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».

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.