасних тенденцій є активне використання аудіо– та відеоконтролю особи, зняття інформації з електронних комунікаційних мереж, спостереження за особою або об’єктом, встановлення місцезнаходження радіоелектронного засобу, контролю за вчиненням злочину та виконання спеціального завдання щодо розкриття діяльності організованої групи чи злочинної організації. Саме ці негласні дії дозволяють отримати інформацію про механізм координації дій злочинців, канали зв’язку між учасниками угруповання, характер їх ієрархії та способи ухвалення рішень.

Сучасні умови функціонування кримінального середовища характеризуються широким використанням месенджерів, анонімних акаунтів, VPN–сервісів, криптовалют, закритих форумів та засобів шифрування інформації. Це зумовлює необхідність технічного вдосконалення негласних слідчих дій та залучення спеціалістів у сфері цифрової криміналістики, кібербезпеки та телекомунікацій. У межах тактичних операцій особливого значення набуває не лише отримання інформації, а й її своєчасна аналітична обробка, зіставлення з іншими доказами та побудова криміналістичних моделей злочинної діяльності.

Важливою особливістю сучасних тактичних операцій є поєднання негласних слідчих (розшукових) дій із заходами оперативного супроводу та аналітичної роботи. Так, результати спостереження можуть використовуватися для визначення місць проведення майбутніх обшуків, встановлення каналів постачання зброї чи наркотичних засобів, виявлення місць зберігання речових доказів або документування контактів між співучасниками [2]. Водночас результати аудіо– та відеоконтролю нерідко стають підставою для формування нових слідчих версій та планування подальших етапів тактичної операції.

Особливого значення набуває контроль за вчиненням злочину як складна форма негласної діяльності, що дозволяє документувати механізм злочинної діяльності в реальному часі. У сучасних умовах така форма використовується під час розслідування незаконного обігу зброї, наркотичних засобів, корупційних правопорушень, торгівлі людьми та інших латентних злочинів. Водночас проведення таких заходів потребує суворого дотримання процесуальних гарантій, оскільки будь–які порушення можуть призвести до визнання доказів недопустимими або створення ризиків провокації злочину.

Суттєвою особливістю використання негласних слідчих (розшукових) дій у сучасних умовах є необхідність урахування високого рівня протидії розслідуванню. Організовані злочинні угруповання активно використовують заходи контрспостереження, зміну телефонів та SIM–карт, шифрування повідомлень, використання посередників, перевірку лояльності учасників та інші форми конспірації. У зв’язку з цим проведення тактичних операцій потребує максимальної секретності, багаторівневої координації між слідчими, оперативними працівниками та прокурором, а також ретельного планування часових меж та етапів реалізації операції.

В умовах воєнного стану особливості проведення негласних слідчих дій значно ускладнюються через нестабільну оперативну обстановку, переміщення населення, активізацію незаконного обігу зброї та підвищений рівень суспільної небезпеки окремих злочинів. Воєнні дії створюють додаткові труднощі щодо організації спостереження, технічного документування, забезпечення безпеки учасників кримінального провадження та збереження конфіденційності оперативної інформації. Крім того, окремі злочинні угруповання використовують воєнний стан як прикриття для незаконного переміщення зброї, контрабанди, легалізації майна та інших кримінальних схем.

У сучасних умовах особливого значення набуває проведення тактичних операцій, пов’язаних із викриттям внутрішньої структури організованих злочинних угруповань. Саме негласні слідчі (розшукові) дії дозволяють встановити роль організатора, координаторів, виконавців, осіб, відповідальних за фінансування, логістику, охорону чи легалізацію злочинних доходів. Використання аудіоконтролю, спостереження, контролю листування та виконання спеціального завдання сприяє формуванню комплексного уявлення про механізм функціонування злочинної організації.

Окремою проблемою сучасного використання негласних слідчих (розшукових) дій є необхідність забезпечення балансу між ефективністю розслідування та дотриманням прав людини. Негласне втручання у приватне життя, комунікації та пересування особи повинно відповідати принципам законності, пропорційності та обґрунтованості. У зв’язку з цим важливого значення набуває належне процесуальне оформлення результатів негласних дій, дотримання порядку отримання дозволів слідчого судді та забезпечення контролю за законністю проведення таких заходів.

Суттєву роль у сучасних тактичних операціях відіграє аналітичний компонент. Результати негласних слідчих (розшукових) дій повинні не лише накопичуватися, а й систематизуватися, зіставлятися між собою, аналізуватися з урахуванням часових, територіальних та поведінкових закономірностей. Саме аналітична обробка дозволяє виявляти приховані зв’язки між епізодами злочинної діяльності, визначати центри координації угруповання та прогнозувати подальші дії злочинців.

Важливим напрямом розвитку сучасних тактичних операцій є використання цифрових технологій та автоматизованих систем аналізу інформації. Йдеться про використання програм для аналізу телефонних з’єднань, геолокаційних даних, цифрових слідів, фінансових операцій та електронного листування. Такі засоби значно підвищують ефективність негласних слідчих (розшукових) дій, особливо у провадженнях щодо транснаціональної організованої злочинності та кіберзлочинів.

Не менш важливим є питання взаємодії між слідчими, оперативними підрозділами, прокурорами та спеціалістами під час проведення тактичних операцій. Ефективність негласних слідчих (розшукових) дій значною мірою залежить від своєчасного обміну інформацією, узгодженості дій, належного розподілу функцій та єдиного планування. В умовах сучасної криміногенної ситуації ізольоване використання окремих негласних заходів не забезпечує необхідного результату, тоді як їх системне поєднання у межах тактичної операції створює можливість для повного документування злочинної діяльності.

Таким чином, використання негласних слідчих (розшукових) дій під час проведення тактичних операцій у сучасних умовах характеризується комплексністю, технологічністю, високим рівнем конспірації та необхідністю

постійної адаптації до змін кримінального середовища. Сучасні умови вимагають інтеграції процесуальних, оперативно–розшукових та аналітичних можливостей, використання цифрових технологій, забезпечення міжвідомчої взаємодії та суворого дотримання правових гарантій. Саме системне та професійне використання негласного інструментарію дозволяє ефективно протидіяти організованій злочинності, латентним кримінальним правопорушенням та складним формам протидії досудовому розслідуванню.

Перелік використаних джерел:

1. Журавель В.А. Тактичні операції в системі криміналістичних засобів протидії злочинності. Теорія та практика судової експертизи і криміналістики. 2006. № 6. С. 30−36.

2. Юхно, О. О. Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних слідчих (розшукових) дій : [навч. посіб.]. О. О. Юхно, О. О. Загуменний. 2– ге вид., доп. і перероб. Харків. Колегіум. 2020. 116 с.

DOI https://doi.org/10.32837/11300.33579

Тіщенко Валерій
доктор юридичних наук, професор,
професор кафедри криміналістики,
судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
член–кореспондент НАПрН України
ORCID: https://orcid.org/0000–0002–2441–7535

Бєлік Лариса
кандидат юридичних наук, доцент,
дослідник Середньо-Шведського університету,
м. Сундсвалль, Швеція
ORCID: https://orcid.org/0000–0003–2183–6635
e–mail: larysa.bielik1@gmail.com

СЛІДЧА СИТУАЦІЯ ЯК ОСНОВА ТАКТИЧНИХ І СТРАТЕГІЧНИХ РІШЕНЬ У ДОСУДОВОМУ РОЗСЛІДУВАННІ

У тезах досліджується значення слідчої ситуації у формуванні тактичних і стратегічних рішень під час досудового розслідування. Розглянуто її сутність, класифікацію та роль у виборі слідчих дій, тактичних операцій і побудові програми розслідування.

Ключові слова: слідча ситуація; досудове розслідування; криміналістична тактика; тактичні операції.

Tishchenko Valerii †
Doctor of Legal Sciences, Professor,
Professor at the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Corresponding Member of the National Academy of Legal Sciences of Ukraine

Bielik Larysa
Candidate of Legal Sciences, Associate Professor,
researcher at Mid-Sweden University,
Sundsvall, Sweden

INVESTIGATIVE SITUATION AS THE BASIS FOR TACTICAL AND STRATEGIC DECISIONS IN PRE–TRIAL INVESTIGATION

The theses examine the significance of the investigative situation in the formation of tactical and strategic decisions during pre–trial investigation. Its essence, classification, and role in the selection of investigative actions, tactical operations, and the development of an investigation program are analyzed.

Keywords: investigative situation; pre–trial investigation; criminalistic tactics; tactical operations.

Сучасний етап розвитку криміналістики характеризується зростанням значення ситуаційного підходу у формуванні теоретичних положень криміналістичної тактики та методики розслідування кримінальних правопорушень. Важливість оцінки слідчої ситуації обумовлюється тим, що саме вона визначає можливість правильного вибору напряму розслідування, постановки тактичних і стратегічних завдань, а також застосування найбільш ефективних криміналістичних засобів. Окремі положення щодо сутності та значення слідчої ситуації були раніше досліджені авторами у фаховій науковій публікації, присвяченій проблемам ситуаційного підходу у криміналістиці [1].

Розслідування кримінальних правопорушень являє собою складну інформаційно–пізнавальну діяльність, спрямовану на встановлення факту події, механізму її вчинення, осіб, причетних до кримінального правопорушення, а також інших обставин, що мають доказове значення. У процесі такої діяльності слідчий постійно стикається зі змінами інформаційної обстановки, що обумовлює необхідність оцінки наявної ситуації та прийняття відповідних процесуальних і тактичних рішень.

У криміналістичній науці питання слідчої ситуації посідає важливе місце протягом багатьох десятиліть. Ще О.М. Колесніченко зазначав, що вибір напряму розслідування визначається не лише видом кримінального правопорушення, а передусім характером і змістом вихідної інформації, яка формує відповідну слідчу ситуацію [2]. Надалі концепція слідчої ситуації активно розвивалася у працях В.О. Коновалової, В.Ю. Шепітька, В.М. Шевчука, В.А. Журавля та інших науковців [3; 4; 5].

У сучасній криміналістиці слідча ситуація розглядається як сукупність умов, факторів та інформаційних даних, що характеризують стан розслідування на певному етапі кримінального провадження та впливають на вибір напряму і засобів діяльності слідчого.

Формування конкретної слідчої ситуації залежить від багатьох чинників, серед яких:

– місце і час вчинення кримінального правопорушення;

– характер та джерела вихідної інформації;

– наявність або відсутність очевидців;

– стан матеріальної обстановки місця події;
– поведінка учасників кримінального провадження;
– наявність протидії розслідуванню;
– повнота і достовірність отриманих доказових даних.

Важливе значення має криміналістичний аналіз слідчої ситуації. Такий аналіз дозволяє визначити інформаційну насиченість ситуації, її складність, конфліктність, а також перспективи вирішення тактичних і стратегічних завдань.

Криміналістичний аналіз доцільно проводити за кількома напрямами:

1. оцінка часово–просторових характеристик події;
2. аналіз походження та змісту первинної інформації;
3. оцінка стану джерел доказової інформації;
4. встановлення ступеня достовірності отриманих відомостей;
5. виявлення ознак протидії розслідуванню;
6. аналіз поведінки підозрюваних та інших учасників кримінального провадження.

У криміналістиці прийнято виділяти різні види слідчих ситуацій: типові і специфічні, прості і складні, сприятливі та несприятливі, конфліктні і безконфліктні, початкові, проміжні та завершальні [6]. Подібна класифікація має важливе значення для практики, оскільки дозволяє визначити найбільш ефективні форми та методи діяльності слідчого.

На тактичному рівні слідча ситуація безпосередньо впливає на:

– постановку тактичних завдань;
– вибір слідчих (розшукових) дій;
– визначення доцільності проведення тактичних операцій;
– моделювання поведінки учасників слідчої дії;
– вибір тактичних прийомів подолання протидії.

Особливого значення ситуаційний підхід набуває у конфліктних ситуаціях. Наприклад, при допиті особи, яка надає неправдиві показання, слідчий повинен оцінити характер конфлікту, визначити можливі способи психологічного впливу та обрати відповідні тактичні прийоми для викриття неправдивої інформації.

У складних ситуаціях для вирішення окремого тактичного завдання проведення однієї слідчої дії може бути недостатнім. У таких випадках виникає необхідність проведення тактичної операції, яка являє собою систему взаємопов’язаних процесуальних, оперативно–розшукових та організаційних заходів, спрямованих на досягнення конкретної мети [7].

Тактична операція проводиться на основі попереднього аналізу слідчої ситуації та включає:

– постановку тактичного завдання;
– визначення мети операції;
– планування комплексу дій;
– реалізацію запланованих заходів;

– оцінку отриманих результатів.

У методиці розслідування слідча ситуація набуває стратегічного значення, оскільки саме вона визначає загальний напрям розслідування, зміст програми слідчих дій та послідовність перевірки версій.

Особливу роль відіграє аналіз вихідної слідчої ситуації на початковому етапі розслідування. Саме на цьому етапі формуються перші слідчі версії, визначаються першочергові тактичні завдання, обираються процесуальні та криміналістичні засоби отримання доказової інформації.

Важливим елементом ситуаційного підходу є побудова та перевірка слідчих версій. Версії виступають інструментом організації пізнавальної діяльності слідчого та забезпечують цілеспрямований характер розслідування. Кожна слідча дія повинна бути спрямована на перевірку певної версії або встановлення конкретної обставини кримінального правопорушення.

У сучасних умовах ситуаційний підхід слід розглядати як один із базових принципів формування окремих криміналістичних методик. Типові слідчі ситуації дозволяють створювати алгоритми дій слідчого, що підвищує ефективність розслідування та забезпечує більш раціональне використання криміналістичних засобів.

Доцільним є застосування такого алгоритму організації розслідування:

1. аналіз і оцінка вихідної слідчої ситуації;
2. постановка тактичних і стратегічних завдань;
3. висунення та систематизація слідчих версій;
4. визначення комплексу слідчих (розшукових) дій і тактичних операцій;
5. оцінка отриманих результатів;
6. коригування програми розслідування відповідно до нової слідчої ситуації.

Таким чином, слідча ситуація є важливою категорією сучасної криміналістики, що має як теоретичне, так і практичне значення. Її правильний аналіз та оцінка дозволяють забезпечити ефективне планування досудового розслідування, обрати оптимальні тактичні засоби та своєчасно реагувати на зміни інформаційної обстановки.

Ситуаційний підхід повинен розглядатися як необхідна складова криміналістичної тактики та методики розслідування, а також як важливий напрям подальших наукових досліджень у сфері криміналістики.

Перелік використаних джерел:

1. Тіщенко В.В., Бєлік Л.С. Слідча ситуація у теорії криміналістики і практиці розслідування. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2025. Вип. 90. Ч. 4. С. 348–354. DOI: https://doi.org/10.24144/2307–3322.2025.90.4.50.

2. Колесніченко А.Н. Наукові і правові основи методики розслідування окремих видів злочинів: дис. … докт. юрид. наук. Харків, 1967. 509 с.

3. Коновалова В.О., Шепітько В.Ю. Криміналістична тактика: теорії і тенденції. Харків: Гриф, 1997. 256 с.

4. Криміналістика: підручник / за ред. В.М. Шевчука. Харків: Право, 2024. 1008 с.

5. Тіщенко В.В. Теоретичні і практичні основи методики розслідування злочинів: монографія. Одеса: Фенікс, 2007. 260 с.

6. Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія. Харків: Право, 2018. 952 с.

7. Шевчук В.М. Тактичні операції у криміналістиці: теоретичні засади формування та практичної реалізації: монографія. Харків: Апостіль, 2013. 440 с.

DOI https://doi.org/10.32837/11300.33580

Торбас Олександр
доктор юридичних наук, професор,
завідувач кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–1465–4238
e–mail:torbas.oleksandr@gmail.com

ДО ПОНЯТТЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

У тезах досліджено сучасні підходи до розуміння поняття електронних доказів у кримінальному процесі та проаналізовано основні наукові позиції щодо визначення їх правової природи. Зроблено висновок, що основні проблеми використання електронних доказів у кримінальному провадженні пов’язані не стільки з відсутністю законодавчого визначення цього поняття, скільки зі складністю їх належної фіксації, збереження та подальшого процесуального використання.

Ключові слова: кримінальний процес, докази, доказування, електронні докази

Torbas Oleksandr
Doctor of Law, Professor,
Head of the Department of Criminal Procedure at
National University «Odesa Law Academy»,
Odesa, Ukraine

THE CONCEPT OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEDURE

The theses examine modern approaches to understanding the concept of electronic evidence in criminal procedure and analyze the main scientific positions regarding the determination of its legal nature. It is concluded that the main problems associated with the use of electronic evidence in criminal proceedings are related not so much to the absence of a legislative definition of this concept as to the difficulties of its proper collection, preservation, and further procedural use.

Keywords: criminal procedure, evidence, proving, electronic evidence.

Стрімкий розвиток інформаційних технологій та цифровізація суспільних відносин зумовили суттєве зростання ролі електронної інформації у кримінальному провадженні. Сьогодні значна частина відомостей, які можуть мати доказове значення, створюється, передається та зберігається в електронній

формі – у мобільних телефонах, комп'ютерах, хмарних сервісах, месенджерах та інших цифрових системах. У зв'язку з цим особливої актуальності набуває питання визначення правової природи електронних доказів, їх місця у системі доказування та особливостей використання у кримінальному процесі. Так, КПК України лишається єдиним процесуальним кодексом, який не містить поняття «електронні докази», а всі відомості, які можуть мати доказове значення та які перебувають у цифровому вигляді, будуть оцінюватись як «типові» джерела доказів, які передбачені ст. 84 КПК України. У зв'язку з цим особлива увага практиків приділяється науковим дослідженням сутності поняття «електронні докази» у кримінальному провадженні.

Варто зауважити, що вчені досить активно досліджували це питання. Так, електронні докази розглядають як «інформацію, що зберігається в електронному вигляді на будь–яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах та відповідає вимогам ст. 84 КПК України» [1, с. 112]; «дані про обставини, що мають значення для кримінального провадження й існують у нематеріальному вигляді в межах технічного носія чи каналу зв'язку та сприйняття і дослідження яких можливе за допомогою технічних засобів і програмного забезпечення» [2, с. 211] тощо. О.Г. Козицька зробила висновок, що «за своєю суттю електронний доказ є цифровим об'єктом, який був засобом чи знаряддям вчинення кримінального правопорушення, зберіг електронно–цифрові сліди кримінального правопорушення, був предметом або об'єктом вчинення кримінального правопорушення або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [3, с. 420].

Також вчена зазначає, що за своєю природою електронний доказ являє собою цифровий об'єкт, який може виконувати різні функції у механізмі кримінального правопорушення. Зокрема, він може виступати засобом або знаряддям його вчинення (наприклад, шкідливе програмне забезпечення, використане для несанкціонованого доступу до інформації, чи телеграм–канал, створений з метою збуту наркотичних засобів тощо). Крім того, електронний доказ може містити електронно–цифрові сліди кримінального правопорушення, зокрема відеозаписи з камер спостереження із зафіксованим зображенням правопорушника, метадані щодо часу входу конкретного користувача до автоматизованої системи, інформацію про електронні перекази коштів, переданих як неправомірна вигода, та інші подібні відомості. Також цифровий об'єкт може бути предметом кримінального правопорушення (наприклад, вебсайт із порнографічними матеріалами) або об'єктом кримінально протиправного посягання, як–от незаконно поширюваний у мережі Інтернет об'єкт авторського права чи викрадена криптовалюта. Окрім цього, електронні докази можуть містити іншу інформацію, здатну підтверджувати факти та обставини, що мають

значення для кримінального провадження, зокрема характеризувати особу обвинуваченого через відомості, розміщені у соціальних мережах [3, с. 420].

Не можна стверджувати, що не були зроблені спроби ввести поняття «електронний доказ» до КПК України [4], проте КПК і досі лишається єдиним процесуальним кодексом, в якому законодавчо не закріплено дане поняття. Значна кількість і практиків, і вчених стверджує, що такі зміни мають бути введені максимально оперативно, адже це значно ускладнює процес доказування щодо кримінальних правопорушень, які вчиняються, наприклад, у кіберпросторі. В той же час більш виваженою вигладяє позиція, відповідно до якої введення в КПК даного терміну не вирішіть основні проблеми, які виникають під час використання таких відомостей. Основна складність виникає не у розумінні, а у фіксації та подальшому використанні таких доказів. Наприклад, фактично єдиним способом фіксації відомостей, отриманих з відкритих джерел, досі лишається складання протоколу огляду веб–сайтів, що вимагає від слідчого виконати багато паперової роботи лише для того, щоб зберегти відео або фото з відкритих джерел на фізичний носій. Тому основний напрям вдосконалення має бути направлений не стільки на визначення сутності даного поняття (хоча применшувати значення цього питання теж не варто), скільки на забезпечення законного і одночасно з цим легкого способу фіксації та використання електронних доказів.

Перелік використаних джерел:

1. Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. Проблеми законності. 2019. Вип. 146. С. 179–191.

2. Сіренко О.В. Електронні докази у кримінальному провадженні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2019. Вип. 14. С. 208–212.

3. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2020. № 8. С. 418–421.

4. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів від 01.09.2020 р. № 4004. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6977

DOI https://doi.org/10.32837/11300.33581

Федоров Владислав
аспірант кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID ID: https://orcid.org/0000–0000–0000–0000
e–mail: fedorov.vlad02@gmail.com

ОБСТАНОВКА ВЧИНЕННЯ РОЗБІЙНИХ НАПАДІВ ІЗ ЗАСТОСУВАННЯМ ВОГНЕПАЛЬНОЇ ЗБРОЇ У ВОЄННИЙ ТА ПОСТВОЄННИЙ ПЕРІОД

Досліджено особливості обстановки вчинення розбійних нападів із застосуванням вогнепальної зброї у воєнний та поствоєнний період. Визначено її основні елементи, вплив воєнних факторів на механізм злочинної діяльності та значення для криміналістичної практики.

Ключові слова: розбійний напад, вогнепальна зброя, обстановка вчинення злочину, воєнний стан, поствоєнний період, криміналістична характеристика, слідова картина.

Fedorov Vladyslav
postgraduate student of the Department of Criminalistics, Forensic Examinations and Polygraphology, National University »Odesa Law Academy», Odesa, Ukraine

THE SITUATION REGARDING ROBBERIES INVOLVING THE USE OF FIREARMS DURING THE WAR AND IN THE POST–WAR PERIOD

This study examines the specific characteristics of the circumstances surrounding armed robberies involving the use of firearms during the wartime and post–war periods. It identifies the key elements of these circumstances, the impact of wartime factors on the dynamics of criminal activity, and the implications for forensic practice.

Key words: robbery, firearms, circumstances of the offence, martial law, post–war period, forensic profile, crime scene evidence.

Обстановка вчинення кримінального правопорушення традиційно розглядається як один із ключових елементів криміналістичної характеристики злочинів, оскільки вона відображає сукупність об’єктивних умов, за яких здійснюється злочинна діяльність, та справляє безпосередній вплив на спосіб підготовки, вчинення і приховування кримінального правопорушення [1]. Особливого значення дослідження обстановки набуває під час розслідування розбійних нападів, учинених із застосуванням вогнепальної зброї, оскільки саме

ця категорія злочинів характеризується високим рівнем суспільної небезпеки, значною ймовірністю заподіяння тяжких тілесних ушкоджень або смерті потерпілим, а також суттєвими труднощами у встановленні та документуванні обставин події.

В умовах воєнного стану в Україні та в перспективі поствоєнного періоду спостерігається істотна трансформація криміногенного середовища, що безпосередньо впливає на характер розбійних нападів із використанням вогнепальної зброї. Збройна агресія спричинила значне поширення різних видів стрілецької зброї, боєприпасів, вибухових пристроїв та інших засобів ураження серед населення. Частина такої зброї перебуває у законному володінні військовослужбовців, представників правоохоронних органів та осіб, залучених до виконання завдань територіальної оборони, проте певна її кількість незаконно потрапляє до цивільного обігу. За таких умов вогнепальна зброя дедалі частіше використовується як інструмент вчинення корисливо–насильницьких кримінальних правопорушень, зокрема розбоїв.

Під обстановкою вчинення розбійних нападів із застосуванням вогнепальної зброї доцільно розуміти систему просторових, часових, соціально–психологічних, організаційних та інших умов, у межах яких здійснюється підготовка, реалізація та приховування злочинного посягання. До її структури належать місце події, час вчинення злочину, особливості навколишнього середовища, наявність або відсутність свідків, рівень технічної оснащеності об’єкта посягання, умови воєнного або поствоєнного функціонування відповідної території, а також поведінка учасників кримінального провадження.

Однією з характерних рис воєнного періоду є зміна просторової структури злочинності. Значна кількість розбійних нападів вчиняється у районах, які безпосередньо зазнали негативного впливу бойових дій або розташовані поблизу зон ведення бойових операцій. У таких місцях спостерігається часткове руйнування інфраструктури, зниження ефективності систем відеоспостереження, перебої в роботі засобів зв’язку та електропостачання, що створює сприятливі умови для злочинної діяльності. Крім того, значне переміщення населення, наявність внутрішньо переміщених осіб та високий рівень соціальної мобільності ускладнюють ідентифікацію злочинців та встановлення можливих свідків події.

Для воєнного періоду характерним є розширення кола об’єктів злочинного посягання. Якщо у мирний час основними цілями розбійних нападів були фінансові установи, торговельні заклади, пункти обміну валют, ювелірні магазини та окремі громадяни, то в умовах війни злочинний інтерес поширюється також на гуманітарні вантажі, транспортні засоби волонтерських організацій, склади матеріально–технічного забезпечення, логістичні центри, підприємства критичної інфраструктури та осіб, діяльність яких пов’язана з обігом значних сум готівки або цінного майна [2]. В окремих випадках об’єктами нападів стають особи, які отримують компенсаційні виплати, гуманітарну допомогу або інші матеріальні ресурси.

Суттєвий вплив на обстановку вчинення розбійних нападів справляє час їх реалізації. У період дії комендантської години злочинці нерідко використовують зменшення кількості громадян на вулицях та обмежену присутність випадкових свідків. Водночас окремі групи правопорушників, навпаки, вчиняють напади у денний час, маскуючи свою діяльність під виконання військових або правоохоронних функцій. Використання військової форми одягу, спеціального спорядження, автомобілів із тактичними позначеннями та інших елементів маскування дозволяє злочинцям вводити потерпілих в оману та мінімізувати ризик викриття на початковому етапі злочинної діяльності.

Особливістю сучасної обстановки є також високий рівень організованості значної частини таких злочинів. Розбійні напади із застосуванням вогнепальної зброї нерідко здійснюються групою осіб із чітким розподілом функцій між учасниками. Одні особи здійснюють збір інформації про майбутній об’єкт посягання, інші забезпечують придбання або зберігання зброї, треті безпосередньо реалізують напад, а окремі учасники відповідають за транспортування викраденого майна та приховування слідів злочину. У зв’язку з цим місце безпосереднього нападу часто є лише одним із елементів більш складної злочинної діяльності, яка охоплює значну територію та передбачає використання декількох локацій.

У воєнний період істотно змінюється характер застосування вогнепальної зброї. Якщо раніше зброя здебільшого використовувалася як засіб психологічного впливу на потерпілого, то нині частіше спостерігається її реальне застосування для придушення опору, залякування або усунення свідків. Наявність бойового досвіду у частини правопорушників підвищує рівень їх підготовленості до використання зброї та здійснення насильницьких дій. Це призводить до збільшення кількості випадків заподіяння тяжких тілесних ушкоджень під час розбійних нападів та ускладнює процес затримання озброєних злочинців.

Важливим компонентом обстановки є інформаційне середовище, у якому здійснюється злочинна діяльність. Сучасні злочинці активно використовують цифрові технології для збору відомостей про потенційних потерпілих, відстеження маршрутів пересування, координації дій співучасників та контролю за оперативною обстановкою. Соціальні мережі, месенджери, сервіси геолокації та відкриті електронні ресурси нерідко стають джерелом інформації про майновий стан потерпілих, місця зберігання матеріальних цінностей або особливості режиму роботи об’єктів, які плануються для нападу.

У поствоєнний період криміногенна ситуація також може залишатися складною через значну кількість незареєстрованої зброї, соціально–економічні труднощі, процеси демобілізації та необхідність адаптації окремих категорій населення до мирного життя. За таких умов існує ризик формування стійких кримінальних груп, які використовуватимуть незаконно отриману зброю для вчинення корисливо–насильницьких злочинів. Відповідно обстановка розбійних

нападів характеризуватиметься збереженням високого рівня озброєності злочинців, їх мобільності та здатності швидко змінювати місце перебування.

Для криміналістичної практики дослідження обстановки вчинення розбійних нападів із застосуванням вогнепальної зброї має важливе значення, оскільки дозволяє формувати типові версії щодо особи злочинця, способу його дій, джерел походження зброї та можливих напрямів подальшого переміщення. Аналіз особливостей місця події, характеру використаної зброї, способу проникнення до об'єкта, маршруту відходу та інших елементів обстановки сприяє встановленню механізму злочину й визначенню оптимального комплексу слідчих (розшукових) дій та оперативно–розшукових заходів [3].

Таким чином, обстановка вчинення розбійних нападів із застосуванням вогнепальної зброї у воєнний та поствоєнний період характеризується комплексом специфічних ознак, зумовлених наслідками збройного конфлікту, поширенням зброї серед населення, трансформацією криміногенного середовища та зміною структури злочинності. Її характерними рисами є використання територій із порушеною системою безпеки, розширення кола об'єктів посягання, підвищення рівня організованості злочинних груп, активне використання цифрових технологій та зростання небезпеки реального застосування вогнепальної зброї. Урахування зазначених особливостей є необхідною передумовою розроблення ефективних криміналістичних рекомендацій щодо виявлення, розкриття та розслідування таких кримінальних правопорушень.

Перелік використаних джерел:

1. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів: монографія. Одеса: Фенікс, 2007. 260 с.

2. Ягольник О. М. Способи вчинення розбійних нападів на інкасаторів. Європейські перспективи. № 2, 2020. С. 117–124.

3. Галаган В. І., Яковенко М. О. Особливості методики розслідування нерозкритих грабежів і розбоїв минулих років: монографія. МВС України, Луган. держ. ун–т внутр. справ ім. Е. О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. 256 с.

DOI https://doi.org/10.32837/11300.33582

Федорчук Олександр
кандидат юридичних наук,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0009–0002–1945–8647
e–mail: criminalistic@onua.edu.ua

КОРЕЛЯЦІЙНІ ЗАЛЕЖНОСТІ СТРУКТУРНИХ ЕЛЕМЕНТІВ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ПОСАДОВИХ ОСІБ ТА ВПЛИВ ЇХ ПІЗНАННЯ НА ПРОЦЕС РОЗСЛІДУВАННЯ

Акцентована увага на важливості пізнання кореляційних залежностей під час пізнання злочинної діяльності посадових осіб як у межах оперативно–розшукової діяльності: так і досудового розслідування. Окреслені окремі форми кореляційних залежностей між елементами злочинної діяльності зважаючи на статус посадової особи, рівень її повноважень та окремі інші чинники. Визначені основні напрями використання результатів такої пізнавальної діяльності під час безпосереднього здійснення досудового розслідування такої категорії кримінальних правопорушень.

Ключові слова: злочинна діяльність, посадова особа, механізм злочинної діяльності, криміналістичне пізнання, кореляційні залежності.

Fedorchuk Oleksandr
Candidate of Law
Associate Professor, Department of Criminalistic, Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

CORRELATION DEPENDENCES OF STRUCTURAL ELEMENTS OF CRIMINAL ACTIVITY OF OFFICIALS AND THE INFLUENCE OF THEIR KNOWLEDGE ON THE INVESTIGATION PROCESS

The emphasis is on the importance of knowing correlation dependencies when learning about the criminal activity of officials both within the framework of operational and investigative activities: and pre–trial investigation. Certain forms of correlation dependencies between elements of criminal activity are outlined, taking into account the status of the official, the level of his authority and certain other factors. The main

directions of using the results of such cognitive activity during the direct implementation of pre–trial investigation of this category of criminal offenses are determined.

Keywords: criminal activity, official, mechanism of criminal activity, forensic cognition, correlation dependencies.

Пізнання злочинної діяльності як під час оперативно–розшукового документування, так і під час досудового розслідування є комплексним процесом[1;3], який за своєю гносеологічною спрямованістю має забезпечити виявлення та встановлення не лише обставин, які підлягають доказуванню у межах конкретного кримінального провадження, а й інших важливих складових, котрі впливають на прийняття стратегічних та тактичних рішень. Безумовно, що на усіх етапах кримінального переслідування, одним із центральних об'єктів такого пізнання є механізм злочинної діяльності, який як теоретична категорія доволі детально досліджений на монографічному рівні провідними науковцями[2]. У той же час, слушно звернути увагу, що під час пізнання його структурних елементів вагоме значення має не скільки вивчення кожного із них автономно, скільки встановлення кореляційних залежностей між ними, що доволі фрагментарно розглянуто у межах наук кримінально–правового циклу[4]. Більше того, саме такий пізнавальний акцент є одним із пріоритетів під час розслідування кримінальних правопорушень у сфері службової діяльності, які характеризують складними технологіями реалізації, наявністю корупційної інфраструктури та активною протидією кримінальному переслідуванню з боку фігурантів.

Перш за все, необхідно звернути увагу, що кореляційні залежності структурних елементів злочинної діяльності посадових осіб становлять складну багаторівневу систему взаємозумовлених кримінально значущих факторів, які формують внутрішню логіку функціонування механізму таких форм злочинної діяльності. У сучасній криміналістичній доктрині дослідження таких залежностей набуває особливого значення, оскільки дозволяє не лише встановлювати окремі ознаки протиправної поведінки, а й виявляти приховані закономірності взаємодії між суб'єктом злочину, способом реалізації злочинного наміру, характером управлінських функцій, системою комунікацій, матеріальними слідами та результатами злочинної діяльності. Саме кореляційний аналіз структурних компонентів злочинної діяльності посадових осіб створює можливість переходу від фрагментарного сприйняття окремих фактів до комплексного моделювання механізму протиправної поведінки у сфері службової діяльності.

Сутність кореляційних залежностей у структурі злочинної діяльності полягає у встановленні стійких функціональних, інформаційних, організаційних та поведінкових зв'язків між окремими елементами кримінальної протиправності. Такі зв'язки можуть мати прямий, опосередкований, латентний або циклічний характер. Вони проявляються у взаємній зумовленості службового статусу особи та способу вчинення злочину, між рівнем владних повноважень та механізмом приховування протиправної діяльності, між організаційною структурою установи

та формою незаконного розподілу матеріальних ресурсів. У цьому аспекті злочинна діяльність посадових осіб не є хаотичним набором окремих дій, а функціонує як цілісна адаптивна система, в межах якої кожен структурний елемент змінюється під впливом інших складових, що і характеризує суть кореляційних залежностей між ними.

Особливе значення має кореляційний взаємозв'язок між посадовим статусом суб'єкта та змістом обраної ним технології злочинної діяльності. Чим вищий рівень адміністративних або управлінських повноважень має посадова особа, тим складнішого та багаторівневого характеру набуває механізм реалізації злочинного наміру. У таких випадках спостерігається тенденція до використання прихованих управлінських рішень, багатоступеневих схем фінансового маскування, маніпуляцій із документацією та створення штучних процедурних бар'єрів для контролюючих органів. Водночас нижчий рівень службових повноважень зазвичай корелює із примітивними способами незаконного збагачення, які мають більш очевидний характер і залишають значну кількість матеріальних та документальних слідів.

Кореляційні залежності також простежуються між функціональними обов'язками посадової особи та характером предмета злочинного посягання. Посадові особи, діяльність яких пов'язана з розподілом бюджетних ресурсів, значно частіше використовують механізми фіктивного фінансування, штучного завищення вартості робіт або маніпуляцій із тендерними процедурами. Натомість особи, наділені контрольними чи дозвільними функціями, тяжіють до корупційних форм злочинної діяльності, пов'язаних із незаконним впливом на прийняття рішень, штучним створенням адміністративних перешкод або вибірковим застосуванням нормативних вимог. Таким чином, функціональний зміст службової компетенції прямо впливає на модель злочинної поведінки та визначає специфіку механізму злочинної діяльності.

Важливою складовою кореляційного аналізу є взаємозалежність між способом вчинення злочину та моделлю його приховування та подальшою посткримінальною поведінкою. У сфері службової злочинності способи приховування майже ніколи не існують автономно, а формуються паралельно із самою злочинною схемою. Це зумовлено високим рівнем професійної обізнаності посадових осіб щодо механізмів державного контролю, аудиту та внутрішньої перевірки. У результаті виникає своєрідна кримінальна симетрія, за якої кожна дія щодо незаконного отримання вигоди супроводжується заздалегідь підготовленим механізмом документального або організаційного маскування. Така залежність дозволяє прогнозувати окремі елементи механізму приховування навіть за наявності мінімального обсягу вихідної інформації.

Суттєве криміналістичне значення має кореляція між структурою міжособистісних зв'язків посадових осіб та стійкістю злочинної діяльності. Чим вищий рівень інтеграції суб'єкта у систему неформальних службових комунікацій,

тим складнішими стають механізми виявлення та документування злочинної діяльності. У таких умовах формується феномен колективної латентності, за якого окремі учасники злочинної схеми виконують вузько спеціалізовані функції та володіють лише фрагментарною інформацією про загальний механізм протиправної діяльності. Це забезпечує високий рівень конспірації та ускладнює процес доказування. Одночасно зростає кореляційна залежність між тривалістю злочинної діяльності та ступенем її інституційного прикриття.

Окремого наукового аналізу потребує взаємозв'язок між інформаційним середовищем функціонування посадової особи та характером злочинної активності. В умовах цифровізації управлінських процесів дедалі більшого значення набувають інформаційно–аналітичні кореляції між електронним документообігом, цифровими слідами, фінансовими транзакціями та поведінковими моделями суб'єкта. Використання електронних систем управління створює одночасно як нові можливості для прихованої злочинної діяльності, так і додаткові джерела цифрових слідів, здатних відображати приховані закономірності злочинної поведінки. Саме тому сучасний криміналістичний аналіз службової злочинності дедалі частіше базується на побудові багатовекторних кореляційних моделей, які дозволяють виявляти аномальні управлінські рішення, нетипові фінансові операції та штучно сформовані адміністративні процеси.

Кореляційні залежності проявляються також у взаємозв'язку між мотиваційною сферою посадової особи та характером злочинної діяльності. Матеріальна мотивація здебільшого корелює із систематичними формами незаконного збагачення, тоді як владно–статусна мотивація обумовлює використання службових повноважень для забезпечення політичного, корпоративного або адміністративного впливу. У ряді випадків формується змішаний тип мотиваційної структури, де матеріальна вигода поєднується з прагненням до збереження управлінського контролю або посилення особистого впливу в межах державного чи корпоративного середовища.

У методологічному аспекті дослідження кореляційних залежностей структурних елементів злочинної діяльності посадових осіб має надзвичайно важливе значення для формування криміналістичних методик розслідування. Встановлення стійких закономірностей між окремими компонентами злочинного механізму дозволяє здійснювати прогнозування прихованих елементів злочинної діяльності, моделювати поведінку суб'єктів, визначати потенційні джерела доказової інформації та формувати оптимальні тактичні рішення. У цьому контексті кореляційний підхід трансформується з суто статистичного інструмента у самостійну методологічну основу аналітичного забезпечення протидії службовій злочинності.

Таким чином, кореляційні залежності структурних елементів злочинної діяльності посадових осіб відображають внутрішню системність та закономірність функціонування службової злочинності як складного соціально–правового явища.

Їх наукове дослідження дозволяє не лише поглибити розуміння механізму протиправної поведінки у сфері службової діяльності, але й сформувати нові підходи до криміналістичного прогнозування, виявлення латентних зв'язків, побудови аналітичних моделей та вдосконалення системи доказування у кримінальних провадженнях щодо досліджуваної категорії.

Перелік використаних джерел:

1. Багран С.С. Пізнавальна діяльність слідчого: криміналістичний та процесуальний аспекти : дис… докт. філософ. : 081. Кропивницький. 2024. 258 с.

2. Волобуєв А.Ф. Механізм злочину та його зв'язок з концептуальними положеннями криміналістики: монографія. Кривий Ріг. Вид. Р.А. Козлов. 2019. 122 с.

3. Ковальова О.В. Інформаційна парадигма досудового розслідування в Україні: теоретико–прикладний аспект : монографія. Одеса. Видавничий дім «Гельветика». 2022. 320 с.

4. Синчук С.С. Кореляційні залежності між елементами криміналістичної характеристики та їх використання у методиці розслідування вбивств: автореф. дис… канд. юрид. наук: 12.00.09. Харків. 2024. 20 с.

DOI https://doi.org/10.32837/11300.33585

Хижняк Євген
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–8263–0353
e–mail: khyzhniak@onua.edu.ua

СУТНІСТЬ КООРДИНАЦІЇ ТА ВЗАЄМОДІЇ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ З РІЗНИМИ СУБ'ЄКТАМИ ПІД ЧАС ОПЕРАТИВНО–РОЗШУКОВОГО ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЗА ФАКТОМ ВЧИНЕННЯ УМИСНИХ ВБИВСТВ

Тези розкривають сутність координації підрозділів кримінальної поліції в розслідуванні умисних вбивств. Розмежовано поняття «координація» та «взаємодія», визначено функції та завдання координаційної діяльності. Обґрунтовано роль координації в забезпеченні оперативно–розшукового супроводження проваджень.

Ключові слова: координація, взаємодія, кримінальна поліція, умисне вбивство, досудове розслідування, оперативно–розшукове забезпечення.

Khyzhniak Yevhen
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminalistics, Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

THE ESSENCE OF COORDINATION AND INTERACTION BETWEEN CRIMINAL POLICE UNITS AND VARIOUS SUBJECTS DURING THE OPERATIONAL–SEARCH SUPPORT OF CRIMINAL PROCEEDINGS REGARDING INTENTIONAL HOMICIDES

The theses reveal the essence of coordination between criminal police units in the investigation of intentional homicides. The concepts of «coordination» and «interaction» are differentiated, and the functions and tasks of coordination activities are defined. The role of coordination in ensuring the operational–search support of criminal proceedings is substantiated.

Keywords: coordination, interaction, criminal police, intentional homicide, pre–trial investigation, operational–search support.

Деякі вчені пропонують серед структурних елементів окремої криміналістичної методики виділяти положення, що стосуються «забезпечення координації дій правоохоронних органів у розслідуванні та взаємодії з контролюючими та іншими державними органами, об'єднаннями громадян» [2, с.243]. Попри той факт, що у криміналістичній літературі категорії «взаємодія» та «координація» іноді вживаються як тотожні поняття, слід погодитися із думкою вчених, які вказують на різну природу такої діяльності. Досить влучно, на нашу думку, зазначають В. Шамрай та І. Олійник, що координація становить собою функцію одного із суб'єктів системи, у той час як взаємодія відображає один із принципів діяльності, засіб контактів із суб'єктами інших систем [7, с.63], однак як «координація», так і «взаємодія» отримують своє втілення саме через контакт конкретних суб'єктів. Ю.С. Назар вказує на той факт, що координація повинна розглядатися як необхідна передумова узгодженої діяльності кількох суб'єктів, які мають спільну мету, тобто як організаційна основа процесу взаємодії. При цьому її функції не вичерпуються організаційним етапом, у зв'язку із чим вона може проявлятися на етапах безпосередньої реалізації рішення (безпосередньої взаємодії) та контролю за виконанням такого рішення [5, с.18]. Такий підхід підкреслює організаційно–управлінську роль координації безпосередньо під час реалізації взаємодії між суб'єктами в рамках певного кримінального провадження та її вплив на якість здійснення такої взаємодії. Відповідно координація та взаємодія не є та не можуть бути тотожними поняттями в межах досудового розслідування, проте повинні досліджуватися науковцями при розробці криміналістичних положень із урахуванням специфіки кожного із них.

В.І. Коломієць визначає, що координація передбачає чітке визначення завдань, ролей та обов'язків різних органів, а також забезпечення ефективного обміну інформацією, ресурсами та досвідом між ними, а також вказує, що вона спрямована на досягнення спільних цілей у сфері розслідування злочинів. На його думку, роль координації полягає у тому, що вона дозволяє: оптимально поєднати зусилля та ресурси органів досудового розслідування в процесі здійснення спільної діяльності; усунити дублювання повноважень різних органів державної влади, а також розподілити їх завдання та функції в процесі здійснення досудового розслідування; виробити єдиний підхід до розслідування кримінальних проваджень та забезпечити узгодженість дій органів досудового розслідування; розробити єдину Стратегію боротьби зі злочинністю взагалі, а також у напрямку проведення досудового розслідування, зокрема; забезпечити швидкий обмін інформацією між суб'єктами взаємодії [1, с.147–148]. Наведений підхід дозволяє розглядати координацію через призму забезпечення належного здійснення взаємодії, що є досить доречним на нашу думку.

Подібним чином до співвідношення координації та взаємодії підходить С. Сівко, пропонуючи розглядати взаємодію як категорію, яка поглинає поняття координації, оскільки остання спрямована на створення відповідного режиму

відносин між суб'єктами, при якому виконання ними узгоджених завдань досягається з найменшими витратами сил, засобів та часу [6, с.29]. Такий підхід є досить логічним, адже в межах розслідування конкретного кримінального правопорушення необхідність у координації дій учасників такого розслідування виникає лише після того, як вони починають взаємодіяти між собою задля вирішення конкретних завдань розслідування та досягнення його кінцевої мети.

При цьому важливою обставиною здійснення координації є її нормативна регламентованість. У цьому сенсі слушною є думка В.О. Мощонського, який координацію правоохоронних органів пропонує розглядати як визначену законодавством України організаційно–упорядковуючу діяльність спеціально уповноважених органів та посадових осіб, яку спрямовано на формування і створення умов, визначення основних пріоритетів та забезпечення інших аспектів взаємодії правоохоронних органів із виконання покладених на них завдань і функцій [4, с.14].

У рамках досліджуваної нами тематики координація може бути визначена як спрямована на створення організаційно–управлінських умов якісної взаємодії різних суб'єктів досудового розслідування діяльність, що забезпечує досягнення кінцевої мети за рахунок оптимального поєднання ресурсів та методів роботи таких суб'єктів.

Визначення координації саме через призму діяльності обумовлено її специфікою та змістом, адже їй властиві усі загальні принципи, притаманні всякій свідомій діяльності: постановка мети, обумовленої потребами й інтересами особистості; вибір об'єкта, на який буде спрямована діяльність; вибір способів, засобів та умов досягнення поставленої мети; розрахунок власних сил і можливостей та вирішення питання про доцільність підключення додаткових учасників; виділення й оцінка проміжних та кінцевих результатів; корегування процесу організації та здійснення кожного наступного етапу діяльності [3, с.16].

У контексті взаємодії підрозділів кримінальної поліції з різними суб'єктами під час оперативно–розшукового забезпечення кримінального провадження за фактом вчинення умисних вбивств, координація є ключовим елементом для забезпечення ефективності розслідування. Вона передбачає узгодження дій різних суб'єктів для досягнення спільної мети – швидкого, повного та неупередженого розслідування злочину.

Завдання координації включають:

визначення пріоритетів та напрямків протидії злочинності, що передбачає розробку та впровадження пріоритетів кримінально–правової політики, а також сучасних підходів до боротьби зі злочинністю, зокрема умисними вбивствами. Координація допомагає визначити основні напрямки та проблемні аспекти в діяльності правоохоронних органів щодо запобігання та протидії таким злочинам, ґрунтуючись на аналізі їх структури, динаміки та прогнозуванні тенденцій;

розробку та реалізацію спільних заходів, спрямованих на: своєчасне виявлення та розкриття умисних вбивств; забезпечення швидкого реагування та

ефективного збору первинної інформації оперативними підрозділами кримінальної поліції; припинення злочинної діяльності, у тому числі – попередження вчинення злочинцем інших кримінально караних діянь; повне та всебічне розслідування за рахунок узгодження оперативно–розшукових заходів (наприклад, збір орієнтуючої інформації, встановлення свідків, спостереження) з процесуальними діями слідчого (наприклад, допити, обшуки, вилучення доказів) для забезпечення їх взаємодоповнюваності та ефективності; усунення причин та умов, що сприяли вчиненню умисних вбивств, та розробка пропозицій для їх усунення на системному рівні;

забезпечення ефективного постійного та своєчасного обміну необхідною інформацією між підрозділами кримінальної поліції, слідчими, прокурорами та іншими залученими суб'єктами;

оптимізацію використання сил та засобів за рахунок уникнення дублювання функцій та дій суб'єктів, залучених до процесу розслідування вбивства, що підвищує ефективність роботи кожного підрозділу;

вдосконалення законодавства шляхом підготовки пропозицій щодо вдосконалення законодавства у сфері боротьби зі злочинністю, зокрема щодо розслідування умисних вбивств, попередження їх учинення та оперативно–розшукового забезпечення процесу досудового розслідування.

Перелік використаних джерел:

1.Коломієць В.І. Поняття та значення координації органів досудового розслідування в Україні. Теоретичні та прикладні проблеми судової експертизи і криміналістики : тези доп. учасників наук.–практ. конф. (Харків, 30 вер. 2022 р.). Харків, 2022. С.146–148.

2.Кофанов А. В., Кобилянський О. Л., Кузьмічов Я. В., Удовенко Ж. В., Хільченко С. В. Криміналістика: питання і відповіді. Навч. посіб. Київ: Центр учбової літератури, 2011. 280 с.

3.Методика і тактика розслідування злочинів : навч.–метод. посіб. / В. В. Тіщенко, О. П. Ващук, Ю. О. Гресь [та ін.]. 4–те вид., допов. й уточ. Одеса : Юридична література, 2019. 108 с.

4.Мощонський В.О. Адміністративно–правові засади взаємодії та координації діяльності правоохоронних органів в умовах дії правового режиму воєнного стану: автореф.дис….канд.юрид.наук: 12.00.07. Кропивницький, 2025. 20 с.

5.Назар Ю.С. Взаємодія територіальних органів внутрішніх справ із місцевими органами виконавчої влади та органами місцевого самоврядування у профілактиці адміністративних правопорушень: дис….канд. юрид. наук: 12.00.07. Львів, 2006. 210 с.

6.Сівко С. «Взаємодія» І «Координація»: масштабність понять. «Legea şi viaţa. 2013. №6. С. 27–29.

7.Шамрай В., Олійник І. Шамрай В. Поняття і суть взаємодії, її значення. Прокуратура, людина, держава. 2004. №1(31). С.60–67.

DOI https://doi.org/10.32837/11300.33588

Чигрина Галина
кандидат юридичних наук, доцент,
доцент кафедри правоохоронної діяльності
Державного податкового університету,
м. Ірпінь, Україна
ORCID: https://orcid.org/0000–0002–4546–0145
e–mail:05071961gl@gmail.com

КЛЮЧОВІ ФОРМИ КРИМІНАЛІСТИЧНОГО СУПРОВОДУ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: СВІТОВИЙ ДОСВІД ДЛЯ УКРАЇНИ

У тезах визначені та проаналізовані ключові форми криміналістичного супроводу правоохоронної діяльності, які включають перехід від виключно паперових запитів до цифровізованих алгоритмів взаємодії, спільних слідчих груп та транскордонних систем автоматизованого обміну криміналістичними даними. Акцентовано увагу на тому, що впровадження світового досвіду криміналістичного супроводу правоохоронної діяльності в Україні вимагає трансформації традиційного процесуального залучення криміналістів у гнучкі інструменти міжнародного та міжвідомчого співробітництва, передбачає належне законодавче забезпечення; сучасне технічне та технологічне оснащення правоохоронної діяльності; відповідне оновлення навчальних програм підготовки правоохоронців.

Ключові слова: правоохоронна діяльність, криміналіст, криміналістичний супровід, взаємодія, співробітництво

Chyhryna Halyna
Ph.D. in Law, Associate Professor,
Associate Professor of the Department of Law Enforcement Activity
State Tax University,
Irpin, Ukraine

KEY FORMS OF FORENSIC SUPPORT OF LAW ENFORCEMENT ACTIVITIES: WORLD EXPERIENCE FOR UKRAINE

The theses identify and analyze key forms of forensic support for law enforcement activities, which include the transition from exclusively paper–based requests to digitalized interaction algorithms, joint investigation teams, and cross–border systems of automated forensic data exchange. It is emphasized that the implementation of world experience in forensic support for law enforcement activities in Ukraine requires the transformation of the traditional procedural involvement of forensic scientists into

flexible tools of international and interagency cooperation, provides for appropriate legislative support; modern technical and technological equipment for law enforcement activities; and appropriate updating of training programs for law enforcement officers.

Keywords: law enforcement activities, a criminalist, forensic support, interaction, cooperation

Криміналістичний супровід правоохоронної діяльності, як комплекс наукових, технічних та організаційних заходів, забезпечує фахове виявлення, фіксацію та дослідження фактичних даних, сприяючи розкриттю і розслідуванню кримінальних правопорушень у розумні строки, дозволяючи правоохоронним органам надавати суду беззаперечні, науково обґрунтовані докази.

Складовими криміналістичного супроводу правоохоронної діяльності традиційно є: техніко–криміналістичне забезпечення (застосування спецтехніки, ДНК–аналізу, дактилоскопії та балістики на місці події та під час проведення інших процесуальних дій); тактичний супровід (розробка планів (схем) допитів, обшуків, відтворення обстановки вчиненого кримінального правопорушення); методичний супровід (створення алгоритмів, розробка методик розслідування конкретних видів кримінальних правопорушень (наприклад, кіберзлочинів, фактів (схем) ухилення від оподаткування, шахрайства з фінансовими ресурсами тощо); експертний супровід (проведення судових експертиз, залучення профільних спеціалістів–криміналістів тощо).

Вивчення сучасних сфер, форм і напрямків криміналістичного супроводу правоохоронної діяльності дозволяє зробити висновки про те, що останнім часом, частіше за інші, в Україні використовуються: цифрова криміналістика (для пошуку доказів у смартфонах, хмарних сховищах та комп'ютерних мережах); аналіз ДНК (для ідентифікації особи за найменшими біологічними слідами, що наразі стало особливо актуальним у зв'язку з воєнними діями на території нашої держави) та участь криміналістів у проведенні процесуальних дій (з метою фахового та оперативного виявлення, фіксації та вилучення матеріальних слідів вчиненого злочину).

Ключовими міжнародними формами криміналістичного супроводу правоохоронної діяльності, які доцільно запроваджувати і в Україні, можна вважати:

1. електронні запити та цифрові платформи криміналістичного аналізу

У країнах ЄС та США криміналістичний супровід правоохоронної діяльності (залучення криміналістів) відбувається через цифрові системи управління завданнями (Task Management Systems). Правоохоронці створюють цифровий ордер (клопотання, запит), який автоматично визначає найближчого вільного фахівця потрібного профілю (наприклад, експерта з оподаткування, крипто–транзакцій або розвідки на основі відкритих джерел (Open Source Intelligence – OSINT), який надає відповідну онлайн–консультацію чи письмовий висновок (звіт).

Значення для України цього досвіду – відхід від паперової бюрократії. Замість класичного письмового запиту (клопотання) впроваджується інтеграція модулів криміналістичного супроводу в єдину Інформаційно–комунікаційну систему правоохоронних органів, яка повинна існувати в державі. Це дозволятиме правоохоронцю (слідчому (детективу), співробітнику оперативного підрозділу) за кілька кліків викликати криміналіста відповідного профілю і одержувати необхідну фахову консультацію, за потреби – письмовий звіт (висновок).

2. залучення правоохоронцями криміналістів через інструменти Спільних слідчих груп (англ. – Joint Investigation Team – JIT)

У зв'язку з розслідуванням воєнних злочинів та діяльності організованих угруповань (транснаціональної, транскордонної злочинності, терористичних актів тощо), залучення правоохоронцями України іноземних криміналістів стало критичною потребою.

На підставі угод з Євроюстом та Міжнародним кримінальним судом (МКС) іноземні експерти–криміналісти залучаються до роботи безпосередньо під час проведення процесуальних дій (огляду місця події, обшуку тощо).

Значення для України цієї форми криміналістичного супроводу у військовий час є особливо актуальним. Форма заяви, в межах кримінального провадження, трансформувалася у міжнародний запит (клопотання) про надання правової допомоги або тристоронні меморандуми. Іноземні криміналісти привозять власні ДНК–лабораторії та 3D–сканери для фіксації руйнувань, інтегруючи свої звіти безпосередньо у кримінальні провадження (наприклад: системи ANDE Rapid DNA (зокрема модель ANDE 6C) – це портативні повністю автоматизовані ДНК–лабораторії для ідентифікації людини за 90–105 хвилин. Вони дозволяють отримувати точні результати (ДНК–профілі) без спеціальних наукових знань у польових умовах або на місці події).

3. аутсорсинг та залучення недержавних («приватних») криміналістів

Сучасні кіберзлочини та фінансові шахрайства (махінації) потребують специфічних знань, яких часто немає у штатних експертів–криміналістів правоохоронного органу.

Вдалим прикладом міжнародного досвіду є модель Forensic Science Providers (Велика Британія, США), коли правоохоронці можуть залучати акредитовані приватні лабораторії або незалежних сертифікованих криміналістів.

Зазначена форма криміналістичного супроводу може мати практичне значення також і для правоохоронної діяльності України. Так, чинний Кримінальний процесуальний кодекс України (далі – КПК України) дозволяє залучати спеціалістів на договірній основі стороною захисту чи обвинувачення. Сучасною підставою для такого криміналістичного супроводу може бути цивільно–правова угода (контракт) про надання експертних/консультаційних послуг у поєднанні з процесуальним залученням спеціаліста за постановою слідчого (прокурора, детектива – стаття 110 КПК України (Процесуальні

рішення)). (Наприклад: такий підхід може бути актуальним при виявленні та розслідуванні правоохоронцями кіберінцидентів за участю «білих хакерів», як спеціалістів. (Білі хакери (або етичні хакери) – це фахівці з кібербезпеки, які використовують свої навички для злому комп'ютерних систем, мереж і додатків з дозволу їхніх власників. Їхня головна мета – виявити вразливості до того, як ними скористаються зловмисники («чорні хакери»), і допомогти компаніям посилити захист. Знання і навички «білих хакерів» правоохоронці можуть використовувати у протидії злочинності, як альтернативу криміналістичним знанням).

4. непроцесуальні (консультаційні) форми криміналістичного супроводу через відеозв'язок

Дистанційне залучення до правоохоронної діяльності криміналістів зменшує витрати часу та коштів.

Як показує міжнародний досвід, використання захищених каналів зв'язку для отримання оперативних «онлайн–консультацій» криміналіста під час проведення процесуальної дії (огляду місця події, обшуку тощо) в режимі реального часу значно скорочує строки досудового розслідування та посилює у рази можливості правоохоронців щодо виявлення, фіксації та вилучення речових слідів вчиненого правопорушення.

Українські правоохоронці успішно можуть запроваджувати «онлайн–консультації» криміналістів, оформлюючи їх у формі доручення на проведення дистанційної консультації (через системи відеоконференцзв'язку). При цьому криміналіст, перебуваючи у головній лабораторії, координує дії слідчого (детектива) на периферії через боді–камеру.

Враховуючи викладене, можна зробити наступні висновки:

криміналістичний супровід правоохоронної діяльності значно підсилює можливості правоохоронців у протидії злочинності;

– перспективним завданням є створення Єдиної державної інформаційно–комунікаційної системи та розробка уніфікованого електронного бланка заяви (запиту, клопотання) на криміналістичний супровід правоохоронної діяльності, де чітко розмежовуватимуться завдання для криміналіста: відбір біологічних зразків, фіксація цифрових доказів, кримінальний аналіз зав'язків тощо;

– залучення українських правоохоронних органів до баз даних системи Prüm, яка діє з 2005 року. Хоча мережа (система) Prüm діє насамперед у межах Європейського Союзу, через механізми співпраці до неї можуть залучатися правоохоронні органи з інших країн (зокрема України) або міжнародні організації на кшталт Interpol, що займаються питаннями розслідування кримінальних правопорушень. Це сприятиме повноцінному автоматизованому використанню іноземного криміналістичного досвіду, забезпечить фаховий криміналістичний супровід вітчизняної правоохоронної діяльності, дозволить оперативно протидіяти транскордонній злочинності та тероризму шляхом надсилання електронних запитів з метою визначення результату у режимі «hit/no–hit»

(«збіг/відсутність збігу») (автоматичний збіг) за профілями ДНК, відбитками пальців та даними реєстрації транспортних засобів країн ЄС.

Таким чином, вивчення міжнародного досвіду показало, що сучасні форми криміналістичного супроводу правоохоронної діяльності передбачають перехід від виключно паперових запитів до цифровізованих алгоритмів взаємодії, спільних слідчих груп (англ. – Joint Investigation Team – JIT) та транскордонних систем автоматизованого обміну криміналістичними даними. Але впровадження цього досвіду в Україні не можливе без трансформації традиційного процесуального залучення експертів–криміналістів (спеціалістів) у гнучкі інструменти міжнародного та міжвідомчого співробітництва.

DOI https://doi.org/10.32837/11300.33589

Чіпко Наталія
кандидат юридичних наук, доцент кафедри криміналістики,
судових експертиз та поліграфології
Національний університет «Одеська юридична академія»,
м. Одеса,Україна
ORCID: https://orcid.org/0000–0002–4008–817X
e–mail:chipkonatali@gmail.com

СУЧАСНЕ ШАХРАЙСТВО У СФЕРІ ПЛАТІЖНИХ СИСТЕМ

У тезах розглядаються сучасні форми шахрайських дій у сфері платіжних систем. Особливу увагу приділено найпоширенішим видам та схемам шахрайства. Проаналізовано основні причини поширення незаконних операцій у платіжному середовищі, недосконаліть систем захисту та активний розвиток цифрових технологій.

Ключові слова: шахрайство, веб–сайт, цифрові платіжні системи, фішинг, фармінг, скімінг.

Nataliia Chipko
Candidate of Law, Associate Professor of the Department of Criminalistics,
Forensic Examinations and Polygraphology
National University «Odesa Law Academy»,
Odesa, Ukraine

MODERN FRAUD IN THE SPHERE OF PAYMENT SYSTEMS

The theses examine modern forms of fraudulent actions in the field of payment systems. Particular attention is paid to the most common types and schemes of fraud. The main reasons for the spread of illegal transactions in the payment environment, the imperfection of protection systems and the active development of digital technologies are analyzed.

Key words: fraud, website, digital payment systems, phishing, farming, skimming.

Інтенсивний розвиток інформаційно–комунікаційних технологій у XXI столітті суттєво трансформував повсякденне життя людей. Сучасна реальність неможлива без активного використання цифрових інструментів, мобільних пристроїв та всесвітньої мережі Інтернет. Важливою складовою цифрової інфраструктури стали інноваційні фінансові сервіси, серед яких особливе значення мають електронні гаманці та інші види безготівкових платіжних систем.

Для безлічі користувачів електронні платіжні технології стали звичним засобом здійснення фінансових операцій. Вони забезпечують оперативність,

зручність і певний рівень захисту коштів у порівнянні з традиційними методами зберігання грошей. Однак, незважаючи на вдосконалення технічних рішень і заходів безпеки, цифрове фінансове середовище продовжує залишатися вразливим. Для зловмисників ці системи – не лише об'єкт інтересу, а й поле для реалізації злочинної діяльності.

У зв'язку з поширенням цифрових платіжних інструментів та зростанням обсягів електронних транзакцій, особливої значущості набуває дослідження протиправної діяльності у цій сфері. Шахрайські дії, спрямовані на заволодіння фінансовими ресурсами користувачів електронних гаманців, становлять серйозну загрозу для інформаційної безпеки та економічної стабільності. Тому вивчення механізмів, методів і характерних ознак цифрового шахрайства є надзвичайно актуальним у сучасних умовах та потребує системного наукового аналізу.

Однією з найпоширеніших ознак цифрового шахрайства є отримання повідомлення, дзвінка чи листа від невідомої особи або організації. Такі звернення зазвичай супроводжуються створенням штучного відчуття терміновості або загрози. Наприклад, користувачу можуть повідомити про нібито заблокований банківський рахунок, помилку під час оплати чи навіть виграш у розіграші. Головна мета подібних повідомлень – спонукати людину до негайних дій, не залишаючи часу на перевірку інформації.

Шахраї часто використовують гіперпосилання, які ведуть на підроблені веб–сторінки, що зовні нагадують офіційні сайти банків, державних установ чи відомих компаній. На таких сторінках користувача можуть попросити ввести логін, пароль або дані банківської картки. У деяких випадках у листах додаються вкладення з шкідливими файлами, відкриття яких може призвести до зараження пристрою вірусом чи програмою для зчитування інформації.

Ще однією типовою рисою цифрового шахрайства є використання емоційних маніпуляцій. Повідомлення можуть містити погрози, залякування або, навпаки, обіцянки швидкої вигоди. Наприклад, людину переконують, що її рахунок буде заблоковано, якщо вона негайно не перерахує кошти або не введе дані. Такі методи спрямовані на те, щоб змусити жертву діяти імпульсивно, без критичного осмислення ситуації.

Часто шахрайські повідомлення можна розпізнати за мовними особливостями. У них трапляються граматичні, орфографічні чи пунктуаційні помилки, неприродний стиль мовлення або використання слів, що нехарактерні для офіційного спілкування. Також підроблені листи можуть містити неправильно оформлені логотипи компаній, спотворені кольори або інші дрібні, але показові невідповідності.

Ще однією важливою ознакою є незначні відмінності в адресах веб–сайтів. Зловмисники можуть замінювати одну літеру, цифру чи символ, роблячи домен майже ідентичним до справжнього (наприклад, paypaI.com замість paypal.com). Крім того, варто звертати увагу на наявність захищеного протоколу з'єднання

(https). Якщо сайт його не має, введення особистих даних на такій сторінці є небезпечним.

Щодо видів шахрайства у сфері платіжних систем, слід зазначити, що вищевказані риси мають на меті допомогти особі розпізнати, що це кіберзлочинність, однак, для повного розуміння подій, необхідні знання, який саме вид досліджуваних протиправних дій використовується у певній ситуації.

Фішинг є найпоширенішим і водночас найстарішим видом шахрайства в Інтернеті. Його суть полягає у тому, що злочинці надсилають електронні листи, сповіщення або повідомлення в соціальних мережах, які зовні виглядають як офіційні звернення від банку, служби підтримки чи платіжної системи. У таких повідомленнях користувач отримує прохання перейти за вказаним посиланням.

Перейшовши за посиланням, людина потрапляє на підроблений сайт, який візуально майже не відрізняється від справжнього. На ньому користувач самостійно вводить свої персональні або фінансові дані – логін, пароль, номер картки, CVV–код тощо. У результаті ця інформація потрапляє безпосередньо до шахраїв.

Так, у справі № 674/1782/19 Дунаєвським районним судом Хмельницької області встановлено, що з метою власного збагачення, обвинувачений, з власного комп`ютера за допомогою орендованого обладнання хостинг провайдера ТОВ «ТаймВеб» https://timeweb.com створив та розмістив ряд фейкових ресурсів, які імітували можливість перегляду аудіовізуальних творів чи отримання ряду безкоштовних стікерів до соціальних мереж, однак були налаштовані таким чином, що здійснювали викрадення інформації введеної користувачами мережі про власні логіни та паролі доступу до облікових записів. Посилання на фішингові ресурси обвинувачений розповсюджував в соціальній мережі «Вконтакте» https://vk.com, зокрема з облікових записів користувачів аккаунтів здобутих незаконним шляхом [1].

Скімінг (Skimming) спочатку виник як спосіб крадіжки даних банківських карток через спеціальні пристрої, встановлені на банкоматах чи платіжних терміналах. Проте сьогодні цей вид шахрайства отримав нові онлайн–форми.

В інтернет–просторі «веб–скімінг» полягає у впровадженні шкідливих скриптів у код вебсайтів або онлайн–магазинів. Коли користувач здійснює покупку чи вводить дані своєї картки, зловмисники перехоплюють цю інформацію в момент введення. Найчастіше такі атаки відбуваються на сайтах, де недостатньо оновлюється система безпеки. Жертви навіть не підозрюють про компрометацію своїх даних, оскільки процес оплати виглядає абсолютно стандартно.

Фармінг (Pharming) – більш складний і технічно витончений метод шахрайства. Його суть полягає у перенаправленні користувача на фальшивий сайт навіть тоді, коли він вводить правильну адресу офіційного ресурсу. Це може відбуватися через зараження комп’ютера шкідливим програмним забезпеченням або зміну налаштувань DNS–сервера. У результаті користувач бачить сторінку, яка виглядає ідентично справжній, проте всі введені дані (логін, пароль, номер

картки) автоматично передаються на сервери шахраїв. Фармінг особливо небезпечний тим, що навіть досвідчений користувач не завжди здатен одразу розпізнати підміну.

Для запобігання таким атакам важливо використовувати лише захищені з'єднання (https) та регулярно оновлювати антивірусні системи.

Соціальна інженерія (Social Engineering) – це маніпулятивна технологія, що ґрунтується не на технічному зламі систем, а на психологічному впливі на людину. Метою шахраїв є змусити користувача добровільно розкрити конфіденційні дані або виконати дії, вигідні зловмисникам – наприклад, підтвердити переказ, надіслати код із SMS або встановити шкідливу програму.

Зазвичай шахраї представляються працівниками банку, служби підтримки, поліції чи навіть близькими знайомими. Вони створюють ситуації довіри або страху, наприклад, повідомляючи про нібито блокування картки чи спробу несанкціонованого входу. Людина, прагнучи швидко вирішити проблему, надає потрібну інформацію, не перевіривши її достовірність.

У сучасних умовах соціальна інженерія часто поєднується з використанням зламаних акаунтів у соціальних мережах або підроблених профілів, що підвищує ефективність шахрайських схем.

Одним із нових різновидів шахрайства є створення фіктивних онлайн–платформ, що видають себе за легальні фінансові сервіси або інвестиційні компанії. Такі ресурси пропонують користувачам «вигідні умови інвестування», «швидкий прибуток» або «гарантовані виплати». На перший погляд, сайт може мати професійний дизайн, ліцензійні символи, відгуки «реальних користувачів» і навіть технічну підтримку. Насправді ж усі внесені кошти надходять безпосередньо на рахунки шахраїв. Коли користувач намагається вивести свої гроші, платформа просто припиняє роботу або блокує обліковий запис.

Такі схеми активно поширюються через рекламу в соціальних мережах, фейкові новини та фішингові розсилки. Особливо часто вони орієнтовані на початківців, які не мають достатнього досвіду в інтернет–інвестиціях або криптовалютних операціях.

Отже, інтенсивна цифровізація фінансового простору зумовила появу нових можливостей для користувачів, проте водночас – створила підґрунтя для виникнення різноманітних форм шахрайства у сфері електронних платежів. Боротьба з цифровим шахрайством має стати пріоритетним напрямом державної політики у сфері інформаційної безпеки. Усвідомлення ризиків, критичне мислення та відповідальна поведінка користувачів у цифровому середовищі є ключовими чинниками забезпечення фінансової безпеки в умовах стрімкого розвитку інформаційно–комунікаційних технологій.

Перелік використаних джерел:

1. Вирок Дунаєвського районного суду Хмельницької області від 13.12.2019 по справі № 674/1782/19. URL:https://reyestr.court.gov.ua/Review/86357578.

DOI https://doi.org/10.32837/11300.33586

Черниш Юрій
аспірант кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», м. Одеса, Україна
ORCID: https://orcid.org/0009–0000–7029–740X
e–mail:chernyshyurii@onua.edu.ua

ТИПОВІ СИТУАЦІЇ ПОДАЛЬШОГО ЕТАПУ РОЗСЛІДУВАННЯ КОНТРАБАНДИ КУЛЬТУРНИХ ЦІННОСТЕЙ

У тезах аналізуються критерії початку подальшого етапу розслідування контрабанди культурних цінностей. Обґрунтовано типологію слідчих ситуацій за рівнем протидії підозрюваних. Досліджено важливість координації дій між слідчими, оперативними та митними підрозділами як чинника ефективності розслідування злочинів.

Ключові слова: подальший етап розслідування, контрабанда, культурні цінності, слідча ситуація, протидія, взаємодія правоохоронних органів.

Chernysh Yuriy
postgraduate student of the Department of Criminalistics, Forensic Examinations and Polygraphology, National University «Odesa Law Academy», Odesa, Ukraine

TYPICAL SITUATIONS OF THE SUBSEQUENT STAGE OF INVESTIGATING THE SMUGGLING OF CULTURAL PROPERTY

The theses analyze the criteria for the beginning of the subsequent stage of investigating the smuggling of cultural property. A typology of investigative situations based on the level of suspect opposition is substantiated. The importance of coordination between investigative, operational, and customs units as a factor in the effectiveness of crime investigation is explored.

Keywords: subsequent stage of investigation, smuggling, cultural property, investigative situation, opposition, interaction of law enforcement agencies.

Аналіз існуючих наукових точок зору та матеріалів практики, щодо визначення моменту початку подальшого етапу розслідування, то переважна більшість вчених схиляється до думки про необхідність врахування появи у досудовому розслідувані фігури підозрюваного. Так, О.С. Тарасенко пропонує виокремлювати слідчі ситуації подальшого етапу розслідування з моменту вручення особі повідомлення про підозру [3, с.454]. Т.А. Воліков стверджує, що

фактично подальший етап розслідування починається після завершення проведення комплексу першочергових слідчих (розшукових) дій, які спрямовані на вирішення тактичних завдань початкового етапу розслідування, зокрема встановлення особи правопорушника та його затримання [1, с.984]. І якщо із твердженням про те, що подальший етап розслідування необхідно виділяти із появою у слідства підозрюваної особи, що безпосередньо змінює інформаційний характер слідчої ситуації, то дискусійним все ж таки видається теза щодо затримання особи або вручення повідомлення про підозру. На практиці є досить поширеними випадки, коли слідство у процесуальному порядку зібрало достатню кількість доказів та ідентифікувало злочинця або групу злочинців, однак у силу ряду обставин (особа переховується від слідства, перебуває за кордоном, перебуває на окупованій території тощо) безпосереднє затримання та вручення повідомлення про підозру є об'єктивно неможливим.

В.М. Шевчук пропонує вирізняти типові слідчі ситуації наступного (подальшого) етапу розслідування на основі врахування критерію ставлення підозрюваного до повідомлення про підозру [4, с.149], а О.А. Самойленко пропонує також враховувати наявність протидії з боку підозрюваного [2, с.189].

На нашу думку, в контексті специфіки розслідування контрабанди культурних цінностей в основу виділення типових слідчих ситуацій подальшого етапу розслідування доцільним є врахування саме критерію протидії, що дозволяє визначити наступні їх види:

Ситуація 1. Ситуація мінімальної (пасивної) протидії, коли підозрюваний формально співпрацює зі слідством, не чинить активного тиску на свідків, а лінія захисту будується на запереченні умислу або посиланні на «необізнаність» щодо культурної цінності предмета.

Ситуація 2. Ситуація активної доказової протидії, коли підозрюваний системно заперечує обставини, подає альтернативні документи, надає суперечливі пояснення, ініціює проведення повторних експертиз, оскаржує процесуальні рішення та всіляко затягує досудове розслідування.

Ситуація 3. Ситуація протидії розслідуванню контрабанди культурних цінностей з боку ОЗУ, яка характеризується високим рівнем організованості, корупційними ризиками впливу на правоохоронні органи, експертні установи та свідків, узгодженням показань між членами ОЗУ та переховуванням від слідства.

Як випливає із описаних типових слідчих ситуацій та тактичних засобів вирішення тактичних завдань, окреслених нами в рамках кожної із названих ситуацій, важливою складовою забезпечення якісного виявлення та розслідування злочинної діяльності, пов'язаної із контрабандою культурних цінностей, виступає належним чином організована та здійснювана взаємодія між слідчими та оперативними підрозділами правоохоронних органів з митними органами, а також іноземними колегами та міжнародними інституціями.

Перелік використаних джерел:

1.Воліков Т.А. Типові слідчі ситуації подальшого етапу розслідування кримінальних правопорушень проти власності. Наукові перспективи. 2024. № 7(49). С.981–990.

2.Самойленко О.А. Типові слідчі ситуації наступного етапу розслідування злочинів, скоєних у кіберпросторі. Актуальні проблеми держави і права. 2019. Вип.82. С.188–194.

3.Тарасенко О.С. Типові слідчі ситуації подальшого етапу досудового розслідування незаконного зайняття рибним промислом. Право і суспільство. 2024. №1. Т.2. С.452–456.

4.Шевчук В.М. Слідча ситуація: поняття, структура, види та їх значення для оптимізації розслідування злочинів. Юридичний науковий електронний журнал. 2014. №1. С.146–150. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17277/1/Shevchuk_146–150.pdf

DOI https://doi.org/10.32837/11300.33590

Чумак Сергій
кандидат юридичних наук,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–0486–1890
e–mail: sergey25100104@gmail.com

ЦИФРОВІЗАЦІЯ СУДОВОЇ ФОТОГРАФІЇ У ЗБИРАННІ ДОКАЗІВ

У тезах проаналізовано значення цифрової судової фотографії, як сучасного засобу документування місць скоєння злочинів, а також у судово–експертній діяльності як важливого способу збирання та закріплення доказів, необхідних для будь–якого розслідування на місці злочину.

Ключові слова: судова фотографія, цифровізація, правоохоронні органи, методи, експертне дослідження.

Chumak Serhiy
Candidate of Law, Associate Professor of the Department of Criminalistics,
Forensic Examinations and Polygraphology,
National University «Odesa Law Academy»,
Odesa, Ukraine

DIGITALIZATION OF FORENSIC PHOTOGRAPHY IN EVIDENCE COLLECTION

The thesis analyzes the importance of digital forensic photography as a modern means of documenting crime scenes, as well as in forensic activities as an important way of collecting and securing evidence necessary for any investigation at a crime scene.

Key words: forensic photography, digitization, law enforcement agencies, methods, expert research.

Сучасна злочинність постійно вдосконалює свої методи і боротьба з нею старими методами не приносить очікуваних результатів. Тому настала необхідність переозброєння слідчих, оперативних і експертно–криміналістичних підрозділів правоохоронних органів новими технічними засобами виявлення, фіксації, дослідження та пред'явлення суду об'єктивних доказів у наочному вигляді.

Одним із таких засобів є криміналістична (судова) фотографія та її цифрофікація.

Спеціальні прийоми фотозйомки, дозволяють виявити неозброєним оком різноманітні об'єкти, наприклад, дописки в документах, сліди травлення,

підчищення, а також зафіксувати швидкоплинні процеси, наприклад, обертання кулі під час польоту, зіткнення транспортних засобів та ін.

До виникнення цифрової фотографії стадії фотографічного процесу були більш розтягнуті в часі і складалися з наступних етапів:

1) фотозйомка;

2) негативний процес;

3) позитивний процес.

Для отримання видимого зображення з прихованого зображення утвореного на плівці, необхідно послідовно виконати ряд наступних дій:

– фотоматеріал проявити у спеціальному розчині – проявнику;

– фотоматеріал швидко (попередньо) промити, вилучаючи залишки проявника;

– фотоматеріал опустити у спеціальний розчин – фіксаж, тобто його закріпити;

– фотоматеріал ретельно (остаточно) промити у проточній воді та висушити.

Позитивний процес є останньою стадією фотографічного процесу — отримання з негативного матеріалу позитивного зображення – фотокартки. Обробка позитивного матеріалу аналогічна негативному процесу.

Значним недоліком фотозйомки на плівку — це втрата зображення на будь–якому етапі під час негативного процесу.

Другим недоліком такої фотографії є те, що негативи і фотографії з часом псуються, зникає зображення, особливо якщо навіть було незначне порушення негативного або позитивного процесу

Поява цифрової фотографії кардинально змінила цілі напрями криміналістики — від балістики з її тонким аналізом мікрорельєфу на кулях і гільзах до трасології, що вивчає сліди злому, та автоматизованої дактилоскопії. Сьогодні цифрові фотографії міцно увійшли до судової практики, як самостійні докази; проте їх використання вимагає виконання суворих вимог, таких як необхідно підтверджувати справжність знімків та надавати повну документацію про процес зйомки.

При цьому зберігається традиційний криміналістичний підхід – усі фотоматеріали обов’язково копіюються на захищені носії та супроводжуються вичерпними протоколами зйомки. Цифрова фотографія відкриває широкі перспективи для криміналістичної практики. Насамперед, вона є ефективним інструментом фіксації речових доказів — після оцифрування та комп’ютерної обробки такі знімки можуть бути включені безпосередньо до експертного висновку або оформлені у вигляді фототаблиць.

Особливої значимості цифрова фотографія набуває в дослідницькій роботі — комп’ютерні методи обробки зображень дозволяють виявляти малопомітні сліди, аналізувати закреслені або залиті тексти, відновлювати пошкоджені документи, значно підвищуючи інформативність та доказову цінність матеріалів.

Цифрова фотографія відкриває можливості для автоматизації багатьох видів експертиз.

Сучасні цифрові технології значно спростили процес створення, редагування та розповсюдження фотоматеріалів, що природно породжує сумніви в їхній достовірності.

Сучасні технології обробки зображень відкривають перед експертами нові горизонти — тепер складні фотографічні дослідження можна проводити в стислий термін, при цьому відпадає потреба у трудомісткому підборі спеціальних фотоматеріалів та методів їх обробки.

Переваги цифрових фото:

– можливість розглянути фотографії без зволікання — це основна перевага знімків: їх можна детально вивчити і у разі потреби повторити зйомку;

– зняті кадри не потребують прояву;

– простота у використанні;

– якість зображення;

– надійність;

– ефективність;

– можливість збільшення зображення;

– безстрокове збереження цифрового зображення.

Основні недоліки цифрофікації судової фотографії пов’язані з ризиками недостовірності доказів, складнощами перевірки достовірності знімків та недосконалістю законодавчої бази при оцінці цифрових доказів.

Згідно ст. 94 КПК України слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожен доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів — з точки зору достатності та взаємозв’язку для прийняття відповідного процесуального рішення.[1]

Положення про достовірність доказів стосується судової фотографії, коли виникають сумніви і необхідно встановити достовірність носія цифрової фотографії.

Ключові проблеми:

–вразливість до фальсифікації. Цифрові зображення легко піддаються ретушуванню, фотомонтажу та видаленню даних. Це знижує їх доказове значення, оскільки справжність кадру ставиться під сумнів.

–недостатня правова база. Інформація про час, дату, геолокацію та параметри зйомки може бути випадково спотворена (наприклад, при збою налаштувань камери) або навмисно змінена, що ускладнює прив’язку знімка до справи.

Існують різні методи дослідження та виявлення монтажу цифрових зображень. Але це кропітка та надто об'ємна робота, яка потребує значного часу та матеріальних затрат.

На сьогодні, розроблені методики дослідження ознак монтажу цифрових зображень на основі аналізу ентропії шумів. Програмне забезпечення дозволяє проводити дослідження з метою виявлення ознак монтажу на основі аналізу ентропії шумів цифрових зображень з максимізацією комплексного критерію, що враховує ентропію та дисперсію зображення. Воно може бути використано як на локальних комп'ютерах, так і з використанням потужного серверного обладнання у режимі віддаленого доступу через веб–інтерфейс, у тому числі, з використанням малопотужних мобільних терміналів користувача (смартфонів, планшетів, тощо), що суттєво полегшить роботу експертів з дослідження монтажу цифрових зображень або при встановленні їх достовірності (автентичності).[2, с.261]

На сьогоднішній день, незважаючи на недоліки цифрової фотографії, практично все перешло на цифрофікацію судової фотографії, але виконуючи фотографування необхідно враховувати можливості подальшого використання цифрової фотозйомки. Якщо це орієнтуюча або оглядова фотозйомка, яка в основному має інформаційне значення, то достатньо фотозйомку надавати як додаток до протоколу певної слідчої дії у виді фототаблиці. А такі фотознімки як вузловий та особливо детальний, які можуть використовуватись в експертному дослідженні, або можуть визвати сумніви суду в достовірності зображення, то необхідно буде надати і носій цієї цифрової фотографії, тому що тільки експертне дослідження може встановити факт монтажу або його відсутність. Це є основним недоліком цифрової фотографії відносно плівочної фотозйомки , коли до фотографії надавався негатив зображення на плівці.

Цифрова фотозйомка сьогодні залишається одним із найбільш ефективних та популярних способів фіксації інформації у кримінальному провадженні. Наступним етапом розвитку названої технології має стати 3D сканування криміналістично–значущих об'єктів, яке може бути здійснено з використанням фотограмметричного методу судової фотозйомки, що підкреслює актуальність дослідження сутності напрямків його застосування у кримінальному провадженні.

Перелік використаних джерел:

1.Кримінальний процесуальний кодекс України (Відомості Верховної Ради України (ВВР), 2013, № 9–10, № 11–12, № 13, ст.88)

2.Чорный С. В., О. Брендель О. І, А. Роман А. І. Виявлення ознак редагування цифрових зображень за допомогою методу стенографічного аналізу шумів. / Теорія і практика судової експертизи і криміналістики. №20. 2019., с. 253–263. https://doi.org/10.32353/khrife.2.2019.19

DOI https://doi.org/10.32837/11300.33591

Шереметов Сергій
завідувач лабораторії військових досліджень,
Київський науково дослідний інститут судових експертиз
Міністерства юстиції України,
м. Київ, Україна
ORCID: https://orcid.org/0009–0003–3381–5003
e–mail: serhii.sheremetov@kndise.gov.ua

КАДРОВЕ ЗАБЕЗПЕЧЕННЯ НДУСЕ ЯК СКЛАДОВА ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У ВІЙСЬКОВІЙ СФЕРІ

Проаналізовано проблеми, які виникають при проведенні судових військових експертиз, пов'язаних із військовими злочинами в Збройних Силах України (далі–ЗСУ) та правоохоронних органах, на які розповсюджуються статути ЗСУ, пов'язаних з їх повсякденною та оперативною (бойовою) та іншою діяльністю в умовах триваючої збройної агресії та воєнного стану в Україні. Приділено увагу проблемі комплектування підрозділів НДУСЕ з проведення військової експертизи кадрами. Визначено необхідність, удосконалення нормативної бази, формування спеціалізованих експертних осередків та впровадження сучасних інформаційних технологій. Окрему увагу приділено організаційно–правовим аспектам та практичним проблемам реалізації експертної діяльності у воєнний час.

Ключові слова: судова військова експертиза, криміналістика, воєнні злочини, військові кримінальні правопорушення, доказування, воєнний стан, військова техніка, озброєння.

Sheremetov Sergii
Head of the Military Research Laboratory
Kyiv Scientific Research Institute of Forensic Expertise
of the Ministry of Justice of Ukraine,
Kyiv, Ukraine

STAFFING OF RESEARCH INSTITUTIONS OF FORENSIC EXAMINATION AS A COMPONENT OF EXPERT SUPPORT FOR THE INVESTIGATION OF CRIMES IN THE MILITARY SPHERE

The problems arising during the conduct of forensic military examinations related to military crimes in the Armed Forces of Ukraine, hereinafter referred to as the AFU, and in law enforcement agencies subject to the statutes of the AFU, connected with their daily, operational, combat and other activities under the conditions of ongoing armed aggression and martial law in Ukraine, have been analyzed. Attention is paid to the

problem of staffing the units of research institutions of forensic examination responsible for conducting military examinations. The need to improve the regulatory framework, establish specialized expert units and introduce modern information technologies has been identified. Separate attention is paid to organizational and legal aspects, as well as practical problems of implementing expert activity during wartime.

Key words: forensic military examination, criminalistics, war crimes, military criminal offences, proving, martial law, military equipment, weapons.

Формулювання цілей статті. Аналіз сучасного стану судової військової експертизи в контексті кадрового забезпечення, визначення ключових окремих проблем та перспективи удосконалення судово–військової експертизи як системного інструменту кримінального процесу у сфері оборони.

Постановка проблеми. Незважаючи на досить короткій строк існування з початку створення, судова військова експертиза стрімко розвивається.

Беззаперечним є факт її актуальності не тільки в мирний час. Події сьогодення – відсіч Україною збройної агресії, підкреслюють її актуальність. Нажаль, саме під час ведення бойових дій, істотно зросла злочинність, пов’язана з Силами оборони України. Бойові дії є одним із каталізаторів стрімкого зростання військові кримінальні правопорушення та воєнних злочинів.

На сучасному етапі існування і розвитку, Україна повинна адекватно реагувати на виклики і загрози, які прийняли вкрай загрозливий характер. Їх можна поділити на 2 групи: внутрішні і зовнішні.

До внутрішніх проблем відносяться:

– гостра міжпартійна конфронтація, неспроможність поступитися політичними амбіціями, політична боротьба «на знищення» з використанням спекуляцій на питаннях безпеки, надмірного популізму, поступове зростання розриву між так званою політичною елітою та суспільством;

– критичне розшарування суспільства за регіональними, політичними, майновими, релігійними, мовними ознаками;

– плинність кадрів державного апарату, брак стратегічного державного підходу до планування стратегічного розвитку країни і суспільства, організації взаємодії залучених галузей і органів виконавчої влади, посадових осіб, мотивації та контролю організації з метою досягнення координації людських, фінансових, природних і технологічних ресурсів, необхідних для ефективного виконання завдань (менеджменту);

– не завжди зрілість демократичних інститутів, недостатня укомплектованість судової системи і як наслідок – перепони до забезпечення належного рівня дотримання прав і свобод громадян;

– розбалансованість системи національної безпеки через неузгодженість реформ у різних структурах сектору безпеки, послаблення можливостей

реагування на кризові явища, зростання протиріч між змістом і темпами реформування Збройних Сил, інших структур сектору безпеки, з одного боку, і процесом наближення України до членства в НАТО – з іншого;

– критичний стан озброєння та військової техніки, складнощі у забезпеченні матеріально–технічної та бойової підготовки Збройних Сил. [1]

Особливо необхідно відмітити наявність випадків викривлених морально–етичних норм життя суспільства, яке надає поштовх скоєнню кримінальних правопорушень. З цього приводу можна навести приклади, коли посадові особи вчиняють правопорушення у «гуманітарному» напрямку (зловживаючи у процесах «розподілу бюджетних коштів», «постачання продукції», «надання послуг» тощо), ставлячи за мету особисте збагачення. Така діяльність інколи набуває ланцюгового характеру і ставить під загрозу існування самої держави, органів влади. Враховуючи скоєння таких тяжких злочинів як розкрадання бюджетних коштів, постачання неякісної продукції в тому числі для Сил оборони України (амуніції, засобів індивідуального захисту, продуктів харчування), привласнення гуманітарної допомоги, незаконна виплата винагороди за фіктивну участь у бойових діях тощо, можна говорити про нову епоху злочинності, до якої мають причетність представники так званої «еліти» суспільства.

До головних зовнішніх загроз для національної безпеки України відноситься:

– послаблення дієвості міжнародного права, побудованого на застарілих принципах міжнародних інститутів, та відповідно – зменшення зовнішніх гарантій безпеки України;

– …;

– наявність глобальних ризиків і загроз, таких, як тероризм, розповсюдження ЗМУ, нелегальна міграція тощо. [1]

Особливо необхідно відмитити скоєння державами з високім економічним розвитком і, як наслідок, з високім

У зв’язку з існуванням чисельних небезпечних явищ в Україні суттєво посилюється значущість й збереження людського потенціалу держави: наукового, виробничого, демографічного. Здатного протистояти загрозам і забезпечувати розвиток держави. Важливим серед інших завдань є не лише збереження наукового потенціалу експертних установ, а й розвиток окремих галузей судової експертизи, які вийшли на передній план у розслідуванні злочинів в умовах війни.

З початком ведення бойових дій з метою відсічі Україною збройної агресії зріс показник правопорушень з боку військових службових (посадових) осіб за ознаками кримінальних правопорушень, передбачених КК України, які вчиняються при виконанні службових (посадових) обов’язків. До цього переліку можна віднести:

незаконне заволодіння представниками силових структур матеріальними засобами громадян України;

незаконне проникнення в житлові приміщення;

незаконне застосування стрілецької та іншої зброї відносно цивільного населення, в тому числі, яке спричинило загибель та поранення цивільного населення на блок–постах і населених пунктах, оселях громадян;

незаконне нарахування та отримання грошової винагороди за участь у бойових діях;

незаконне отримання благодійної (волонтерської) допомоги;

залишення озброєння і військової техніки (ОВТ), боєприпасів, матеріальних засобів (МЗ) в місцях ведення бойових дій;

прийняття управлінських рішень, які призвели до втрат ОВТ, боєприпасів, матеріальних запсобів, особового складу;

привласнення військовими службовими (посадовими) особами, у тому числі високопосадовцями, грошових коштів у великих розмірах;

закупівля майна і продуктів харчування за явно завищеними цінами з порушенням процедур закупівель тощо.

Деякі злочини, особливо у фінансово–господарській сфері, набули широкого розголосу, що викликає у населення України обурення, розчарування та недовіру до влади.

Тому пріоритетним завданням є необхідність всебічного забезпечення законності у сфері оборони, військового управління, діяльності Збройних Сил України, правоохоронних органів, на яких розповсюджуються вимоги Статутів Збройних Сил України.

Вирішення цього завдання потребує постійної відданої праці із запобігання, виявлення і розслідування правопорушень у тісної взаємодії з підрозділами державних експертних служб України, адже практично будь який процес доказування ґрунтується на результатах судових експертиз. [2, с.16]

На сучасному етапі судово–військова експертиза не лише сприяє розслідуванню кримінальних правопорушень, пов’язаних з військовою службою та військовими і воєнними злочинами, але й виконує стратегічну функцію – забезпечує формування належної доказової бази у контексті міжнародно – правової відповідальності держави – агресора.

Вона призначена для визначення правомірності та наслідків дій або бездіяльності посадових осіб військових формувань у рамках дотримання нормативних вимог і бойових завдань. Це дослідження має багатогранний характер і охоплює як матеріальні докази, так і комплексну оцінку основної бойової діяльності, документів та поведінки військовослужбовців, потребує спеціальних військових знань та міждисциплінарний підхід при проведенні військової експертизи – дослідження спектру (різноманітності) питань (напрямів) діяльності.

Якісне забезпечення кадрами НДУСЕ судовими експертами за спеціальністю 16.1 «Військові дослідження» є запорука якісних експертних висновків.

Зазначене вимагає від судового експерта за спеціальністю 16.1 «Військові дослідження» широкого спектру знань оперативно –тактичного та оперативно – стратегічного рівнів. Ці знання повинні бути необхідними і достатніми для виконання судових військових експертиз з урахуванням складності експертних досліджень.

Водночас судові військові експертизи істотно відрізняються за:

обсягом матеріалів кримінального провадження (МКП);

необхідністю аналізу документів оперативного (бойового) планування

(в тому числі таємних та цілком таємних, які знаходяться в режимно – секретних органах (РСО) відповідних правоохоронних структурах (СБУ, ДБР, прокуратура, інш.);

застосуванням спеціальних військових знань.

Міждисциплінарний підхід – спектр (різноманітність) питань (напрямів) діяльності, які підлягають експертизі та потребують індивідуального підходу (відсутні методики) при дослідженні діяльності:

посадових (службових) осіб та органів військового (іноді державного)

управління на стратегічному, оперативному та тактичному рівнях;

посадових (службових) осіб та структурних підрозділів, які не є

органами військового управління, але за дорученнями зазначених органів військового (іноді державного) управління здійснюють управління оборонними ресурсами;

посадових (службових) осіб та суб’єктів (органів військового

управління, військових частин, організацій, установ тощо).

Повсякденна діяльність та виконання оперативних (бойових) і спеціальних завдань Силами оборони (Міністерство оборони України, Збройні Сили України, Служба безпеки України, Державна прикордонна служба України, Національна гвардія України тощо) передбачають наявність відповідних знань і проведення досліджень за такими видами забезпечення:

1. оперативне (тактична та оперативна розвідка, забезпечення зв’язку,

інженерне, маскування, захист від зброї масового ураження, метеорологічне, навігаційне, картографічне, ППО, РЕБ тощо.);

2. авіаційно–технічне (метеорологічне, метрологічне, інженерно–авіаційне (озброєння, боєприпаси, інш.), аеродромно–технічне тощо);

3. військово–морське (мінно–торпедне, картографічне, навігаційне, метеорологічне, шкіперське, лоцманське, метрологічне, ракетне тощо.);

4. логістичне (матеріально технічне):

– фінансове (кошти на функціонування, виплати, закупівля озброєння, оновлення техніки);

– технічне забезпечення: ремонт, технічне обслуговування, виробництво та постачання озброєння та військової техніки (ОВТ), запасних частин, інструментів і приладдя (ЗІП);

– транспортне;

– утримання запасів паливно–мастильних матеріалів (ПММ), боєкомплектів, ЗІП, засобів зв'язку тощо;

– речове; продовольче; квартирно–експлуатаційне;

– танко–технічне; автотехнічне;

5. медичне (медична допомога, реабілітація, санаторно курортне, тощо);

6. морально–психологічне;

7. організаційно–правове (правове забезпечення: регулювання військової дисципліни, законності, відносин у сфері оборони законами України та нормативно правовими актами; кадрове забезпечення: підготовка, профкваліфікація, кадрове резервування, ротація, кадровий облік, кадрова політика, тощо).

Кожний вид забезпечення – окрема дисципліна і військовий експерт повинен знати (вивчити, з'ясувати) вид забезпечення при проведенні військової експертизи (дослідженні дій (бездіяльності) військових посадових осіб та обставин їх діяльності).

Під час проведення судової військової експертизи щодо дій (бездіяльності) вищого військово–політичного керівництва держави (Верховного Головнокомандувача, Міністра оборони України, Головнокомандувача Збройних Сил України, Голови Служби безпеки України тощо) експерт досліджує нормативно–правові акти, що регламентують діяльність зазначених посадових осіб, у тому числі документи з обмеженим доступом (таємні, цілком таємні).

Отже, вищевказане наочно свідчить про те, яким спектром знань повинен володіти судовий експерт при проведенні судової експертизи за спеціальністю 16.1 «Військові дослідження».

Судова військова експертиза як форма спеціального дослідження об'єктів, процесів і явищ військової діяльності 84до 2015 року науково – дослідними установами судових експертиз Міністерства юстиції України не проводилися. Зазначена експертиза була введена в дію наказом Міністерства юстиції України від 27.07.2015 № 1350/5.

Попри наявність нормативних і методичних основ, судово – військова експертиза стикається з рядом проблем: відсутність єдиних стандартів, складність технічної оцінки тактичних/оперативних дій військових частин (підрозділів), угрупувань військ (сил), обмеженість доступу експертів до секретної інформації, недосконалість механізмів взаємодії між органами слідства, прокуратури та військового управління, відсутність оновлених керівних документів з метою вирішення проблеми кадрового забезпечення, в тому числі комплектування підрозділів НДУСЕ для проведення військових досліджень.

На ринку праці в Україні мається доволі значна кількість офіцерів запасу, які мають освіту оперативно – тактичного та оперативно – стратегічного рівнів, досвід проходження дійсної військової служби, відповідають пред'явленим вимогам щодо володіння спеціальними знаннями. Щоб стати військовим судовим

експертом, їм потрібно пройти навчання з теоретичних, організаційних, процесуальних питань судової експертизи та стажування. Скласти іспит, отримати свідоцтво (стати атестованим судовим експертом) за спеціальністю. Значне збільшення постанов органів досудового розслідування про призначення судових військових експертиз, в тому числі комісійних та комплексних, вимагає якомога швидкого комплектування кадрами (судовими експертами) НДУСЕ для виконання військових експертиз.

Отже, програма навчання з теоретичних, організаційних, процесуальних питань судової експертизи, стажування, складання іспиту, отримання свідоцтва повинні відповідати сучасним викликам – бути скороченими за часом, формування групи (груп) для складання іспиту необхідно здійснювати не за принципом набрання не менш мінімально необхідної кількості осіб, а за принципом необхідності оперативного реагування на ускладнену обстановку стосовно військових і воєнних злочинів. Тобто процес атестування повинен бути постійним, конвеєрним, а не періодичним. Так би мовити «кулеметні курси», а для виключення браку в діяльності атестованого експерта, широко застосовувати інститут наставництва, обмін досвідом, проведення круглих столів, семінарів тощо.

Другий аспект, якій потребує вирішення, це організаційно–штатна структура підрозділу (–лів) якій (–яки) проводять військові дослідження в НДУСЕ. Вона повинна відповідати поточним і перспективним завданням.

Проведення різнопланових судових військових експертиз вимагає або збільшення штатної чисельності і комплектування кадрами, які мають освіту за різними напрямками (сухопутний, ППО, ВМС, авіаційний, спецвійська, фінансовий тощо) в монопідрозділі (лабораторія, відділ, сектор), або створення відділів (секторів) в лабораторії за напрямками проведення досліджень.

Аналіз змісту постанов та їх перелік питань, наряду з «класичними військовими питаннями», свідчить про тенденцію збільшення експертиз, проведення яких потребує не тільки загальновійськових знань експерта (–тів), а й спеціальних (профільних) знань та досвіду, щодо діяльності МО України і застосування ЗС України, їх видів та родів військ (Повітряних сил (ПС+ППО), Військово–морських сил (ВМС), Сил безпілотних систем (СБС), радіоелектронної боротьби (РЕБ), Сил спеціального призначення, інш. та їх структурних підрозділів (департаментів, головних управлінь, військових частин спеціального призначення тощо).

Актуальність і проблематика:

1. Стрімке зростання обсягу робіт у зв’язку з повномасштабною агресією (5 рік війни), збільшенням кількості проваджень за напрямом 16.1 «Військові дослідження» (воєнні злочини, злочини у військовій сфері та злочини проти національної безпеки України).

2. Розширення предмету досліджень: від класичних військово–управлінських рішень та дій/бездіяльності посадових осіб – до комплексних

економічних правопорушень у сфері оборонних закупівель, матеріально–технічного забезпечення, обігу військового майна, будівництва, логістики тощо.

3. Дефіцит методології й кадрів: чинні підходи судової військової експертизи переважно зберігають первісний стан із мінімальним оновленням, що ускладнює забезпечення єдиних стандартів якості висновків; брак експертів із релевантним досвідом у господарській/фінансовій сфері оборони.

4. Мультиагентність замовників (ДБР, СБУ, НПУ та ін.) створює різноманітність питань, які вимагають команд із комплементарними спеціальностями та чіткої координації, щоб уникнути затримок і відмов у прийнятті матеріалів.

5. Ризики недопустимості доказів через методичні прогалини або неузгодженість з процесуальними вимогами, що особливо критично у справах про воєнні злочини та злочини проти національної безпеки, резонансних злочинів.

6. Зростаюча кількість постанов про проведення експертиз

7. Невідповідність існуючої організаційно–штатної структури підрозділу (лабораторії, відділу, сектору) військових досліджень та дефіцит кадрів потребам проведення різноманітних видів експертиз за напрямом досліджень.

Нормативно–правові підстави:

1. Наказ Міністерства юстиції України від 08.10.1998 № 53/5 (Інструкція та Науково–методичні рекомендації) – визначає завдання, загальні вимоги до призначення та проведення експертиз/досліджень і необхідність належного методичного забезпечення в тому числі внесення змін.

2. Кримінальний процесуальний кодекс України (ст. 216) – визначає підслідність кримінальних правопорушень, що зумовлює різноплановість замовників експертиз (ДБР, СБУ, Національна поліція тощо) та потребу в міждисциплінарній експертизі.

3. Інші відомчі акти та методичні матеріали, що регулюють експертну діяльність у воєнний період та практику дослідження воєнних злочинів.

Пропонована цільова модель

Отже, з метою забезпечення спроможності підрозділу (лабораторії) оперативно та якісно виконувати зростаючий обсяг і складність судових військових експертиз у кримінальних провадженнях, пов’язаних із військовими, воєнними та злочинами проти національної безпеки, у т.ч. з елементами господарської діяльності органів військового управління та військових частин пропонується:

1. Створення потужних підрозділів в НДУСЕ як окремі структурні підрозділи для проведення різноманітних військових експертиз за спеціальністю 16.1 «Військові дослідження».

2. Для підвищення статусу та наукового потенціалу НДУСЕ ввести в штат підрозділу (лабораторії) наукові посади.

Виходячи з вищевикладеного, пропонується наступна організаційно–штатна структура підрозділу (лабораторії) в НДУСЕ:

варіант

Скорочення: ЛВД – лабораторія військових досліджень;

ВДДОВУ – відділ досліджень діяльності органів військового управління;

ВДДВ – відділ дослідження діяльності військ;

ВДДСВГД – відділ досліджень діяльності спеціальних військ, сил логістики, медичного забезпечення, оборонних закупівель та господарської діяльності;

СЕ – судовий експерт;

ПНС (НС) – провідний науковий (науковий) співробітник.

Завдання функції відділів:

оцінка рішень і дій/бездіяльності посадових осіб МОУ, органів військового управління та військових частин ЗС України; дослідження алгоритмів планування/застосування сил, управлінських процедур, документування й контролю;

аналіз відповідності дій військових посадових осіб (військовослужбовців) та посадових осіб (працівників ЗС України) вимогам НПА, доктринам, наказам, стандартам, бойовим статутам та міжнародного гуманітарного права.

Штатна чисельність та управління підрозділу (–лів) (лабораторії):

Керівництво Лабораторії:

завідувач,

заступник завідувача з завданнями та функціями координації міжвідділових кейсів, контроль строків/якості, розвиток методик.

Відділ (–ли):

завідувач відділу,

4 судових експерта та 1 провідний науковий (науковий) співробітник (методолог/галузевий куратор).

Резерв/сумісна команда швидкого реагування:

формується з числа експертів трьох відділів для комісійних, складних, об’ємних/термінових досліджень.

Секретаріат/діловодство:

за рахунок окремої штатної одиниці – інженера (відповідної категорії) підрозділу (лабораторії), для уніфікації обігу матеріалів, діловодства, опрацювання протоколів, проектів рішень, інше.

Функціональні нововведення:

Міждисциплінарні експертні групи під кожне провадження – головуючий експерт, який відповідає за координацію всієї експертизи у конкретному провадженні.

Єдиний методичний контур: план створення та оновлення методик, чек–листи для прийняття матеріалів і шаблони завдань експертам – чіткі інструкції для усвідомлення завдання при виконанні процесів і етапів дослідження.

Система забезпечення якості: система контролю якості: внутрішні перевірки компетенції експерта.

Навчання й підготовка кадрів: програма підвищення кваліфікації: оборонні закупівлі, фінанси, міжнародне гуманітарне право, аналіз відкритих даних та моделювання бойових дій (співпраця з провідним навчальним закладом – Національним університетом оборони України, департаментами МОУ та головними управліннями ГШ ЗСУ).

Партнерство з правоохоронними органами і академічними закладами: науково–практичні конференції, спільні семінари, забезпечення актуальними чинними керівними документами, обмін даними щодо типових помилок і потреб слідства.

Очікувані результати:

Скорочення середніх строків виконання експертиз, комісійних і комплексних експертиз на 20–30% завдяки паралельному опрацюванню та кращій логістиці матеріалів.

Збільшення пропускної спроможності підрозділу (лабораторії) щонайменше на 30–40% без втрати якості за рахунок спеціалізації відділів і стандартизації процесів.

Підвищення якості висновків: зменшення кількості повернень/відмов у прийнятті матеріалів, мінімізація процесуальних ризиків щодо допустимості доказів.

Завершення розроблення/оновлення методик.

Кадровий резерв: постійна активна підготовка нових судових експертів.

Ресурсні наслідки:

Кадрові: введення посад – 3 відділа × (4/5 експертів + 1 ПНС/НС.) = 15/18 фахівців + 1 заступник завідувача Лабораторії (за наявності частина посад – через переведення/оптимізацію) та інженера Лабораторії + завідувач Лабораторії. ∑ = 19/21 особа.

Матеріально–технічні: робочі місця, ПЗ для доступу до баз відкритих даних інформації, засоби моделювання та візуалізації.

Фінансові: введення посад в найкоротший час; пріоритет – укомплектування ВДДСВГД, заступника завідувача та інженера лабораторії.

Управління ризиками:

Нестача кандидатів: зміни до програми навчання, стажування та порядку атестування, залучення експертів з інших НДУСЕ за сумісництвом, звільнившихся судових експертів.

Методичні прогалини: подолання методичних прогалин: залучення провідних науковців, спільна командна робота експертів над методиками, швидке випробування нових підходів на навчальних прикладах.

Процесуальні ризики: дотримання вимог КПК і наказів, залучення юристів під час формулювання питань експерту.

Етапи впровадження:

Місяць 1–2: Затвердження структури та переліку справ, розробка положень підрозділу (лабораторії, відділів) та посадових інструкцій, призначення на посади (виконуючих обов'язки) завідувачів відділів і заступника завідувача лабораторії

Місяць 2–3: Укомплектування відділів, початок навчання, стажування та атестування судових експертів.

Місяць 7–12: повноцінна робота всіх трьох відділів; зовнішній аудит якості; перегляд і актуалізація методик; звіт за коефіцієнтом корисної дії та пропозиції на наступний рік.

Перелік використаних джерел:

1. Актуальні проблеми реалізації політики національної безпеки України в оборонній сфері. Вип. 27 / За заг. ред. В. П. Горбуліна. Київ ДП НВЦ «Євроатлантикінформ», 2006. 192 с.

2. Бандурка О. М. Становлення і напрями розвитку судової експертної служби в Україні. Тези доповідей науково–практичної конференції, присвяченої пам'яті Заслуженого професора М. С. Бокаріуса (м. Харків, 20 грудня 2016 року).

3. Методика проведення судових військових експертиз щодо оцінки дій посадових осіб (керівників, командирів, начальників)–суб'єктів боротьби з тероризмом, в ході антитерористичної операції: Методика. Київ: КНДІСЕ, 2018 (реєстраційний код 16.1.02).

4. Методика проведення судових військових експертиз, пов'язаних з рівнем обороноздатності держави: Методика. Київ: КНДІСЕ, 2018 (реєстраційний код 16.1.03).

5. Великий тлумачний словник сучасної української мови: уклад. та голов. ред. В. Т. Бусел. Київ; Ірпінь: Перун, 2005. VIII, 1728 с.

6. Конституція України.

7. Наказ Міністерства юстиції України від 08.10.1998 № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково–методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» (із змінами).

8. Наказ Міністерства юстиції України від 19.04.2012 №611/5 «Про затвердження Довідника кваліфікаційних характеристик посад працівників науково–дослідних установ судових експертиз Міністерства юстиції України» (із змінами).

9. Баличева А.С., Антонюк П.Є. Проблемні аспекти проведення судової експертизи в Україні в умовах воєнного стану. Матеріали І Всеукраїнської науково–практичної конференції 29 лютого 2024 року URL: https://jurist.net.ua/wpcontent/uploads/2024/02/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA2024–2.pdf. (дата звернення: 15.05.2026).

10. Військова експертиза. URL: https://kndise.gov.ua/expertise/military–examinations (дата звернення: 15.05.2026).

11. Григоренко Ю. Проблеми правової невизначеності статусу фахівців, залучених до проведення експертиз. URL: https://unba.org.ua/publications/10801–problemi–pravovoi–neviznachenosti–statusu–fahivciv–zaluchenih–do–provedennya–ekspertiz.html.

12. Бершов Г.Є. Військова експертиза у кримінальному провадженні. URL: https://doi.org/10.32631/vca.2024.1.18. (дата звернення: 15.05.2026).

13. Кримінальний кодекс України : Кодекс України; Кодекс, Закон від 05.04.2001 № 2341–III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341–14

14. Кримінальний процесуальний кодекс України : Кодекс України; Закон, Кодекс від 13.04.2012 № 4651–VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651–17

15. Про судову експертизу : Закон України від 25.02.1994 № 4038–XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4038–12

16. Про оборону України : Закон України від 06.12.1991 № 1932–XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1932–12

17. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року : Протокол; ООН від 08.06.1977 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/995_199

DOI https://doi.org/10.32837/11300.33592

Шершенькова Вікторія
кандидат юридичних наук, доцент,
доцент кафедри оперативно–розшукової та поліцейської діяльності
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0002–3123–8578
e–mail:shershenkova2017@ukr.net

ЗБІР ДОКАЗІВ СТОСОВНО ВІЙСЬКОВИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

У тезах розглянуто засади збору доказів щодо військових кримінальних правопорушень в умовах воєнного стану в Україні. Проаналізовано, які слідчі (розшукові) дії проводяться для розслідування військових кримінальних правопорушень. Визначено обставини через які під час розслідування військових кримінальних правопорушень виникають труднощі у збиранні доказів і через це деякі особи не будуть притягнуті до кримінальної відповідальності.

Ключові слова: злочинність, докази, слідчі дії, військові кримінальні правопорушення, запобігання.

Shershenkova Viktoriia
Candidate of Law Sciences, Associate Professor,
Associate Professor of the Department of Operational
Investigation and Police Activities, National University «Odesa Law Academy»,
Odesa, Ukraine

COLLECTION OF EVIDENCE REGARDING MILITARY CRIMINAL OFFENSES UNDER MARTIAL STATE IN UKRAINE

The theses consider the principles of collecting evidence regarding military criminal offenses under martial law in Ukraine. It analyzes what investigative (search) actions are carried out to investigate military criminal offenses. It identifies the circumstances that cause difficulties in collecting evidence during the investigation of military criminal offenses and because of this, some individuals will not be held criminally liable.

Key words: crime, evidence, investigative actions, military criminal offenses, prevention.

З початком повномасштабного вторгнення Росії на територію України в нашій країні зменшився загальний рівень злочинності, але це посприяло збільшенню кількості військових кримінальних правопорушень, у зв’язку з складними умовами служби в армії, під впливом багатьох факторів та обставин,

що мають вплив на стан військовослужбовців. Питання військової злочинності набуває особливої актуальності та становить ризик для суспільства, військової безпеки та національної безпеки України.

При розгляді військових кримінальних правопорушень необхідно приділяти всебічному аналізу обставин їх вчинення, збору доказів, які мають відповідати критеріям належності, допустимості, достовірності, достатності, адже вони мають вагоме значення при розслідуванні.

Так, доказування – це відтворення події кримінального процесу, з'ясування її сутності і підготовка на підставі цього відповідних процесуальних дій. Він включає в себе збирання, перевірку, оцінку доказів у справах щодо військових кримінальних правопорушень [2].

Під час проведення досудового розслідування військових кримінальних правопорушень, збір доказів є складним та довготривалим процесом, а також має проводитися відповідно до чинних норм Кримінального процесуального кодексу України (КПК України), тобто має відбуватися проведення необхідних слідчих розшукових дій та негласних слідчих розшукових дій, витребування відомостей, документів, висновків та вчинення інших дій не заборонених законом.

В залежності від класифікації військових кримінальних правопорушень, задля збирання доказів проводяться наступні слідчі (розшукові) дії передбачені КПК України:

– огляди місця подій та документів, що мають необхідні відомості (ст. 237 КПК України);

– проведення обшуку (ст. 234 КПК України);

– допит (ст. 224 КПК України);

– пред'явлення особи для впізнання (ст. 228 КПК України);

– пред'явлення речей для впізнання (ст. 229 КПК України);

– експертизи (ст. 242 КПК України);

– слідчий експеримент (ст. 240 КПК України);

– зняття інформації з електронних комунікаційних мереж (ст. 236 КПК України);

– розшук підозрюваного (ст. 281 КПК України) [1].

Дані дії необхідно проводити відповідно до вимог законодавства, з дотриманням встановленого порядку та за наявності передбачених дозволів уповноважених суб'єктів [3].

Разом з тим, навіть дотримуючись всіх процедур передбачених законодавством, виникають труднощі у збиранні доказів. Оскільки величезна кількість військових кримінальних правопорушень вчиняється у зоні бойових дій, на лінії фронту, непідконтрольних територіях, у місцях де руйнуються матеріальні об'єкти, знищуються сліди скоєння військових кримінальних правопорушень, а також природні явища можуть перешкоджати при розслідуванні.

Кримінальні правопорушення такого характеру найчастіше за все розслідуються вже коли Україна відновлює контроль над своїми тимчасово окупованими територіями. Розслідування можуть розпочати відразу ж або через об'єктивні обставини дещо пізніше. Як результат, через втрачений час докази, матеріали, сліди вчинення військові кримінальні правопорушення тощо можуть зникнути або бути знищеними, все це ускладнює розслідування військових кримінальних правопорушень.

Також слід зазначити, що Україна стикається з безпрецедентними викликами, які необхідно швидко вирішувати. Серед яких критичними є забезпечення національної безпеки та запобігання злочинності.

До прикладу, сьогодні безпілотні літальні апарати використовуються не лише для оборони України, а вже були зафіксовані випадки вчинення кримінальних правопорушень (замахів на вбивство та підготовки терактів), на територіях де не ведуться бойові дії.

У зв'язку з цим необхідно на законодавчому рівні урегулювати використання безпілотних літальних апаратів, це має бути така контрольована система обігу, щоб мінімізувати ризики їх застосування у злочинних цілях. Таку небезпеку для суспільства не можна виключати і у післявоєнний період.

Окрім цього, слід враховувати й ту обставину, що військовослужбовцям з бойовим досвідом необхідна буде підтримка з боку держави щодо повернення до мирного життя, щоб вони не були втягнуті до кримінального середовища.

З огляду на це, було підготовлено законодавчий проєкт, який передбачав порядок використання безпілотних літальних апаратів у післявоєнний період, але його було відхилено через певні не доопрацювання щодо класифікації безпілотних літальних апаратів.

Таким чином, у ході розслідування військових кримінальних правопорушень виникають різні труднощі у збиранні доказів, фіксуванні факту вчинення правопорушення, що може затягуватися на невизначений строк, і як наслідок цього, деякі особи не будуть притягнуті до кримінальної відповідальності.

Збір доказів – це доволі складний і важливий процес, а його ефективність визначає не лише результат конкретного кримінального провадження, а й рівень довіри суспільства до розслідування військових кримінальних правопорушень та вчинення справедливого правосуддя в умовах воєнного часу.

Перелік використаних джерел:

1.Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року. № 4651–VI. URL: https://surl.lt/iilfin

2.Кримінальний процес: підруч. / кол. авт. ; кер. авт. кол. канд. юрид. наук, доц. В. М. Федченко. 3–є вид., доп. і перероб. У 2–х ч. Ч. 1 «Досудове провадження». Дніпро : Дніпроп. держ. ун–т внутр. справ, 2022. 544 с. URL: https://surl.li/dcqraj

3.Лупій С., Крижановський А. Слідчі (розшукові) дії: поняття, значення та види. Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки» № 4 (36), 2022. С. 210–215. URL: https://lnk.ua/VHlzaX7vc

DOI https://doi.org/10.32837/11300.33593

Яцкевич Руслан
доктор філософії за спеціальністю 081 – Право,
перший заступник начальника Департаменту внутрішньої безпеки
Національної поліції України, полковник поліції,
м. Київ, Україна
ORCID: https://orcid.org/0009–0008–9352–7077
e–mail:nuoua2025ord@onua.edu.ua

СКЛАДОВІ ПРОФЕСІЙНОЇ КОМПЕТЕНЦІЇ ПРАЦІВНИКІВ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ, ЯКІ ЗАБЕЗПЕЧУЮТЬ ПРОТИДІЮ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Акцентована увага на питаннях необхідності наукового аналізу та дослідження окремих питань кадрового забезпечення оперативних підрозділів, які здійснюють протидію організованим формам злочинної діяльності. Виокремлена та охарактеризована система компетенцій, якими має володіти працівник оперативного підрозділу для ефективної організації роботи щодо протидії діяльності організованих злочинних угруповань.

Ключові слова: організована злочинність, організовані злочинні угруповання, оперативні підрозділи, оперативний працівник, компетенції.

Yatskevich Ruslan
Doctor of Philosophy in specialty 081 – Law,
First Deputy Head of the Department of Internal Security of the National Police of Ukraine, Police Colonel,
Kyiv, Ukraine

COMPONENTS OF PROFESSIONAL COMPETENCE OF EMPLOYEES OF OPERATIONAL UNITS THAT PROVIDE COMBAT TO ORGANIZED CRIME

The emphasis is on the need for scientific analysis and research of individual issues of staffing operational units that counter organized forms of criminal activity. The system of competencies that an employee of an operational unit must possess for the effective organization of work on countering the activities of organized criminal groups is identified and characterized.

Keywords: organized crime, organized criminal groups, operational units, operational employee, competencies.

Аналіз останніх наукових досліджень свідчить про пожвавлення інтересу вчених до формування комплексної стратегії протидії організованій злочинності в Україні[1; 2; 3; 4]. У той же час, аналітичне опрацювання наукових джерел

свідчить про відсутність системного вивчення кадрового забезпечення реалізації вказаного напряму наукової діяльності, зокрема комплексного дослідження відповідної системи компетенцій, якими має володіти працівник оперативного підрозділу, який за своєю основною функціональною спрямованістю забезпечує протидію організованим формам злочинної діяльності.

Водночас, у сучасних умовах трансформації організованої злочинності, її інтеграції у фінансово–економічні, політичні, інформаційні та транснаціональні процеси особливого значення набуває питання формування професійної компетенції працівників оперативних підрозділів, діяльність яких спрямована на виявлення, документування, локалізацію та нейтралізацію організованих злочинних угруповань. Організована злочинність у XXI столітті характеризується високим рівнем адаптивності, конспіративності, ресурсної забезпеченості, використанням сучасних технологій, корупційних механізмів та елементів гібридного впливу, що обумовлює необхідність якісного переосмислення професійних вимог до суб'єктів оперативно–розшукової діяльності.

Перш за все, необхідно відзначити, що професійна компетенція працівника оперативного підрозділу у сфері протидії організованій злочинності є багаторівневою інтегративною системою знань, навичок, аналітичних здібностей, морально–психологічних якостей та практичних алгоритмів поведінки, що забезпечують здатність ефективно реалізовувати оперативно–розшукову функцію в умовах підвищеного ризику, інформаційної невизначеності та активної протидії з боку кримінального середовища.

Однією з ключових складових професійної компетенції виступає нормативно–правова компетентність, яка передбачає глибоке знання кримінального, кримінального процесуального, оперативно–розшукового, антикорупційного та міжнародного законодавства. Працівник оперативного підрозділу повинен не лише орієнтуватися у нормативній базі, але й володіти навичками її практичного застосування в умовах швидкої зміни криміногенних процесів. Особливого значення набуває здатність правильно інтерпретувати правові межі оперативного втручання, забезпечувати допустимість отриманої інформації та дотримання балансу між інтересами безпеки держави і правами людини. У протидії організованій злочинності правова помилка оперативного працівника може призвести не лише до втрати доказової перспективи, але й до руйнування складної багаторівневої оперативної комбінації.

Важливе місце у структурі професійної компетенції займає оперативно–тактична компетентність, яка охоплює систему спеціальних знань і практичних навичок щодо організації негласної діяльності, формування агентурного апарату, проведення оперативних комбінацій, оперативного проникнення, документування злочинної діяльності та забезпечення конспірації. У сфері протидії організованій злочинності оперативно–тактична компетентність набуває особливого значення через необхідність функціонування в умовах високої латентності злочинів та

багаторівневого захисту організованих злочинних угруповань. Працівник повинен вміти прогнозувати поведінку членів злочинного угруповання, моделювати їхні реакції, формувати сценарії розвитку оперативної ситуації та адаптувати тактичні рішення до динаміки кримінального середовища.

Не менш важливою є інформаційно–аналітична компетентність, яка у сучасних умовах фактично перетворюється на фундамент оперативної діяльності. Організовані злочинні угруповання активно використовують цифрові технології, криптографічні засоби зв'язку, фінансові схеми легалізації активів, міжнародні логістичні маршрути та складні механізми приховування інформації. У зв'язку з цим працівник оперативного підрозділу повинен володіти навичками кримінального аналізу, аналізу великих масивів даних, побудови аналітичних моделей, встановлення прихованих зв'язків між суб'єктами та подіями, а також використання сучасних інформаційно–пошукових систем. Інформаційно–аналітична компетентність забезпечує можливість переходу від реактивної моделі протидії злочинності до проактивного виявлення загроз.

Самостійною складовою професійної компетенції є психологічна компетентність, що включає здатність до психологічного впливу, комунікативної адаптації, профайлінгу, розпізнавання маніпулятивних моделей поведінки та управління конфліктними ситуаціями. Працівник оперативного підрозділу функціонує у середовищі постійного психологічного напруження, ризику та інформаційного тиску. Водночас ефективність негласної роботи, зокрема з громадянами значною мірою залежить від рівня психологічної підготовки працівника. У протидії організованій злочинності психологічна компетентність також включає здатність виявляти ознаки внутрішньої деструкції злочинної групи, конфліктів між її учасниками та потенційних точок оперативного впливу.

Особливого значення набуває стратегічно–прогностична компетентність, яка передбачає здатність оцінювати тенденції розвитку організованої злочинності, прогнозувати трансформацію кримінальних ринків, аналізувати ризики кримінального впливу на державні інститути та формувати довгострокові моделі оперативного реагування. Сучасна організована злочинність дедалі частіше функціонує за принципами мережевої децентралізації, що ускладнює використання традиційних методів протидії. Саме тому оперативний працівник повинен мислити не лише категоріями окремого злочину, а й категоріями кримінальної системності, кримінальної інфраструктури та кримінального впливу на суспільні процеси.

У структурі професійної компетенції також необхідно виділити міжвідомчу та комунікаційну компетентність, оскільки сучасна протидія організованій злочинності неможлива без інтеграції зусиль різних правоохоронних, фінансових, прикордонних, антикорупційних та міжнародних інституцій. Працівник оперативного підрозділу повинен володіти навичками міжвідомчої координації, обміну інформацією, побудови спільних алгоритмів реагування та функціонування у складі оперативних груп. Особливу актуальність це має у сфері

транснаціональної злочинності, де ефективність діяльності залежить від швидкості міжнародної комунікації та взаємодії.

Суттєвого значення набуває і технологічна компетентність, що передбачає здатність використовувати сучасні технічні засоби негласного отримання інформації, цифрові інструменти аналізу, системи геоаналітики, OSINT–технології, засоби кіберрозвідки та програмні комплекси кримінального аналізу. Цифровізація організованої злочинності призводить до того, що недостатній рівень технологічної підготовки оперативного працівника фактично формує професійну неспроможність у протидії сучасним кримінальним загрозам.

Водночас професійна компетенція працівника оперативного підрозділу не є статичною категорією. Її зміст постійно змінюється під впливом трансформації злочинності, розвитку технологій, міжнародних безпекових процесів та еволюції кримінальних практик. Саме тому професійна компетентність повинна розглядатися як динамічна система безперервного професійного розвитку, що включає постійне оновлення знань, удосконалення практичних навичок, адаптацію до нових оперативних викликів та формування інноваційного типу професійного мислення.

Таким чином, можна підсумувати, що професійна компетенція працівників оперативних підрозділів, які забезпечують протидію організованій злочинності, є комплексною багатокомпонентною системою, що поєднує правові, тактичні, аналітичні, психологічні, технологічні та етичні елементи. Її ефективність визначається не лише рівнем професійної підготовки окремого працівника, але й здатністю оперативних підрозділів функціонувати як інтелектуально–аналітична система державної безпеки, орієнтована на випереджальне виявлення та нейтралізацію кримінальних загроз.

Перелік використаних джерел:

1. Бахуринська О.О. Перспективні напрями протидії організованій злочинності в Україні. Право і суспільство. №6. 2018. С. 182–188.

2. Басиста І.В. Організована злочинність: сучасні українські реалії та кроки до протидії. Науково–інформаційний вісник Івано–Франківського університету права імені Короля Данила Галицького. Серія: Право. Вип. 15. Т.2. 2023. С. 202–207

3. Доценко О.С. Стратегічна мета та тактичні завдання протидії організованій злочинності в Україні. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2019. №41. Том 1. С. 69–73

4. Литвиненко В.І., Пригунов П.Я. Протидія організованій злочинній діяльності в Україні крізь призму останніх правових новел (міжнародний та вітчизняний досвід). Право.ua. №2. 2020. С.54–63

Наукове видання

КРИМІНАЛІСТИКА МАЙБУТНЬОГО: ЦИФРОВІ ІННОВАЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, ГЛОБАЛЬНІ ВИКЛИКИ ТА ЗАГРОЗИ

Матеріали Міжнародної науково-практичної конференції

(Одеса, 5 червня 2026 р.)

Електронне видання

Відповідальні за випуск/укладачі:

Лариса Аркуша

Антоніна Черемнова

Пьотр Пєтькович

Укладачі:

Юлія Гресь

Анна Колодіна

Олександра Стаурська

Олександр Чернов

Підписано до друку 24.11.2025.

Формат А4 (210×297 мм). Ум-друк. арк. 27,4.

Scientific publication

CRIMINALISTICS OF THE FUTURE: DIGITAL INNOVATIONS, ARTIFICIAL INTELLIGENCE, GLOBAL CHALLENGES AND THREATS

Proceedings of the International Scientific and Practical Conference

(Odesa, *5 June 2026*)

Electronic edition

Responsible for the release/compilers:

Larysa Arkusha

Antonina Cheremnova

Piotr Pietkovich

Compilers:

Yulia Hres

Anna Kolodina

Oleksandra Staurska

Oleksandr Chernov

Signed for printing 11/24/2025.

Format A4 (210×297 мм). Printed. sheets 27,4.

564