ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції

1

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 1

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 1

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 1. – 772 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 11. КРИМІНАЛІСТИКА, СУДОВА ЕКСПЕРТИЗА, ПСИХОЛОГІЯ ТА МЕДИЦИНА У ЗАБЕЗПЕЧЕННІ СУДОЧИНСТВА

4. Пожар В. Г. Деякі проблемні аспекти представництва потерпілого в кримінальному судочинстві. *Актуальні проблеми правознавства. Науковий збірник юридичного факультету ТНЕУ* / редкол.: М. О. Баймуратов та ін. Тернопіль : Астон, 2012. Вип. 2. С. 272-277.

Ключові слова: інститут представництва, учасники кримінального провадження, потерпілий, представник, види представництва, законне представництво, договірне представництво.

Keywords: institution of representation, participants in criminal proceedings, victim, representative, types of representation, legal representation, contractual representation.

Лукащук Каріна Русланівна
Національний університет «Одеська юридична академія»,
аспірантка кафедри кримінального процесу

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ У ВОЄННИЙ ПЕРІОД

У сучасному світі, де технології стрімко розвиваються, зростає й роль цифрових інструментів у забезпеченні національної безпеки, зокрема у боротьбі зі злочинністю в умовах воєнного періоду. Кіберзлочинність стає все більш актуальною проблемою для країн, які перебувають у стані військового конфлікту. Використання штучного інтелекту (далі – ШІ) та інших цифрових технологій стає важливим елементом у боротьбі зі злочинними групами, що ведуть свою діяльність у кіберпросторі, здійснюючи атаки на критичну інфраструктуру, поширюючи дезінформацію та здійснюючи фінансові злочини, зокрема через криптовалюти.

В умовах війни кіберзлочинність набуває нових форм і проявів, ставши одним із ключових елементів гібридної війни. Сучасні операції в кіберпросторі надають зловмисникам унікальну можливість для анонімності, мінімізації витрат та значного прискорення процесів атак. Ці фактори роблять кіберзлочини ефективними інструментами для порушення економічної, соціальної та політичної стабільності країни.

Один із найбільш поширених інструментів кіберзлочинців під час воєнних дій – атаки на критичну інфраструктуру. Це може бути інфраструктура енергетична, транспортна, фінансова та телекомунікаційна. Такі атаки здатні спричинити серйозні наслідки для стабільного функціонування держави, що в умовах війни може мати катастрофічні наслідки для обороноздатності та морального духу суспільства [1].

За даними Державної служби спеціального зв'язку та захисту інформації України, з початку російського вторгнення в Україну кількість кібератак на критичну інфраструктуру зросла на 400% порівняно з довоєнними роками. Зокрема,

в 2022 році відбулося кілька значних атак на енергетичні системи України, що ставили під загрозу енергетичну безпеку та стабільність життєдіяльності держави.

Іншою важливою складовою кіберзлочинної діяльності є інформаційні кампанії, які спрямовані на поширення неправдивої інформації, маніпуляції в соціальних мережах та створення фейкових новин. Такі кампанії можуть мати серйозний вплив на громадську думку, підривати довіру до офіційних джерел інформації та дестабілізувати суспільство. В умовах війни психологічні операції, спрямовані на деморалізацію населення та армії, мають значну роль.

За даними того ж Держспецзв'язку, кількість кіберінцидентів в Україні у 2022 році зросла в 2,8 рази, а кількість кампаній із дезінформації перевищила 200 [2]. Поширення фейкових новин та маніпуляцій в соціальних мережах створює хаос, який складно контролювати та який ускладнює не лише внутрішню політику, а й міжнародну стабільність.

Суттєву роль у фінансуванні кіберзлочинної діяльності відіграють криптовалюти. Завдяки своїй анонімності та децентралізованій природі криптовалюти дають можливість зловмисникам здійснювати нелегальні фінансові операції, обходячи традиційні фінансові механізми та правоохоронні органи. Це стало серйозною проблемою в боротьбі з фінансовими злочинами, оскільки звичайні методи моніторингу та регулювання фінансових потоків стають малоефективними для криптовалютних транзакцій [3].

Згідно з дослідженням FATF, у 2022 році частка криптовалютних транзакцій, що пов'язані з незаконною діяльністю, зросла до 2,1% [4]. Технологія блокчейн, яка є основою криптовалют, забезпечує високу рівень анонімності та складність виявлення злочинних операцій, що ще більше ускладнює боротьбу з фінансовими злочинами.

Штучний інтелект (ШІ) і технології машинного навчання можуть стати ефективними інструментами для виявлення та протидії кіберзлочинності. За допомогою алгоритмів машинного навчання можна аналізувати великі масиви даних, що дозволяє швидко виявляти підозрілі транзакції, а також несанкціонований доступ до інформаційних систем.

Дослідження показують, що використання штучного інтелекту для аналізу фінансових операцій у криптовалютних мережах дозволяє виявляти схеми відмивання грошей та інші нелегальні операції, а також покращити швидкість та точність виявлення таких операцій. Це дозволяє ефективно реагувати на зростаючу кіберзлочинність і забезпечити більш високий рівень безпеки.

Іншим важливим напрямом у боротьбі з кіберзлочинністю є використання великих даних для аналізу та виявлення аномальних дій у кіберпросторі. Цей підхід дозволяє відслідковувати великі обсяги інформації, що надходять з різних джерел, та виявляти потенційні загрози ще на етапі їх формування.

Однак важливим аспектом у боротьбі з кіберзлочинністю є міжнародна співпраця між державами та правоохоронними органами. Технології, які використовуються зловмисниками, постійно розвиваються, і це створює потребу в

адаптації законодавства до нових реалій. Міжнародна співпраця у галузі кібербезпеки, обмін досвідом та спільне використання новітніх технологій можуть значно підвищити ефективність боротьби зі злочинністю в кіберпросторі.

У періоди війни кіберзлочинність стає важливою складовою ведення війни, що має стратегічне значення для дестабілізації суспільства, порушення критичної інфраструктури та фінансування незаконних операцій через криптовалюти. Використання штучного інтелекту, машинного навчання та великих даних дозволяє значно підвищити ефективність виявлення та реагування на кіберзлочини. Однак для того, щоб протистояти цьому виклику, необхідно постійно вдосконалювати законодавство, адаптувати регуляторні механізми та посилювати міжнародну співпрацю у боротьбі з кіберзлочинністю [5].

Уже сьогодні очевидно, що цифрові технології, зокрема штучний інтелект і машинне навчання, мають значний потенціал у боротьбі з кіберзлочинністю, і їхнє використання буде тільки зростати. Технології обробки великих даних і блокчейн можуть значно змінити спосіб, у який ми здійснюємо моніторинг кіберпростору та реагуємо на загрози. Проте попри численні досягнення, важливо врахувати й виклики, що виникають у цьому напрямку.

Одним із найбільш перспективних напрямів є подальший розвиток штучного інтелекту, який стане ще більш потужним інструментом для боротьби з кіберзлочинністю. Із розвитком алгоритмів машинного навчання з'являються нові можливості для передбачення та виявлення кіберзлочинних атак на ранніх етапах їх здійснення. Штучний інтелект може стати незамінним інструментом у розпізнаванні аномалій у мережевому трафіку та фінансових транзакціях, що дозволить своєчасно запобігати атакам і незаконним операціям.

Зокрема, новітні системи ШІ здатні виявляти приховані патерни в великих обсягах даних, що важко помітити людині або традиційним програмним забезпеченням. Це дає змогу своєчасно виявляти шкідливі коди, підозрілі транзакції чи спроби викрадення даних, знижуючи таким чином ризики для національної безпеки. Використання систем ШІ для прогнозування потенційних атак на основі історичних даних і поведінки кіберзлочинців може в значній мірі змінити підхід до забезпечення безпеки.

Список використаних джерел:

1. Ambassadors S. Blockchain Transaction Detection with AI. *Medium*. 2024. URL: https://medium.com/@singularitynetambassadors/blockchain-transaction-detection-with-ai-32508414492f.

2. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit.

3. Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html.

4. Chainalysis Crypto Crime Report 2023. URL: https://hkibfa.io/wp-content/uploads/2023/02/Crypto_Crime_Report_2023.pdf

5. Foley S., Karlsen J. R., Putnins T. J. Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? *Review of Financial Studies.* 2018. vol. 32(5). 63 p.

Ключові слова: штучний інтелект, кіберзлочинність, боротьба зі злочинами, національна безпека, війна.

Keywords: artificial intelligence, cybercrime, crime fighting, national security, war.

Ляховченко Іван Анатолійович
Національний університет «Одеська юридична академія»,
аспірант кафедри кримінального процесу

СУД ПРИСЯЖНИХ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ

Здійснюючи кримінальне провадження, держава повинна забезпечувати баланс між приватними та публічними інтересами. Лише в такий спосіб можна гарантувати досягнення завдань кримінального провадження без ризику необґрунтованого обмеження прав учасників кримінального процесу. Відповідно, задля гарантування цих прав держава намагається імплементувати якомога більше правових інститутів, метою яких є забезпечення гуманізації кримінальної процесуальної діяльності. Одним з таких інститутів і є суд присяжних.

Вчені зазначають, що суд присяжних є колегією громадян, незалежною від професійних суддів, яка формується з осіб, що добре обізнані з умовами життя у своєму регіоні та особливостями соціального середовища, яке вони представляють. Завдяки цьому присяжні мають змогу об'єктивно оцінити наявність або відсутність вини особи у вчиненні кримінального правопорушення та винести справедливе рішення. В Україні суд присяжних функціонує як колегіальний орган, що складається з двох професійних суддів і трьох присяжних, і діє при місцевому (окружному) загальному суді першої інстанції. За клопотанням обвинуваченого він розглядає кримінальні провадження щодо злочинів, за які передбачене покарання у вигляді довічного позбавлення волі. Усі учасники такого суду спільно ухвалюють рішення з усіх питань, що виникають під час судового розгляду, за винятком питань, передбачених частиною третьою статті 331 КПК України [1, с. 17].

На думку В. Г. Шишленка, оскільки саме присяжним належить повноваження встановлювати факт вчинення діяння та винуватість підсудного, інституція суду присяжних повинна відповідати низці принципових ознак. Зокрема, йдеться про чітке розмежування повноважень між професійними суддями та присяжними; організаційну автономію колегії присяжних щодо суддівського складу; відсутність юридичної відповідальності присяжних за прийняте рішення; не-