

ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»
ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»

МИКОЛА КАРЧЕВСЬКИЙ

КРИМІНАЛЬНЕ ПРАВО В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.

**Від несанкціонованого доступу
до «jailbreak» штучного інтелекту**

Монографія

Харків
«Право»
2025

Рецензенти:

Є. О. Письменський, доктор юридичних наук, професор, проректор з наукової роботи Закладу вищої освіти «Університет Короля Данила»;

Р. О. Мовчан, доктор юридичних наук, професор, професор кафедри конституційного, міжнародного і кримінального права Донецького національного університету імені Василя Стуса;

О. В. Копан, доктор юридичних наук, професор, головний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

*Рекомендовано до друку
вченою радою Закладу вищої освіти «Університет Короля Данила»
(протокол № 2 від 25 вересня 2025 року),
вченою радою Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук України»
(протокол № 8 від 29 вересня 2025 року)*

Карчевський М.

К27 Кримінальне право в умовах цифрової трансформації. Від не-санкціонованого доступу до «jailbreak» штучного інтелекту : монографія / Микола Карчевський ; Ун-т Короля Данила ; Ін-т інформації, безпеки і права Нац. акад. прав. наук України. – Харків : Право, 2025. – 176 с.

ISBN 978-617-8617-41-7

Розглядається феномен «синхронізації» між інформатизацією та кримінально-правовим регулюванням, коли нові технології одночасно створюють загрози й відкривають можливості для юстиції. Досліджуються такі напрями: інформаційна безпека як об'єкт кримінально-правової охорони; трансформація традиційних злочинів і формування категорії «комп'ютерних»; використання ІТ та штучного інтелекту в кримінальній юстиції, включно з можливостями кримінологічного аналізу й ризиками зловживань.

Монографія поєднує теоретичний і практичний аналіз: від критики чинної судової практики до прикладів застосування інноваційних платформ на кшталт «CrimeDataLab». Особливу увагу приділено викликам для України в умовах війни, де інформаційна сфера стала одним із ключових полів протистояння.

Робота адресована науковцям, правникам, студентам юридичних факультетів, а також усім, хто цікавиться проблемами інформаційної безпеки й майбутнім кримінального права в епоху цифрових технологій.

УДК43.3/.7:343.9:004.9:004.8

*Олені
Тайсії
Тимофію*

Передмова

Ця монографія народжувалася в поєднанні особистого досвіду, наукових пошуків і дискусій з колегами та студентами. Вона є спробою осмислити кримінальне право крізь призму цифрової трансформації – процесу, який змінює не лише технічні засоби, а й сам спосіб мислення.

Сподіваюся, що книга стане не лише науковим текстом, а й запрошенням до діалогу. Бо право – це завжди розмова про людину, її свободу й гідність навіть тоді, коли воно стосується алгоритмів і кодів.

Під час підготовки цієї монографії як допоміжний засіб пошуку наукових джерел, їх узагальнення та аналізу судової практики було застосовано інструменти штучного інтелекту – ChatGPT, Gemini та Claude. Водночас усі наукові ідеї, висновки й інтерпретації належать авторові, який несе повну відповідальність за зміст цієї праці.

Також ця книга має віртуальну складову, створено спеціалізованих ШІ-помічників¹. Тепер можна не лише гортати сторінки, а й вести розмову з віртуальним співрозмовником, який допоможе зорієнтуватися в розділах монографії, пояснити складні поняття чи підказати, де шукати відповіді. Це своєрідне продовження діалогу між автором і читачем, який виходить за межі друкованого тексту.

І якщо читач, гортаючи сторінки або спілкуючись із ботом, знайде тут не лише відповіді, а й запитання для власних роздумів, це буде найкращим підтвердженням сенсу роботи автора.

¹ QR-код на обкладинці веде до чат-ботів, які пояснюють зміст монографії.

Вступ

15 лютого 1946 року в підвалі Школи електротехніки імені Альфреда Фітлера Мура Пенсільванського університету Джон Преспер Екерт і Джон Моклі подали енергію на блоки 27-тонного пристрою. Зажеврили приблизно 18 000 вакуумних ламп, запрацювали 1500 реле. Машина, яку назвали ЕНІАК (ENIAC – Electronic Numerical Integrator and Computer), почала оброблення перших команд. Інженери програмували цей комп'ютер, використовуючи десятки кабелів, вручну фізично з'єднуючи блоки. Процес зміни програми тривав іноді до двох днів. Тоді це був найпотужніший у світі комп'ютер¹. Більшість дослідників називають цю подію першим використанням електронно-обчислювальної машини.

ЕНІАК коштував уряду США 400 млн доларів. Він працював зі швидкістю кілька тисяч операцій на секунду. Використовувався для доволі вузьких задач: розрахунок балістичних таблиць для артилерії та обчислення в процесі розробки термоядерної бомби².

У 2025 році рейтинг найпотужніших комп'ютерів очолив El Capitan³, який проводить обчислення зі швидкістю в кілька квінтільйонів (одиниця з 18 нулями)⁴ операцій на секунду. Сучасні побутові комп'ютери опрацьовують команди у мільйон(!) разів швидше, ніж ЕНІАК⁵. Співвідношення вартості комп'ютерів до їхньої продук-

¹ ENIAC. *Engineering and Technology History Wiki*. URL: <https://ethw.org/ENIAC> (дата звернення: 21.09.2025) ; The ENIAC by J. Presper Eckert and John W. Mauchly / Computer History Museum. *YouTube*. 2022, June 10. URL: <https://www.youtube.com/watch?v=7GuXDCMfGfA> (дата звернення: 21.09.2025).

² Freiburger P. A., Swaine M. R. ENIAC. *Encyclopedia Britannica*. Last updated: 2025, August 24. URL: <https://www.britannica.com/technology/ENIAC> (дата звернення: 21.09.2025).

³ El Capitan retains top spot in 65th TOP500 list as Exascale Era expands. *TOP500*. URL: <https://top500.org/news/el-capitan-retains-top-spot-65th-top500-list-exascale-era-expands/> (дата звернення: 21.09.2025).

⁴ El Capitan: NSA's first exascale machine. *Advanced Simulation and Computing*. URL: <https://asc.llnl.gov/exascale/el-capitan> (дата звернення: 21.09.2025).

⁵ Для оцінки продуктивності комп'ютерів використовують такі показники: FLOPS (Floating Point Operations Per Second) і ГГц (gigahertz). FLOPS вимірює кількість математичних операцій із плаваючою комою, які можуть бути виконані за одну

тивності продовжує швидко знижуватися. Водночас сфера застосування і надалі розширюється. Так виглядає суспільний процес, який прийнято називати комп'ютеризацією.

Причина цього процесу полягає в постійному зростанні потреби в інформації. Щоб діяти ефективно, сучасній людині потрібно дедалі більше даних, необхідно їх зберігати й обробляти. Проблема обмеженості фізичних можливостей біологічних організмів людство вирішує завдяки комп'ютерам.

Інформатизацією називають «сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, технологічних і виробничих процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій»¹. Тобто інформатизація є сукупністю суспільних процесів, значущість яких визначається забезпеченням інформаційних потреб громадян і суспільства.

В умовах, коли значна частина людства зайнята в процесах інформатизації та комп'ютеризації², коли в цій сфері розміщуються фінансові інвестиції³ та отримуються істотні прибутки і значення інформаційних технологій для безпеки людей, суспільства й держав складно переоцінити, виникає потреба в їх правовому регулюванні. Право дає змогу забезпечити баланс соціальних переваг і ризиків використання інформаційних технологій. Важливою складовою правового регулювання інформатизації є кримінальне право. Воно стосується реакції

секунду. ГГц вимірює тактову частоту процесора, кількість циклів, які процесор може виконати за секунду. Один гігагерц дорівнює одному мільярду циклів на секунду.

¹ Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. *Відомості Верховної Ради України*. 2023. № 51. Ст. 127.

² Із 2014 по 2024 рік кількість фахівців з інформаційних комп'ютерних технологій в ЄС зросла на 62,2%, що майже в 6 разів перевищує зростання (10,6%) загальної зайнятості (ICT specialists in employment. *Eurostat*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment (дата звернення: 21.09.2025)).

³ Наприклад, із початком широкого використання штучного інтелекту інвестиції в цю сферу стали стратегічним пріоритетом для більшості компаній (Piscione D. P. It's Time for Your Company to Invest in AI. Here's How. *Harvard Business Review*. 2025, July 2. URL: <https://hbr.org/2025/07/its-time-for-your-company-to-invest-in-ai-heres-how> (дата звернення: 21.09.2025)).

держави на найбільш небезпечні посягання, є «ultima ratio», останнім засобом, який застосовується лише тоді, коли інші правові механізми є недостатніми.

Саме про кримінально-правове регулювання в контексті розвитку інформаційних технологій ітиметься в цій книзі.

Важливо те, що кримінальне право і впливає на інформатизацію, і перебуває під її впливом. Найбільш вдало цю ситуацію характеризує поняття «синхронізація». Тлумачний словник української мови визначає синхронізацію як приведення до синхронізму (точного збігу в часі. – *Авт.*) двох або кількох періодично змінних явищ чи процесів¹. Синхронізація процесів в інформатиці визначається як приведення двох або декількох процесів до такого їхнього перебігу, коли відсутня конкуренція або взаємне блокування. Синхронізація необхідна тоді, коли процесам, які відбуваються паралельно, потрібна взаємодія.

Ми розглядатимемо процес синхронізації інформатизації та кримінально-правового регулювання. Кримінальне право й інформатизація перебувають у стані постійної взаємодії. Право зменшує негативні наслідки розвитку комп'ютерних технологій. Інформатизація, своєю чергою, надає інструменти для підвищення ефективності кримінально-правового регулювання. Саме це ми й називаємо «синхронізацією» – узгодження двох процесів задля зменшення ризиків і посилення результативності.

Структура книги побудована відповідно до цього підходу. Спершу розглядається поняття інформаційної безпеки як самостійного об'єкта кримінально-правової охорони й види посягань на неї: «комп'ютерні» злочини, правопорушення у сфері обмеженого доступу до інформації та діяння, що впливають на формування інформаційного простору. Далі аналізується, як інформаційні технології сприяють підвищенню ефективності кримінального права – від криміналістичних баз даних до обчислювального кримінологічного аргументування та відкритих даних. Останній розділ – дослідження штучного інтелекту як подвійного явища. З одного боку, засіб оптимізації кримінальної юстиції та законодавчого процесу, з іншого, – він стає новим інструментом злочинців, що збільшує масштаби та створює раніше невідомі форми посягань.

¹ Синхронізація. *Словник української мови. Академічний тлумачний словник (1970–1980)*. URL: <https://sum.in.ua/s/synkhronizacija> (дата звернення: 21.09.2025).

Розділ 1

ІНФОРМАЦІЙНА БЕЗПЕКА

Необхідність у кримінально-правовому стимулюванні позитивного ефекту й мінімізації негативних наслідків інформатизації зумовила появу порівняно самостійного об'єкта посягання, який називатимемо «інформаційна безпека». Раніше ми обґрунтовували визначення та складові цієї групи суспільних відносин¹. Тож варто відновити лінію аргументації та помістити її в контекст актуальних подій.

Отже, інформаційна безпека – це система суспільних відносин щодо реалізації інформаційної потреби особи, суспільства, держави. Ця система складається з трьох елементів: відносини у сфері використання ІТ, відносини у сфері забезпечення доступу до інформації, відносини у сфері формування інформаційного поля.

Насамперед варто вказати на певну непослідовність використання поняття «інформаційна безпека» на рівні нормативно-правових документів. Закон України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. (нині втратив чинність) розглядав інформаційну безпеку як комплекс заходів, спрямованих на забезпечення захисту інформації від неправомірного витоку, перекручення, знищення тощо. Подібний підхід є й у Законі України «Про Національну програму інформатизації», прийнятому 1 грудня 2022 р.

¹ Карчевський М. В., Шульженко Н. В., Куковинець Д. О. Міжнародні стандарти, рекомендації ЄС, прогресивний зарубіжний досвід щодо кримінально-правової охорони інформаційної безпеки. *Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки* : монографія : електрон. наук. вид. / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2023. Розд. 1. С. 4–86. URL: https://ivpz.kh.ua/wp-content/uploads/2024/03/Моно_Інфобезпека_2023_НДІ-ВПЗ_авт_compressed.pdf (дата звернення: 21.09.2025) ; Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.

У контексті безпеки виключно комп'ютерних даних інформаційна безпека розглядається в нормативних документах, що регулюють банківську сферу¹ й безпеку об'єктів критичної інфраструктури².

Водночас рішення Ради національної безпеки і оборони України визначає інформаційну безпеку значно ширше: «Інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом»³.

Широке розуміння інформаційної безпеки характерне і юридичному науковому дискурсу. У дослідженнях у сфері теорії права⁴, основ

¹ Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах : постанова Нац. банку України від 02.07.2019 № 88. URL: <https://zakon.rada.gov.ua/laws/show/v0088500-19> (дата звернення: 21.09.2025) ; Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку : постанова Нац. банку України від 19.05.2021 № 43. URL: <https://zakon.rada.gov.ua/laws/show/v0043500-21> (дата звернення: 21.09.2025).

² Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури : постанова Каб. Міністрів України від 24.03.2023 № 257. URL: <https://zakon.rada.gov.ua/laws/show/257-2023-п> (дата звернення: 21.09.2025).

³ Про Стратегію інформаційної безпеки : рішення Ради нац. безпеки і оборони України від 15.10.2021, введ. в дію Указом Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21> (дата звернення: 21.09.2025).

⁴ Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави : автореф. дис. ... канд. юрид. наук : 12.00.01. Київ, 2011. 19 с.

національної безпеки¹, адміністративного права², кримінології та кримінального права³, політології⁴, міжнародних відносин⁵ інформаційна безпека не обмежується безпекою даних. Це є закономірним відображенням значення інформаційних процесів і масштабу відповідних соціальних змін. Зрозуміло, що визначення такого складного об'єкта, як інформаційна безпека, потребує уточнення залежно від сфери його використання. Ключові моменти кримінально-правового розуміння інформаційної безпеки полягають у наступному.

По-перше, у межах кримінально-правового регулювання інформаційна безпека є об'єктом посягання, тобто системою суспільних відносин. Її розгляд як певного стану або захищеності ресурсів є неправильним.

По-друге, інформаційна складова є майже в кожному виді суспільних відносин. Кримінально-правове регулювання в сфері інформаційної безпеки забезпечується за допомогою норм, що передбачають посягання на різноманітні родові об'єкти.

По-третє, необхідність у кримінально-правовому регулюванні у сфері інформаційної безпеки зумовлюється значенням реалізації інформаційної потреби громадян, суспільства або держави.

¹ Пилипчук В. Г. Теоретико-правові проблеми розвитку законодавства у сфері національної та інформаційної безпеки України. *Інформація і право*. 2025. № 2 (53). С. 9–22. DOI: [https://doi.org/10.37750/2616-6798.2025.2\(53\).334015](https://doi.org/10.37750/2616-6798.2025.2(53).334015) ; Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. ... канд. політ. наук : 21.01.01. Київ, 2005. 20 с.

² Кормич Б. А. Інформаційна безпека: організаційно правові основи : навч. посіб. Київ : Кондор, 2004. 384 с. ; Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. для студентів ВНЗ. Київ : КНТ, 2007. 531 с. ; Ліпкан В. А. Адміністративно-правові основи забезпечення національної безпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.07. Київ, 2008. 34 с.

³ Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України ; Батиргареева В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. 2020. № 1 (32). С. 110–119. DOI: [https://doi.org/10.37750/2616-6798.2020.1\(32\).200388](https://doi.org/10.37750/2616-6798.2020.1(32).200388).

⁴ Сашук Г. М. Безпекові імперативи телевізійного простору України : автореф. дис. ... канд. політ. наук : 23.00.03. Київ, 2005. 16 с.

⁵ Складенко О. А. Сучасні проблеми інформаційної безпеки України в умовах внутрішніх трансформацій. *Актуальні проблеми міжнародних відносин*. 2006. Вип. 64, ч. I. С. 125–131.

Інформаційна безпека розглядається нами як система суспільних відносин, що забезпечує умови для реалізації інформаційних потреб громадян, суспільства й держави. Задоволення цих потреб здійснюється через доступ до актуальної інформації, що, своєю чергою, ґрунтується на функціонуванні інформаційних технологій і наявності відповідного інформаційного ресурсу.

Як складна суспільна категорія інформаційна безпека охоплює три ключові групи відносин: 1) відносини щодо забезпечення доступу до інформаційних ресурсів – створюють передумови для отримання інформації; 2) відносини у сфері формування інформаційного простору – визначають якість, повноту, збалансованість і відповідність інформації суспільним потребам; 3) відносини щодо функціонування інформаційних технологій – забезпечують технічну можливість доступу до інформації, її створення, обробки й поширення.

Стан інформаційної безпеки досягається тоді, коли суб'єкт має у своєму розпорядженні повну, достовірну й достатню для прийняття рішень інформацію, що забезпечує ефективність його діяльності. Такий стан є результатом збалансованої взаємодії зазначених трьох груп суспільних відносин¹.

Серед означених суспільних відносин – ті, які охороняються законом про кримінальну відповідальність і складають зміст інформаційної безпеки як об'єкта кримінально-правової охорони.

¹ Карчевський М. В. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 27. С. 267–272.

Розділ 2

«КОМП'ЮТЕРНИЙ» ЗЛОЧИН

Поблизу затоки Чесапек (Вірджинія, США) 2004 року були виявлені три валізи з частинами тіла 39-річного Б. Макгвайра. Його дружину, М. Макгвайр, визнано винною у вбивстві. Вона використала снадійне, здійснила кілька пострілів у потерпілого, труп розчленувала. Суд призначив їй покарання у виді довічного ув'язнення¹. У комп'ютері засудженої знайдено сліди пошуку за темами: «снодійне», «отрута», «незаконне придбання зброї», а також листування засудженої та її керівника («romantic emails»).

На думку американської дослідниці С. Бреннер, цей випадок можна розглядати як приклад «кіберзлочину». Вона вважає, що є три категорії «кіберзлочинів»: 1) посягання, у яких комп'ютер є метою злочину; 2) посягання, у яких комп'ютер використовується як засіб учинення злочину; 3) посягання, у яких комп'ютер відіграє незначну роль у вчиненні злочину. Як приклад «кіберзлочинів»(!), що належать до третього виду, дослідниця наводить убивство Б. Макгвайра².

Д. Ластгауз в аналітичній статті «Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?»³ пропонує критичний огляд підходів до класифікації кіберзлочинів і їхньої відповідності емпіричній реальності. Він вважає, що дискусія стосовно природи кіберзлочинності тривалий час відбувається між двома підходами: сприйняттям її як цілком нового явища, що вимагає окремого теоре-

¹ Dooley S., Yamada H. 'Suitcase Killer' Melanie McGuire defends innocence from inside prison. *ABC News*. 2020, September 24. URL: <https://abcnews.go.com/US/suitcase-killer-melanie-mcguire-defends-innocence-inside-prison/story?id=73099717> (дата звернення: 21.09.2025).

² Brenner S. W. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara : Praeger, 2010. P. 39–48. (Crime, Media, and Popular Culture / Series eds.: F. Y. Bailey, S. Chermak). DOI: <https://doi.org/10.5040/9798400636554>.

³ Lusthaus J. Reconsidering crime and technology: what is this thing we call cybercrime? *Annual Review of Law and Social Science*. 2024. Vol. 20. P. 369–385. DOI: <https://doi.org/10.1146/annurev-lawsocsci-041822-044042>.

тичного осмислення, або як продовження звичних форм злочинності, адаптованих до цифрового середовища. У підсумку, як зазначає Д. Ластгауз, консенсус у науковій спільноті сформувався навколо більш широкого, інклюзивного підходу: кіберзлочинність – це радше парасольковий термін, який охоплює весь спектр протиправної діяльності в цифровому середовищі, ніж окрема кримінальна категорія¹.

Також зазначається, що однією з найбільш поширених є дихотомічна класифікація кіберзлочинів, яка поділяє їх на: 1) кіберзалежні злочини (cyber-dependent crimes), тобто ті, що не можуть бути вчинені без використання цифрових технологій (наприклад, створення вірусів, DDoS-атаки, злам систем); 2) кіберпосилені злочини (cyber-enabled crimes) – традиційні діяння, які стали масштабнішими або ефективнішими завдяки використанню інформаційно-комунікаційних технологій (ІКТ) (наприклад, шахрайство, відмивання коштів, дитяча експлуатація в Інтернеті). Цей поділ уперше формалізовано у звіті Міністерства внутрішніх справ Великої Британії², а згодом широко застосовано в науковій і правозастосовній практиці.

Однак, на думку Д. Ластгауза, така класифікація часто не витримує перевірки практикою, межа між кіберзалежними й кіберпосиленими посяганнями розмивається. Наприклад, в операціях із використанням зловмисного програмного забезпечення обов'язково беруть участь і технічні спеціалісти (розробники, інфекційні оператори), і класичні кримінальні суб'єкти – шахраї, «мули», відмивачі коштів, які функціонують у сфері звичайної організованої злочинності. Зрештою, автор пропонує відмовитися від жорстких дихотомій і застосовувати функціональне визначення: «Кіберзлочин – це злочин, у якому цифрові технології відіграють істотну роль»³.

¹ Bossler A. M., Berenblum T. Introduction: new directions in cybercrime research. *Journal of Crime and Justice*. 2019. Vol. 42, Iss. 5. P. 495–499. DOI: <https://doi.org/10.1080/0735648X.2019.1692426> ; Leukfeldt E. R., Yar M. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behavior*. 2016. Vol. 37, Iss. 3. P. 263–280. DOI: <https://doi.org/10.1080/01639625.2015.1012409>.

² McGuire M., Dowling S. Cyber crime: A review of the evidence / Home Office. October 2013. (Research Report 75). URL: <https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence> (дата звернення: 21.09.2025).

³ Lusthaus J. Reconsidering crime and technology: What is this thing we call cyber-crime?

У вітчизняній літературі також часто використовується поняття «комп'ютерні» кримінальні правопорушення, або «кіберзлочини». Доволі поширеним є віднесення до цієї категорії всіх суспільно небезпечних посягань, за яких електронне опрацювання інформації є знаряддям їх учинення та/або засобом¹ кримінальних правопорушень, пов'язаних із втручанням у роботу комп'ютерів або використанням комп'ютерів як необхідних технічних засобів².

Якщо погодитися з таким розумінням, «комп'ютерним» кримінальним правопорушенням може визнаватися будь-яке розкрадання, шпигунство, незаконне збирання відомостей, які становлять комерційну таємницю, тощо, якщо воно вчиняється з використанням комп'ютера. Такий підхід не дає змоги відобразити їхню сутність, специфіку й відрізнити від інших, у яких комп'ютер є лише знаряддям, засобом або предметом. Окрім того, подібні міркування та класифікації виглядають дуже спірними з погляду національного кримінально-правового дискурсу. Основою класифікації злочинів у кримінальному праві України є родовий об'єкт. Саме тому ми говоримо про кримінальні правопорушення проти власності чи основ національної безпеки й не міркуємо, наприклад, про лопатні кримінальні проступки.

Водночас у межах англо-американської правової доктрини такий підхід до визначення «комп'ютерних» кримінальних правопорушень є цілком допустимим. Тут матеріально-правові проблеми традиційно розглядаються в нерозривному зв'язку з процесуальними. Використання комп'ютерної техніки в процесі вчинення кримінальних правопорушень завжди зумовлює необхідність застосування специфічних криміналістичних і процесуальних засобів. Саме це і є ключовим аргументом для такого широкого підходу до визначення «комп'ютерних» кримінальних правопорушень.

¹ Азаров Д. Порухення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації. *Право України*. 2000. № 12. С. 72 ; Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, В. В. Бут, В. Д. Гавловський та ін. Київ : Атіка, 2002. С. 65.

² Голубев В. О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту*. 1997. № 2. С. 39–40 ; Лісовий В. «Комп'ютерні» злочини: питання кваліфікації. *Право України*. 2002. № 2. С. 86–88.

На нашу думку, поміщення важливих висновків зарубіжних колег у національний науковий дискурс потребує локалізації. Доречно в межах зарубіжної правової доктрини кримінального права широке визначення «комп'ютерних» кримінальних правопорушень, або «кіберзлочинів» має істотні обмеження для використання в національному юридичному дискурсі. Воно не відповідає класифікації кримінальних правопорушень у кримінальному праві України й, відповідно, не дає змоги виконувати завдання цієї класифікації. На законодавчому рівні кримінально-правового регулювання широке розуміння «комп'ютерних» злочинів не дає розуміння напрямів удосконалення законодавства й визначення критеріїв якості кримінального закону. На правозастосовному – не може розглядатися як інструмент організації та оцінки ефективності правозастосування.

Тобто якщо всі посягання, що вчиняються з використанням комп'ютерів, розглядати як новий вид кримінальних правопорушень, то відповідне оновлення кримінального законодавства має розглядатися як доповнення більшості статей Особливої частини Кримінального кодексу України (КК) кваліфікуючою ознакою «вчинене з використанням ІТ». Це очевидно неправильний шлях. Знову ж таки, якщо використовувати широке визначення «кіберзлочинів» на правозастосовному рівні, доходимо до ще одного повністю неправильного висновку: усі кримінальні правопорушення, вчинені з використанням комп'ютерів, має розслідувати кіберполіція. Зрозуміло, що це також не так. Подібний підхід не сприятиме ефективній роботі правоохоронців.

Широке визначення може бути використано в межах кримінологічних, криміналістичних або кримінально-процесуальних досліджень. У національному кримінально-правовому дискурсі використання такого поняття слід обмежити. Більш доречним буде використання окремих понять для посягань, передбачених розділом XVI Особливої частини КК, і решти посягань, які вчиняються з використанням комп'ютерної техніки. Перші пропонується називати «кримінальні правопорушення у сфері використання інформаційних технологій», другі – «кримінальні правопорушення, що вчиняються з використанням комп'ютерів».

НАУКОВО-ПРАКТИЧНИЙ КОМЕНТАР ДО РОЗДІЛУ XVI ОСОБЛИВОЇ ЧАСТИНИ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ТА КРИТИЧНА ОЦІНКА ПОТОЧНОЇ СУДОВОЇ ПРАКТИКИ

Кримінальні правопорушення, передбачені розділом XVI КК, посягають на *частину* відносин інформаційної безпеки – відносин, пов'язаних із застосуванням спеціальних технічних засобів, у межах яких забезпечується технічна можливість доступу до інформації, її створення, обробки й поширення.

У кримінальному законі наведено чотири види таких засобів: електронно-обчислювальна машина (комп'ютер), автоматизована система, комп'ютерна мережа й мережа електрозв'язку.

Відповідно до визначення міжнародної організації стандартизації, імплементація якого здійснена у ДСТУ ISO/IEC 2382:2017, ЕОМ (комп'ютер) є функціональним блоком, що може виконувати значні обчислення, включно з численними арифметичними й логічними операціями, без втручання людини¹. Відносини інформаційної безпеки, пов'язані з використанням таких пристроїв, – найпростіша форма застосування комп'ютерної техніки для роботи з інформацією. Варто зазначити, що під ЕОМ розуміють не тільки комп'ютери в їх «класичному» виді, а й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини. Йдеться про бор-

¹ ДСТУ ISO/IEC 2382:2017. Інформаційні технології. Словник термінів (ISO/IEC 2382:2015, IDT). Чинний від 01.01.2019. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=75076 (дата звернення: 21.09.2025).

тові комп'ютери транспортних засобів¹, електронні лічильники електроенергії, інші технології, які зараз прийнято об'єднувати поняттям «інтернет речей»².

Відповідно до стандарту ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення» від 1 липня 1994 р. автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, що здійснює цю діяльність³. На відміну від звичайних комп'ютерів, які мають загальне призначення, автоматизовані системи – це комплекси, які забезпечують автоматизацію певного виду діяльності людини. Наприклад, банківський автомат є конструкцією з електронно-обчислювальної машини, засобу ідентифікації користувача, сховища для банкнот і механізму їх видачі. Такий пристрій є автоматизованою системою.

Комп'ютерна мережа – мережа вузлів обробки даних, які з'єднані між собою з метою передачі даних⁴. Ключове завдання, що виконується в межах цих відносин, є забезпечення спільного доступу до інформаційних або апаратних ресурсів мережі. Найвідомішою та найпоширенішою глобальною комп'ютерною мережею є Інтернет.

Закон України «Про електронні комунікації» визначає «електронну комунікаційну мережу» як «комплекс технічних засобів електронних комунікацій та споруд, призначених для надання *електронних комунікаційних послуг*». Своєю чергою, «електронна комунікаційна послуга» полягає в «прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних

¹ Карчевський М. В., Савченко А. В. Особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 30. С. 254–259.

² Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1 : Сфери застосування, ризики і бар'єри, проблеми правового регулювання : монографія / НДІП НАПрН України. Київ : АртЕк, 2018. 344 с.

³ ДСТУ 2226:1993. Автоматизовані системи. Терміни та визначення. Чинний від 01.07.1994. Вид. офіц. Київ, 1994. С. 2.

⁴ ДСТУ ISO/IEC 2382:2017 Інформаційні технології. Словник термінів (ISO/IEC 2382:2015, IDT).

мереж і послуг». Нарешті «електронна комунікація (телекомунікація, електрозв'язок)» – «передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій». Отже, відносно, засобом забезпечення яких є мережі електрозв'язку, полягають у наданні й отриманні послуг електрозв'язку, тобто у використанні мереж електрозв'язку для передачі або приймання інформації.

Водночас наявність у законі про кримінальну відповідальність одночасно з терміном «мережа електрозв'язку» іншого – «комп'ютерна мережа» – фактично означає, що під мережею електрозв'язку треба розуміти всі телекомунікаційні мережі, крім комп'ютерних. Ідеться про мережі міського, міжміського й міжнародного телефонного зв'язку, рухомого (мобільного) зв'язку, проводового радіомовлення, ефірного телерадіомовлення. Такі мережі є предметом несанкціонованого втручання в разі незаконного підключення до мереж кабельного телебачення, створення перешкод під час користування мережами радіозв'язку, мобільного зв'язку тощо.

Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX визначення несанкціонованого втручання (ст. 361 КК) й незаконних дій із шкідливими пристроями (ст. 361-1 КК) сформульоване з використанням іншого переліку технічних засобів опрацювання інформації, ніж той, що використовується в назві розділу XVI і ст. 361-2, 362, 363 та 363-1 КК (табл. 1).

Таблиця 1

**Переліки технічних засобів обробки інформації,
що використовуються в розділі XVI Особливої частини КК**

Перелік технічних засобів обробки інформації, що використовується в назві розділу XVI, ст. 361-2, 362, 363 та 363-1 КК	Перелік технічних засобів обробки інформації, що використовується у ст. 361, 361-1 КК
електронно-обчислювальна машина (комп'ютер);	інформаційна (автоматизована) система;

Кінець табл. 1

Перелік технічних засобів обробки інформації, що використовується в назві розділу XVI, ст. 361-2, 362, 363 та 363-1 КК	Перелік технічних засобів обробки інформації, що використовується у ст. 361, 361-1 КК
• автоматизована система; • комп'ютерна мережа; • мережа електрозв'язку	• електронна комунікаційна система; • інформаційно-комунікаційна система; • електронна комунікаційна мережа

Таке законодавче рішення породжує питання співвідношення понять, що використовуються в назві розділу XVI і ст. 361, 361-1 КК.

Поняття «електронна комунікаційна мережа» є тотожним до розглянутого раніше поняття «мережа електрозв'язку».

Решта видів технічних засобів, перелічених у диспозиції ст. 361 КК, визначаються Законом України «Про захист інформації в інформаційно-комунікаційних системах». Інформаційна (автоматизована) система – організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у виді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб. Інформаційно-комунікаційна система – сукупність інформаційних й електронних комунікаційних систем, які в процесі обробки інформації діють як ціле.

Співвідношення понять «електронно-обчислювальна машина» (ЕОМ), «автоматизована система» (АС) й «інформаційна (автоматизована) система». Раніше ми наводили визначення ЕОМ та АС, які містяться в державних стандартах. Відповідно до визначення, яке міститься в Законі України «Про захист інформації в інформаційно-комунікаційних системах», поняття «інформаційна (автоматизована) система» охоплює і ЕОМ, і АС. Отже, відповідно до чинної редакції ст. 361 КК несанкціонованим втручанням в роботу інформаційної

(автоматизованої) системи слід вважати і порушення роботи окремих комп'ютерів (ЕОМ), і систем, призначених для автоматизації певних видів діяльності людини, наприклад, банкоматів.

Співвідношення поняття «комп'ютерна мережа», що використовується в назві розділу XVI, та понять «електронна комунікаційна система» й «інформаційно-комунікаційна система», що використовуються в ст. 361 і 361-1 КК. Електронними комунікаційними системами є маршрутизатори, комутатори, антени, передавачі тощо. До прикладів інформаційно-комунікаційних систем можна віднести інтегровані системи управління підприємством, хмарні обчислювальні платформи або системи відеоконференцій. Перші та другі, попри певні схожі риси, виконують різні функції. Електронні комунікаційні системи забезпечують інфраструктуру для зв'язку між користувачами або пристроями. Можна сказати, що вони відповідають за фізичну передачу сигналів, таких як радіохвилі, оптичні сигнали в оптоволоконних кабелях тощо. Інформаційно-комунікаційні системи охоплюють ширший спектр функцій. Вони включають не лише передачу інформації, а й її зберігання, обробку, управління та представлення користувачам. Електронні комунікаційні системи забезпечують передачу інформації, можуть бути частиною більш складних систем, але самі собою вони не обробляють і не аналізують дані. Натомість інформаційно-комунікаційні системи інтегрують і можливості передачі даних, і їхньої обробки.

Отже, поняття «комп'ютерна мережа», наведене в назві розділу XVI КК, охоплює поняття «електронна комунікаційна система» й «інформаційно-комунікаційна система», які використано в диспозиціях ст. 361, 361-1 КК¹.

¹ Карчевський М. В., Федюк В. В. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кримінально-правова охорона інформаційної безпеки в Україні* : монографія / за заг. ред. В. І. Борисова, О. О. Пащенко ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. Розд. III. С. 165–187. DOI: <https://doi.org/10.31359/9786178518899>.

3.1. Несанкціоноване втручання (ст. 361 Кримінального кодексу України)

Безпосередній об'єкт складається із суспільних відносин власності на комп'ютерну інформацію та відносин надання й отримання послуг електрозв'язку.

Право власності на комп'ютерну інформацію є сукупністю права й можливості особи володіти інформацією, змінювати, використовувати її для задоволення своєї інформаційної потреби, давати змогу іншим особам використовувати інформацію. Такі суспільні відносини регулюються складним комплексом правових норм. Загальні положення визначаються Законом України «Про інформацію» та, залежно від змісту інформації, конкретизуються в Цивільному кодексі України, Законах України «Про захист персональних даних», «Про цифровий контент та цифрові послуги», «Про медіа», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-комунікаційних системах» тощо.

Суспільні відносини надання та отримання послуг електрозв'язку – забезпечення операторами та провайдерами можливості споживачів телекомунікацій передавати та приймати знаки, сигнали, письмовий текст, зображення, звуки або повідомлення будь-якого роду за допомогою радіо, проводових, оптичних або інших електромагнітних систем за виключенням комп'ютерних мереж¹.

Предметом кримінального правопорушення, передбаченого ч. 1, 2 та 4 ст. 361 КК, є інформаційні (автоматизовані) системи, електронні комунікаційні системи, інформаційно-комунікаційні системи й електронні комунікаційні мережі. Предмет кримінального правопорушення, передбаченого ч. 3 ст. 361 КК, – інформація. Предметом правопорушення, передбаченого ч. 5 ст. 361 КК, можуть бути і наведені технічні засоби роботи з інформацією, і інформація.

¹ Більш докладно див.: Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. С. 116–118.

До предметів кримінального правопорушення, передбаченого ч. 3, 5 ст. 361 КК, належить *комп'ютерна інформація та інформація, що передається каналами електрозв'язку*.

Комп'ютерна інформація – відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника й ціну¹. Характеризується сукупністю трьох ознак: фізичної, економічної і юридичної.

Фізична ознака полягає в наявності носія, котрий зазвичай розуміють як предмет, річ, властивості якої використовують для передачі, зберігання та обробки інформації. Носіями комп'ютерної інформації є оптичні й жорсткі диски, flash-носії, SD-карти, сигнали в мережах передавання даних тощо.

Економічна ознака, ціна. Інформація може бути цінною по суті, оскільки є результатом тривалої роботи значної кількості осіб, а може бути цінною за призначенням, адже її наявність є умовою для вирішення певного завдання.

Юридична ознака комп'ютерної інформації полягає в тому, що вона має бути *чужою* для винного й мати свого власника.

Інформація, що передається каналами електрозв'язку. Якщо комп'ютерна інформація – це відомості, подані у формі, яка дає змогу опрацювати їх за допомогою комп'ютерної техніки, то інформація, що передається мережами електрозв'язку, є *відомостями, поданими у формі, що дає змогу їх приймати або передавати засобами електрозв'язку*. Інформація в цих мережах передається за допомогою сигналів, які є матеріальними носіями передавання інформації.

Об'єктивна сторона. За конструкцією об'єктивної сторони склади несанкціонованого втручання, передбачені ч. 1 і 2 ст. 361 КК, є формальними. Діяння полягає в несанкціонованому втручанні в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем або електронних комунікаційних мереж. Частини 3, 4 й 5 ст. 361 КК передбачають матеріальні склади, аналогічне ч. 1 ст. 361 КК діяння та різні види наслідків.

¹ Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. С. 119–123.

Частина 3 ст. 361 КК передбачає відповідальність за несанкціоноване втручання, якщо воно призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Частина 4 – за несанкціоноване втручання, яке заподіяло значну шкоду чи створило небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Частина 5 – за несанкціоноване втручання, яке призвело до наслідків, передбачених ч. 3 або ч. 4, вчинене під час дії воєнного часу.

Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем або електронних комунікаційних мереж – будь-яка зміна режиму їх роботи, учинена з порушенням встановленого відповідно до законодавства порядку доступу до інформації, що заподіює шкоду суспільним відносинам власності на комп'ютерну інформацію або відносинам у сфері надання послуг електрозв'язку.

Витік комп'ютерної інформації – результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Витік є порушенням такого повноваження власника комп'ютерної інформації, як право розпорядження.

Втрата комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, що дає змогу опрацювати її за допомогою комп'ютерної техніки.

Підробка комп'ютерної інформації – зміна без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.

Блокування комп'ютерної інформації – дії, унаслідок яких унеможливорюється доступ до інформації в системі, є ситуацією, коли комп'ютерна інформація не знищена, не підроблена, але можливості її використовувати немає.

Спотворення процесу обробки комп'ютерної інформації – отримання під час операцій із комп'ютерною інформацією, які здійсню-

валися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми.

Порушення встановленого порядку маршрутизації комп'ютерної інформації відбувається, якщо комп'ютерна інформація, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), ним не отримується або доступ до певних мережевих ресурсів здійснюється з порушенням встановленого порядку.

Витік інформації, що передається мережею електрозв'язку, – результат несанкціонованого втручання в роботу мережі електрозв'язку, унаслідок якого інформація, що передається мережею, стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї.

Втрата інформації, що передається мережами електрозв'язку, – це порушення електрозв'язку у виді неотримання абонентом мережі інформації, якому вона надсилається.

Підробка інформації, що передається мережею електрозв'язку, – такий вплив на носій інформації, що передається мережею електрозв'язку, у результаті якого абонент отримує відомості, котрі не збігаються з тими, що були йому надіслані.

Блокування інформації, що передається каналами зв'язку, – неможливість або значне ускладнення протягом певного часу отримувати чи надсилати інформацію за допомогою цієї мережі.

Порушення порядку маршрутизації інформації в мережі електрозв'язку відбувається, коли інформація, що передається за допомогою мережі конкретному абонентові (абонентам), ним не отримується, а також у випадках отримання інформації, що передається в мережі, на кінцеве обладнання, яке не є складовою цієї мережі. Типовими прикладами несанкціонованого втручання в роботу мереж електрозв'язку з настанням таких наслідків є незаконне підключення телефонних апаратів до мереж телефонного зв'язку, а також незаконне підключення телевізійних приймачів до мереж кабельного телебачення. Проте зазначимо, що існують і більш складні види порушення порядку маршрутизації, які пов'язані, зокрема, з маршрутизацією вхідного міжнародного трафіку на телефонні мережі

загального користування. У судовій практиці такий вид досліджуваних наслідків траплявся в контексті правової оцінки осіб, які займалися незаконною діяльністю щодо надання послуг IP-телефонії.

Під *спотворенням процесу обробки інформації*, що передається каналами електрозв'язку, потрібно розуміти отримання під час роботи технічного засобу зв'язку результатів, що не відповідають його характеристики.

Значною шкодою, згідно з приміткою до ст. 361 КК, вважається така, яка в триста й більше разів перевищує неоподатковуваний мінімум доходів громадян. Зазвичай ця шкода полягає в заподіянні позитивних матеріальних збитків, також може виражатися в упущеній вигоді. Крім утрати або зменшення обсягу інформації, якою володіє потерпілий, у розмір матеріальних збитків від «комп'ютерного» кримінального правопорушення слід вносити також й упущену вигоду, яка може полягати в укладанні не вигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Створення небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Така шкода, як порушення нормальної роботи підприємств, зупинення або порушення складних технологічних процесів, погіршення обороноздатності держави, підрив авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення безпеки руху транспорту тощо.

Суб'єкт *несанкціонованого втручання* загальний; ним є фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивна сторона *несанкціонованого втручання*, передбаченого ч. 1 ст. 316 КК, полягає в усвідомленні винною особою *несанкціонованого характеру* своїх дій та бажанні вчиняти такі дії.

Суб'єктивна сторона *несанкціонованого втручання*, передбаченого ч. 3 ст. 361 КК, полягає в тому, що особа: а) усвідомлювала суспільну небезпеку втручання, тобто фактичні й соціальні ознаки діяння, його *несанкціонованість*; б) передбачала наслідки у вигляді витоку, втрати, підроблення, блокування інформації, спотворення процесу обробки інформації або порушення порядку її маршрутизації;

в) бажала або свідомо припускала настання цих наслідків. Тобто суб'єктивна сторона аналізованого складу може виражатись у вигляді і прямого, і непрямого умислу¹.

Суб'єктивна сторона несанкціонованого втручання, яке заподіяло значну шкоду або тяжкі наслідки (ч. 4, 5 ст. 361 КК), характеризується змішаною формою вини. Психічне ставлення особи до діяння, несанкціонованого втручання виражається в умислі, а до наслідків може бути і умисним, і необережним. У деяких випадках умисне заподіяння похідних наслідків у результаті кримінального правопорушення у сфері використання інформаційних технологій може бути інший склад кримінального правопорушення. Наприклад, знищення комп'ютерної інформації, критично важливої для обороноздатності країни, з метою ослаблення держави не буде вважатися несанкціонованим втручанням, яке заподіяло тяжкі наслідки, а вважатиметься диверсією (ст. 113 КК).

3.2. Шкідливі програмні або технічні засоби (ст. 361-1 Кримінального кодексу України)

Предмет – призначені для несанкціонованого втручання шкідливі програмні засоби та шкідливі технічні засоби.

Ознака «шкідливі» вказує на здатність програмних і технічних засобів завдавати шкоди інформаційним відносинам, які забезпечуються комп'ютерною технікою чи мережами електрозв'язку, або створювати загрозу такої шкоди. Друга ознака, «призначені для несанкціонованого втручання», підкреслює їхнє спеціальне призначення – несанкціоноване втручання в роботу комп'ютерної техніки чи мереж. На відміну від інших комп'ютерних програм і обладнання шкідливі засоби спеціально розробляються для порушення роботи інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем або електронних комунікаційних мереж.

¹ З цього питання див. також: Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження). Київ : Атіка, 2007. С. 190.

Шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу інформаційних, електронних, інформаційно-комунікаційних систем або електронних комунікаційних мереж, – програмне забезпечення, спеціально створене для такого втручання, яке призводить або може призвести до шкоди інформаційним відносинам.

Технічні засоби, призначені для несанкціонованого втручання в роботу інформаційних, електронних, інформаційно-комунікаційних систем або електронних комунікаційних мереж, – різноманітні пристрої та обладнання, розроблені для того, щоб порушувати роботу комп'ютерної техніки або мереж, що спричиняє або може спричинити шкоду інформаційним відносинам.

Кримінальне правопорушення, передбачене ч. 1 ст. 361-1 КК, вважається закінченим із моменту вчинення одного з альтернативних діянь, зазначених у диспозиції. Досліджувана норма передбачає такі форми **об'єктивної сторони**:

- 1) створення шкідливих програмних або технічних засобів із метою використання, розповсюдження або збуту;
- 2) розповсюдження шкідливих програмних або технічних засобів;
- 3) збут шкідливих програмних або технічних засобів.

Створення – результат діяльності щодо розроблення шкідливих засобів у вигляді нового шкідливого програмного або технічного засобу. Створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони – мети використання, розповсюдження або збуту.

Розповсюдження шкідливих програмних засобів – це оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх «закладання» в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення шляхом самовідтворення¹.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний із відчуженням предмета.

¹ Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія : монографія / І. Р. Шинкаренко, В. О. Голубев, М. В. Карчевський, І. Ф. Хараберюш ; МВС України, Донець. юрид. ін-т Луган. держ. ун-ту внутр. справ. Донецьк : РВВ ЛДУВС, 2007. 266 с.

Якщо при розповсюдженні предмет залишається в особи (шкідливе програмне забезпечення продовжує бути на мережевому ресурсі, з якого розповсюджується, повертається шкідливий програмний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває. Збут шкідливих програмних або технічних засобів – оплатне або безоплатне відчуження. Типовим прикладом збуту шкідливих програм є продаж носіїв із записаними на них шкідливими програмами.

Суб'єкт незаконних дій із шкідливими програмними або технічними засобами загальний, ним є фізична осудна особа, яка досягла 16-річного віку.

Оскільки кримінальне правопорушення, передбачене ст. 361-1 КК, характеризується формальним складом, зміст його **суб'єктивної сторони** визначається лише психічним ставленням до діяння і полягає в усвідомленні суспільної небезпечності та протиправності створення, розповсюдження або збуту шкідливих програмних і технічних засобів та бажанні вчинення таких дій. Отже, у цій формі умисел може бути тільки прямим, а його специфіка полягає в тому, що свідомістю особи обов'язково охоплюється розуміння того, що створювані або розповсюджувані засоби спеціально призначені для несанкціонованого втручання.

Обов'язковою ознакою суб'єктивної сторони є усвідомлення особою особливостей та призначення технічних і програмних засобів, які вона поширює. Якщо особа не усвідомлює властивості цих засобів, вона не підлягає кримінальній відповідальності за їх поширення.

3.3. Розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 Кримінального кодексу України)

Об'єктом кримінального правопорушення, передбаченого ст. 361-2 КК, є суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом.

Предметом злочину є інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. Тобто інформація, що є предметом злочину, передбаченого ст. 361-2 КК, характеризується такими ознаками:

- 1) вона належить до інформації з обмеженим доступом;
- 2) зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;
- 3) створена відповідно до чинного законодавства;
- 4) захищена відповідно до чинного законодавства.

До *інформації з обмеженим доступом* згідно зі ст. 21 Закону України «Про інформацію» належить конфіденційна, таємна та службова інформація.

Інформація як предмет кримінального правопорушення, передбаченого ст. 361-2 КК, є комп'ютерною, тобто подана у формі, що дає змогу її оброблення або зберігання з використанням комп'ютерної техніки.

Інформація, що є предметом, *створена відповідно до чинного законодавства*. Розповсюдження або збут інформації, створеної з порушенням законодавства, не є кримінальним правопорушенням, передбаченим ст. 361-2 КК.

До «інформації, захищеної відповідно до чинного законодавства», слід відносити й ту, що підлягає обов'язковому захисту, й ту, захист якої може здійснюватися відповідно до закону. Так, згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» власник системи, у якій оброблюється інформація, що є власністю держави, або інформація з обмеженим доступом, вимогу щодо захисту якої встановлено законом, зобов'язаний утворювати службу захисту інформації (ч. 2 ст. 9 Закону). Крім того, така інформація повинна оброблятися із застосуванням «*комплексної системи захисту інформації з підтвердженою відповідністю*» (ч. 2 ст. 8 Закону). Водночас ч. 2 ст. 21 Закону України «Про інформацію» наділяє громадян та юридичних осіб правом самостійно визначати режим доступу до неї, включно з належністю її до категорії конфі-

денційної. Своєю чергою відповідно до ст. 162 Господарського кодексу України однією з умов наявності такого права є вживання належних заходів до охорони її конфіденційності.

За конструкцією **об'єктивної сторони** правопорушення, передбачене ст. 361-2 КК, є формальним. Воно вважається закінченим із моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженням доступом.

Збут або розповсюдження інформації буде *несанкціонованим*, якщо вчиняється без дозволу власника цієї інформації.

Розповсюдження комп'ютерної інформації з обмеженням доступом – платне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб.

Збут комп'ютерної інформації з обмеженням доступом – платне або безоплатне відчуження.

Суб'єкт – загальний. Якщо збут або розповсюдження інформації з обмеженням доступом учиняє особа, якій інформацію було довірено у зв'язку з виконанням службових або професійних обов'язків, вчинене за наявності відповідних ознак суб'єктивної сторони необхідно кваліфікувати за ст. 232 або ст. 328 КК.

Суб'єктивна сторона цього правопорушення характеризується виною у формі прямого умислу: особа усвідомлює суспільну небезпечність і протиправність збуту або розповсюдження комп'ютерної інформації з обмеженням доступом і бажає вчиняти такі дії. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або розповсюджує, є інформацією з обмеженням доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

3.4. Незаконні дії осіб, які мають право доступу до комп'ютерної інформації (ст. 362 Кримінального кодексу України)

Об'єкт – суспільні відносини власності на комп'ютерну інформацію.

Предмет – інформація, яка опрацьовується в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації.

Об'єктивна сторона розглянутого кримінального правопорушення характеризується наявністю декількох форм:

- 1) несанкціонована зміна комп'ютерної інформації;
- 2) несанкціоноване знищення комп'ютерної інформації;
- 3) несанкціоноване блокування комп'ютерної інформації;
- 4) несанкціоноване перехоплення комп'ютерної інформації, що призвело до її витоку;
- 5) несанкціоноване копіювання комп'ютерної інформації, що призвело до її витоку.

Несанкціонована зміна комп'ютерної інформації – порушення права власності на інформацію шляхом перекручення без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особи, яка має право власності на таку інформацію.

Несанкціоноване знищення комп'ютерної інформації відбувається тоді, коли вона перестає існувати у формі, яка дає змогу її опрацьовувати за допомогою комп'ютерної техніки.

Несанкціоноване блокування комп'ютерної інформації – позбавлення власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено й не підроблено.

Якщо три перші форми є простими, звичайними правопорушеннями з матеріальним складом і вважаються закінченими з моменту настання зазначених наслідків, то структура двох останніх – несанкціонованого перехоплення та копіювання – ускладнена наявністю похідного наслідку – витоку інформації, якому передують такі види порушення права власності на комп'ютерну інформацію, як несанкціоноване копіювання або перехоплення.

Предметом несанкціонованого перехоплення або копіювання є тільки комп'ютерна інформація з обмеженим доступом.

Копіювання комп'ютерної інформації – відтворення, з перевищенням наданих власником прав доступу, комп'ютерної інформації з обмеженим доступом зі збереженням вихідної інформації.

Перехоплення є специфічним видом копіювання, отримання, з перевищенням наданих власником прав, копії інформації з обмеженим доступом за допомогою специфічних технічних засобів під час передавання цієї інформації від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем чи комп'ютерних мереж, у яких опрацьовується така інформація.

Суб'єкт спеціальний – особа, яка має право доступу до комп'ютерної інформації. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації.

Суб'єктивна сторона характеризується виною у формі прямого або непрямого умислу: особа усвідомлює суспільну небезпечність і протиправність своїх дій і бажає або свідомо допускає настання наслідків. Водночас особа має усвідомлювати, що вчиняє такі дії, які є перевищенням повноважень, наданих власником інформації.

3.5. Порухення правил експлуатації комп'ютерної техніки, порядку чи правил захисту інформації (ст. 363 Кримінального кодексу України)

Об'єкт – суспільні відносини, у межах яких забезпечується безпека використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

Правила експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку є вимогами, які висуває власник ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Вони зазвичай містяться в окремих

підзаконних актах (наказах, розпорядженнях), що видаються власником комп'ютерної техніки або мережі електрозв'язку.

Порядок захисту інформації – це визначені нормативно-правовими актами вимоги до створення системи захисту інформації та організації її роботи.

Правила захисту інформації – вимоги до використання системи захисту інформації певного інформаційного ресурсу. Тобто якщо систему захисту певного інформаційного ресурсу не створено, то й неможливо порушити правила захисту цього ресурсу. Те, що систему захисту не створено, може бути визнано, за наявності відповідних нормативно-правових положень, порушенням порядку захисту інформації.

Порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, у яких обробляється недержавна інформація, стосовно якої законодавство не встановлює спеціальних вимог до забезпечення її захисту, а також порушення порядку чи правил захисту такої інформації, якщо воно заподіяло істотну шкоду, вважатиметься кримінальним правопорушенням, передбаченим ст. 363 КК, лише тоді, коли власником інформації або власником засобу автоматизованого опрацювання інформації у формі наказу, розпорядження або іншого офіційного документа закріплено відповідні правила експлуатації, порядок і правила захисту інформації.

Склад правопорушення, передбаченого цією статтею, матеріальний, його **об'єктивна сторона** характеризується такими ознаками:

1) діяння – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації;

2) суспільно небезпечні наслідки – значна шкода;

3) причинний зв'язок між діянням і суспільно небезпечними наслідками.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – недотримання вимог, що висуваються

власником ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі користувача самостійно встановлювати нове програмне або апаратне забезпечення, підключенні комп'ютерної техніки до електромережі без фільтрів, порушенні порядку включення або відключення засобів комп'ютерної техніки тощо.

Порушення порядку захисту комп'ютерної інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи. Прикладом такого діяння може бути використання комп'ютерної техніки для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту.

Порушення правил захисту комп'ютерної інформації – недотримання вимог щодо використання системи захисту інформації певного інформаційного ресурсу. Це може бути, наприклад, неналежне зберігання паролів для доступу до інформації.

Оскільки аналізований склад є матеріальним, він вважатиметься закінченим від моменту настання суспільно небезпечних наслідків – значної шкоди. За змістом закону під значною в цій нормі слід розуміти будь-яку шкоду, заподіяну порушенням нормативів інформаційної безпеки. Водночас у разі якщо вона полягає в заподіянні матеріальних збитків, значною слід уважати таку шкоду, яка в триста й більше разів перевищує неоподатковуваний мінімум доходів громадян.

Суб'єкт кримінального правопорушення, передбаченого ст. 363 КК, спеціальний – особа, яка відповідає за експлуатацію електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації чи засобу її автоматизованого опрацювання та закріпленими на підставі цього наказу функціональними обов'язками.

Суб'єктивна сторона характеризується тим, що діяння може бути вчинено і умисно, і з необережності, а стосовно наслідків можлива тільки необережність. Якщо настання наслідків охоплюється умислом

винної особи, то складу правопорушення, передбаченого ст. 363 КК, немає. У такому разі дії винної особи, за наявності відповідних ознак, необхідно кваліфікувати як умисне пошкодження майна (ст. 194 КК), або як пособництво в несанкціонованому втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електров'язку (ч. 5 ст. 27, ст. 361 КК), або як несанкціоновані дії з комп'ютерною інформацією, учинені особою, яка має доступ до неї (ст. 362 КК).

3.6. Масове розповсюдження повідомлень електров'язку (ст. 363-1 Кримінального кодексу України)

Об'єкт – суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки й мереж електров'язку як технічних засобів забезпечення відносин власності на інформацію.

Предметом цього кримінального правопорушення є повідомлення електров'язку – відомості, подані у виді, що дає змогу їх передавати за допомогою комп'ютерних мереж або мереж електров'язку.

До ознак його об'єктивної сторони належать: 1) діяння – масове розповсюдження повідомлень електров'язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні наслідки – порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електров'язку; 3) причинний зв'язок між діянням і наслідками.

Діяння як ознака об'єктивної сторони цього складу полягає в розповсюдженні повідомлень електров'язку, тобто надісланні певним адресатам копій цих повідомлень, яке, по-перше, є масовим і, по-друге, здійснюється без попередньої згоди адресатів.

Розповсюдження слід уважати *масовим* тоді, коли одне або кілька повідомлень отримує більше ніж один адресат, адже в диспозиції аналізованої статті йдеться про множинність повідомлень електров'язку та їх адресатів. Зазначимо, що поняття «масове» в цій нормі ви-

користовується як оцінне, тобто встановлення того, чи було певне розповсюдження повідомлень електрозв'язку масовим, залежить від аналізу багатьох обставин конкретного розповсюдження (кількість повідомлень або копій повідомлень, їх розмір; кількість адресатів; час, який використано для розповсюдження; технічні характеристики обладнання, що використовувалося для розповсюдження тощо).

Відсутність попередньої згоди адресатів полягає в тому, що адресат ні в якій формі (письмово, усно, шляхом використання електронної пошти або в інший спосіб) не давав згоди на надсилання йому повідомлень, які є предметом правопорушення.

Порушення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку є такою зміною режиму роботи комп'ютерної техніки або мережі електрозв'язку, яка створює загрозу для їх функціонування, тобто погіршення роботи повністю або частково, тимчасове створення перешкод для використання за призначенням.

Припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в тимчасовому або остаточному припиненні функціонування комп'ютерної техніки або мереж електрозв'язку, невиконанні ними завдань щодо зберігання, опрацювання, пересилання чи отримання комп'ютерної інформації або інформації, що передається мережами електрозв'язку.

Суб'єкт цього кримінального правопорушення загальний.

Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно діяння та умисним або необережним ставленням до наслідків. Особа усвідомлює, що вчиняє масове розповсюдження повідомлень електрозв'язку, і бажає вчиняти такі дії, а також вона бажає або свідомо допускає порушення чи припинення роботи комп'ютерної техніки чи мереж електрозв'язку або легковажно розраховує на ненастання таких наслідків.

Особливість складу правопорушення, передбаченого ст. 363-1 КК, полягає передусім в ознаках об'єкта. Ця норма захищає суспільні відносини щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності, тимчасом як більшість інших

норм аналізованого розділу забезпечують кримінально-правову охорону відносинам власності на комп'ютерну інформацію, тобто певному виду інформаційної діяльності. Тому коли масове розсилання повідомлень електрозв'язку призводить, скажімо, до блокування комп'ютерної інформації, а функціонування засобів автоматизованого опрацювання інформації не порушено, ознак складу злочину, передбаченого ст. 363-1 КК, немає. За наявності відповідних ознак такі дії слід кваліфікувати як несанкціоноване втручання (ст. 361 КК), адже шкоду в такій ситуації заподіяно тільки відносинам власності на комп'ютерну інформацію. Водночас якщо особа здійснила, наприклад, масове розповсюдження комп'ютерної інформації з обмеженим доступом, що внаслідок надмірного перевантаження призвело до порушення роботи комп'ютерної мережі, то є ідеальна сукупність злочинів, передбачених ст. 361-2 та ст. 363-1 КК. У цій ситуації шкода заподіюється і відносинам власності на комп'ютерну інформацію з обмеженим доступом, і відносинам щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності.

3.7. Що «не так» із протидією кримінальним правопорушенням у сфері використання інформаційних технологій

Проведене нами дослідження показало, що наведені в судовій практиці «комп'ютерні» кримінальні правопорушення можна поділити на три групи: високої поширеності (64%), середньої поширеності (25%) і низької поширеності (11%). До кримінальних правопорушень високої поширеності належать: зміна даних, здійснена особами, які мають право доступу до комп'ютерної інформації (23%); несанкціоновані транзакції (22%), у цих випадках несанкціоноване втручання інкримінується додатково до крадіжки або шахрайства; розповсюдження або збут комп'ютерної інформації з обмеженим доступом (19%). «Комп'ютерними» кримінальними правопорушеннями

середньої поширеності слід визнати: отримання або використання авторизаційних даних (9%), копіювання інформації, учинене особою, яка має право доступу до неї, якщо це призвело до витоку (6%), внесення даних до реєстрів загальним суб'єктом (5%) і розповсюдження або збут шкідливих засобів (5%). Решту кримінальних правопорушень у сфері використання інформаційних технологій проведене дослідження дає змогу віднести до таких, що характеризуються низькою поширеністю¹.

За особливостями використання засобів кримінально-правового реагування випадки засудження за кримінальні правопорушення, передбачені розділом XVI Особливої частини КК, можуть бути поділені на дві групи: перша характеризується переважним використанням реальних покарань (67–69%) у вигляді штрафів й укладанням угод (69–79%) про визнання винуватості (ст. 361-1, 361-2 КК, 27,6% від обвинувальних вироків); другій характерне більш широке використання звільнення від покарання (63–68%) і менше використання угод (37–54%) про визнання винуватості (ст. 361, 362 КК, 72% від обвинувальних вироків)².

Такі результати актуалізують розгляд питання про ефективність протидії «комп'ютерним» кримінальним правопорушенням. Інтенсивність кримінально-правового впливу, зумовленого «комп'ютерними» злочинами, є нижчою за середню: реальні покарання застосовуються рідше, серед них переважають штрафи. Це відбувається на тлі розширення використання ІТ і зростання вразливості суспільних відносин до зламів систем, DDoS-атак, шкідливого програмного забезпечення тощо. Прогнозованим є підвищення небезпечності цих діянь, однак судова практика не відображає такої тенденції. На нашу думку, у полі зору кримінальної юстиції переважно опиняються найпростіші й найменш небезпечні форми правопорушень. Цей феномен ми визначаємо як примітивізацію правозастосування (докладніше про це йдеться

¹ Карчевський М. В., Федюк В. В. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. С. 170–183.

² Карчевський М. В., Федюк В. В. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. С. 170–183.

в розділі «ІТ та аналіз злочинності»). Ще 2012 року наш аналіз судових рішень за розділом XVI КК показав, що лише 43,71 % із них стосувалися посягань, безперечно суспільно небезпечних, тоді як більше половини (56,29%) – діянь, небезпечність яких є дискусійною¹.

Розглянемо під аналогічним кутом зору дослідження судової практики, проведене нами у 2024 році². 22% судових рішень пов'язані зі здійсненням несанкціонованих транзакцій. У такому разі несанкціоноване втручання інкримінується додатково до крадіжки або шахрайства. Не потребує аргументації теза про те, що в таких обставинах суспільна небезпечність «комп'ютерних» кримінальних правопорушень є опосередкованою та насамперед залежить від характеристики предмета відповідного посягання на власність.

23% досліджених судових рішень пов'язані зі зміною даних, що вчиняється особою, яка має право доступу до них. Вважаємо, що й ця група судових рішень характеризується опосередкованою суспільною небезпечністю. Незаконні зміни інформації в службових автоматизованих системах потребують кримінально-правового реагування не самі собою, а лише тоді, коли такі зміни заподіюють шкоду тим відносинам, для інтенсифікації яких використовується автоматизована система. Якщо працівник банківської установи вносить до АС неправдиві дані про емісію платіжної картки, небезпека його дій визначається не порушенням правил, а створенням умов для подальшого шахрайства. Такі міркування підтверджуються і тим, що серед досліджених судових рішень цієї категорії 40% містить дані про кваліфікацію за сукупністю. Крім зміни комп'ютерної інформації (ст. 362 КК), дії, наприклад, працівників банків кваліфікувалися як шахрайство (ст. 190 КК), медичних працівників, що вносили неправдиві дані про щеплення, – як підкуп працівника (ст. 354 КК) тощо³.

¹ Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. С. 221.

² Карчевський М. В. Практика протидії кримінальним правопорушенням у сфері використання інформаційних технологій. *Питання боротьби зі злочинністю*. 2024. Вип. 48. С. 116–124. DOI: <https://doi.org/10.31359/2079-6242-2024-48-116>.

³ Карчевський М. В. Практика протидії кримінальним правопорушенням у сфері використання інформаційних технологій.

19% проаналізованих судових рішень стосуються розповсюдження або збуту комп'ютерної інформації з обмеженим доступом¹. Системне тлумачення ст. 361-2 КК у взаємозв'язку з іншими нормами чинного КК, що встановлюють відповідальність за незаконні дії з інформацією з обмеженим доступом, свідчить про надмірність цієї кримінально-правової заборони. Єдиним аргументом на користь доцільності існування ст. 361-2 КК можна вважати специфічну форму відомостей – комп'ютерну інформацію. Проте сам собою цей критерій є недостатнім для обґрунтування кримінальної відповідальності: форма інформації не може бути чинником, що визначає підвищену суспільну небезпечність її розповсюдження чи збуту. Відтак випадки відповідальності за незаконні дії з комп'ютерною інформацією з обмеженим доступом (ст. 361-2 КК) також відносимо до судових рішень, пов'язаних із діями, що характеризуються спірною суспільною небезпечністю. Передача стороннім особам даних зі службових АС за умови відсутності ознак інших кримінальних правопорушень на-вряд чи потребує *ultima ratio*².

Отже, три найбільші групи досліджених судових рішень, що в сумі становлять 64% від усієї добірки, характеризуються спірною суспільною небезпечністю. Саме це, на нашу думку, є індикатором проблеми ефективності кримінально-правової протидії «комп'ютерним» кримінальним правопорушенням: *в умовах стрімкої інформатизації більше половини судових рішень стосуються випадків зі спірною суспільною небезпечністю*.

У цьому контексті не можна не звернути уваги на Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX. Закон передбачав зміни до розділу XVI. Зокрема здійснено самостійну криміналізацію несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних

¹ Карчевський М. В. Практика протидії кримінальним правопорушенням у сфері використання інформаційних технологій.

² Докладніше про це йдеться у розділі про «некомп'ютерні» посягання на інформаційну безпеку.

систем, електронних комунікаційних мереж (ч. 1 ст. 361). Дії, які раніше вважалися основним складом кримінального правопорушення, передбаченого ч. 1 ст. 361, стали його особливо кваліфікованим складом (ч. 3 ст. 361) й отримали більш сувору санкцію. В умовах установлених тенденцій примітивізації протидії «комп'ютерним» кримінальним правопорушенням наведені зміни законодавства про кримінальну відповідальність мають негативний потенціал. Вони можуть бути причиною переміщення до сфери кримінальної юстиції ще більшої кількості діянь, які характеризуються спірною суспільною небезпечністю та не потребують заходів кримінально-правового впливу.

У контексті примітивізації протидії «комп'ютерним» кримінальним правопорушенням на окрему увагу заслуговує і наступне питання: як можна пояснити, що відповідно до даних Офісу Генерального прокурора (ОГП), із 2017 до 2023 року кількість обвинувальних матеріалів, надісланих до суду за розділом XVI Особливої частини КК, зростає від 1015 до 2652, а відповідно до даних Державної судової адміністрації кількість осіб, засуджених за «комп'ютерні» злочини, у той самий період змінилася від 42 до 84¹?

Виявлена аномалія даних безсумнівно потребує самостійного дослідження, проте найбільш імовірно видається наступна гіпотеза: розбіжність даних зумовлена особливостями статистичного обліку. У випадку сукупності кримінальних правопорушень Державна судова адміністрація України (ДСА) обліковує судові рішення за найтяжчим обвинуваченням. У подібних випадках Офіс Генерального прокурора обліковує всі обвинувальні матеріали. Зважаючи на зазначене, поясненням аномалії даних може бути припущення про те, що звинувачення в незаконних діях з інформаційними технологіями зазвичай супроводжуються звинуваченнями в більш тяжких злочинах (шах-

¹ Тут і далі для роботи з даними офіційної статистики протидії злочинності нами було використано довідник «Протидія злочинності в Україні: інфографіка», що є у відкритому доступі на аналітичній платформі «CrimeDataLab» (<https://crimedatalab.org/>). Див.: Карчевський М. В. Протидія злочинності в Україні: інфографіка (2013–2024) : інтерактивний довідник, 2024. URL: <https://karchevskiy.com/i-dovidnyk/> (дата звернення: 30.08.2025). Докладніше про цей ресурс ідеться в наступному розділі.

райство, вимагання тощо). Тому в статистичних звітах Офісу Генерального прокурора відповідні обвинувальні матеріали фіксуються, а в звітах ДСА – ні.

Якщо це так, цілком слушним буде провокаційне, але лише на перший погляд, питання: «Настав час замислитися, чи існують насправді «комп'ютерні» злочини?». Якщо переважна більшість випадків супроводжується звинуваченням у вчиненні більш тяжких кримінальних правопорушень, якщо «самостійні» звинувачення характеризуються переважно звільненням від покарання та застосуванням штрафів, чи не буде правильним розглядати «комп'ютерні» кримінальні правопорушення просто як спосіб старої, добре відомої крадіжки або вимагання чи шахрайства?

Зрозуміло, що злочини у сфері використання інформаційних технологій у «чистому» вигляді існують. Це підтверджує моніторинг інцидентів кібербезпеки і в Україні, і в світі. Водночас проведене нами дослідження судової практики фіксує дисбаланс між реальними викликами інформаційної безпеки та кримінально-правовими засобами реагування. Суспільно небезпечні явища, як-от масштабні кібератаки, організовані кампанії зі зламів або масове поширення шкідливих програм, залишаються на периферії судової практики, тоді як найбільш поширеними об'єктами переслідування переважно є прості випадки неправомірного використання ІТ.

Висновки

Попри значні успіхи правоохоронних органів у сфері протидії кіберзлочинності, необхідно визнати, що ми стикаємось із ситуацією, коли значна частина судових рішень щодо протидії кримінальним правопорушенням у сфері використання інформаційних технологій (ст. 361–363-1 КК) стосується діянь, які можна розглядати як допоміжні або похідні від традиційних форм злочинності. Це зумовлює подвійний ефект: з одного боку, забезпечується «видимість» активної протидії кіберзлочинності, а з іншого, – ресурси кримінальної юсти-

ції розпорошуються на переслідування діянь, що не потребують настільки інтенсивного реагування.

Примітивізація протидії злочинним посяганням у сфері ІТ виявляється в тому, що система кримінальної юстиції концентрується переважно на формальних і менш небезпечних посяганнях, тоді як складні та справді загрозливі вияви кіберзлочинності є поза її увагою. Це свідчить про необхідність перегляду пріоритетів кримінальної політики й пошуку нових, більш ефективних моделей реагування.

Вирішення проблеми примітивізації визначає першочергові напрями розвитку кримінально-правового регулювання у сфері використання інформаційних технологій.

Через відсутність у законодавчих визначеннях чітких критеріїв суспільної небезпечності до сфери впливу кримінальної юстиції потрапляють не тільки діяння, які дійсно є суспільно небезпечними, а й ті, які такими не є. Тож обґрунтованим буде встановлення кримінальної відповідальності не просто за несанкціонований доступ або, наприклад, знищення інформації, а за заподіяння істотної шкоди тим суспільним відносинам, у межах яких використовуються інформаційні технології.

Норми розділу XVI Особливої частини КК містять терміни, які неоднаково визначаються і на рівні законодавства, і на рівні наукового тлумачення. Невиправданим видається формулювання кримінально-правових заборон на основі двох майже схожих переліків засобів технічної обробки інформації (автоматизована система, електронно-обчислювальна машина, інформаційна система тощо). Такий підхід не тільки створює небезпеку «технологічної залежності» законодавства, а й ускладнює його використання. Замість складних і неоднозначних переліків технічних засобів надалі є сенс використовувати більш широке поняття. Таким може бути поняття «комп'ютерна система», що визначається в ратифікованій Україною Конвенції про кіберзлочинність¹.

¹ Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. URL: <https://zakon.rada.gov.ua/laws/show/2824-15> (дата звернення: 21.09.2025).

Заборона, передбачена ст. 361-2 КК, є очевидно надлишковою, але більш детально це питання розглянемо в наступному розділі.

Зрештою, кримінальний закон хоч і відіграє ключову роль у протидії злочинам у сфері використання інформаційних технологій, однак сам собою він не може забезпечити комплексного вирішення проблеми. Зменшення ризиків примітивізації правозастосування потребує поєднання правових механізмів із системними освітніми заходами, спрямованими на формування у фахівців належних компетентностей у сфері кібербезпеки, віртуальних активів і права. Важливим є перегляд підходів до оцінки ефективності діяльності правоохоронних органів з акцентом не лише на кількісні, а й на якісні показники, а також розширення міжнародної співпраці у сфері кіберюстиції. Поєднання законодавчого регулювання, професійної підготовки та глобальної взаємодії здатне забезпечити адекватну відповідь на сучасні виклики кіберзлочинності.

Розділ 4

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ ПРОТИ ВЛАСНОСТІ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРІВ

Отже, широке поняття «комп'ютерні» злочини ми ділимо на дві складові: кримінальні правопорушення у сфері використання інформаційних технологій і кримінальні правопорушення, що вчиняються з використанням комп'ютерів. Перші – нова група посягань, що з'явилася через широке застосування комп'ютерної техніки (ст. 361–363-1 КК). Другі – традиційні кримінальні правопорушення, що вчиняються з використанням комп'ютерної техніки. Такий поділ є достатньо поширеним і в науковому, і в правозастосовному дискурсі.

Так, Конвенція Ради Європи про кіберзлочинність («Convention on Cybercrime», Будапештська конвенція, 2001 р.) визначає чотири основні групи кіберзлочинів:

- правопорушення проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями);
- правопорушення, пов'язані з комп'ютерами (підробка, шахрайство);
- правопорушення, пов'язані зі змістом (дитяча порнографія, до цієї групи можна віднести також дії расистського або ксенофобського характеру, передбачені Першим додатковим протоколом до Конвенції);
- правопорушення, пов'язані з порушенням авторських і суміжних прав¹.

¹ Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 21.09.2025).

Генеральна Асамблея ООН 2024 року прийняла Конвенцію ООН проти кіберзлочинності, яка містить уніфіковану класифікацію злочинів, учинюваних із використанням інформаційно-комунікаційних технологій. Згідно з розділом II цієї конвенції (ст. 7–17) передбачено криміналізацію діянь, що можуть бути класифіковані так:

- посягання на цілісність, доступність і конфіденційність комп'ютерних даних та систем (незаконний доступ, незаконне перехоплення даних, втручання в електронні дані, втручання у функціонування ІКТ-систем, шкідливі програмні або технічні засоби);
- шахрайство й підробка з використанням ІКТ;
- злочини проти дітей (обіг матеріалів сексуального насильства над дітьми в інтернеті, вербування чи грумінг дітей із метою вчинення сексуальних злочинів);
- злочини проти приватності (розповсюдження інтимних зображень без згоди);
- злочини, пов'язані з легалізацією доходів, одержаних злочинним шляхом¹.

У 2025 році оприлюднено пропозиції робочої групи Національної академії наук США щодо класифікації комп'ютерних злочинів для цілей збору статистичних даних, аналітики й удосконалення звітності в правозастосуванні. Запропоновано наступний підхід:

- дії, спрямовані проти машин, даних або систем (незаконний доступ, шкідливе ПЗ);
- шахрайство, крадіжки й інші посягання на власність;
- насильницькі дії проти особи несексуального характеру (кіберпереслідування, доксінг², сватінг³);

¹ United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes : Resolution 79/243 adopted by the United Nations General Assembly on 24 December 2024 : A/RES/79/243. URL: <https://undocs.org/en/A/RES/79/243> (дата звернення: 21.09.2025).

² Умисне збирання, розкриття та публікація в інтернеті особистої інформації про людину без її згоди з метою приниження, залякування або заподіяння шкоди (доксінг – від англ. doxing, documents).

³ Повідомлення до екстрених служб про вигадану надзвичайну ситуацію (заручники, стрілянина, вибухівка) за адресою жертви з метою спровокувати збройне втручання силових структур (сватінг – від англ. SWAT – спецпідрозділ поліції США).

- насильницькі дії проти особи сексуального характеру (дитяча порнографія, «revenge porn»¹);
- акти, спрямовані проти груп осіб (кібертероризм, мова ворожечі, масові розсилки);
- дії з побічним використанням цифрових технологій².

Наявність таких класифікацій свідчить про те, що так звані «чис-ті» комп'ютерні злочини, у нашому випадку розділ XVI Особливої частини КК, є неповним переліком змін, що відбулися в протиправній поведінці через появу інформаційних технологій. Із використанням комп'ютерної техніки вчиняється дедалі більше злочинів. Зважаючи на постійне розширення сфери її застосування, це природний процес.

Тут варто зазначити, що оновлення інструментарію злочинців не завжди вимагає внесення змін до кримінального законодавства, перегляду сталих визначень кримінальних правопорушень. Наприклад, інформаційні технології докорінно змінили незаконний збут наркотиків. Маркетплейси в даркнеті, телеграм-канали для поширення психоактивних речовин, спілкування між учасниками злочинних угруповань онлайн, «відмивання» з використанням віртуальних активів – усе це неповний перелік змін протиправного збуту наркотиків. Однак технологічне оновлення цього сегмента злочинності не викликає дискусій у сфері кримінально-правового регулювання.

Водночас із-поміж «традиційних» кримінальних правопорушень, що вчиняються з використанням комп'ютерів, є такі, які вимагають окремого аналізу в контексті кримінально-правового регулювання.

Дослідження судової практики свідчить, що випадки застосування комп'ютерної техніки для здійснення злочинів проти власності можуть бути двох видів: 1) використання комп'ютерної техніки як засобу вчинення злочину проти власності; 2) учинення злочину в сфері

¹ Незаконне розповсюдження інтимних фото або відео особи без її згоди, зазвичай з метою приниження, шантажу або помсти.

² Cybercrime Classification and Measurement : Consensus Study Report / Eds.: H. S. Stern, D. L. Cork ; National Academies of Sciences, Engineering, and Medicine. Washington, DC : The National Academies Press, 2025. XX, 140 p. DOI: <https://doi.org/10.17226/29048>.

використання комп'ютерної техніки (ст. 361–363-1 КК) для подальшого вчинення злочину проти власності або приховування його слідів.

Посягання, які слід відносити до *першої групи*, полягають у використанні інформаційної системи як засобу заволодіння чужою власністю. Наприклад, розміщення фіктивного повідомлення про продаж певних товарів і подальше заволодіння передплатою шляхом обману. Винний не здійснює незаконного перекручення або знищення комп'ютерної інформації, не завдає іншої шкоди функціонуванню комп'ютерних засобів.

Особливість кримінально-правової оцінки посягань, віднесених нами до *другої групи*, у тому, що дії винної особи треба кваліфікувати не тільки як злочин проти власності, а і як злочин у сфері використання інформаційних технологій. Наприклад, банківський працівник вносить неправдиві відомості до АС банку щодо емісії кредитної картки на ім'я певної особи, отримує цю картку, а згодом отримує кредит на згадану особу, не маючи наміру повертати його.

Проведені дослідження свідчать «про відсутність сталої судової практики щодо кримінально-правової кваліфікації шахрайства, учиненого шляхом незаконних операцій із використанням комп'ютерної техніки. Близькі за обставинами вчинення випадки заволодіння чужими цінностями шляхом обману або зловживання довірою під час продажу товарів і послуг із використанням інтернет-майданчиків отримують кримінально-правову оцінку як шахрайство, учинене шляхом незаконних операцій із використанням комп'ютерної техніки, у 67% випадків, у 33% – як звичайне шахрайство. Випадки несанкціонованих транзакцій із використанням платіжних карток або їх реквізитів у 15% випадків суди кваліфікують як шахрайство, у 85% – як крадіжку»¹.

Тож приділимо увагу двом таким питанням: 1) зміст ознак шахрайства, учиненого шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК); 2) кримінально-

¹ Усманов Р. А. Шахрайство з використанням електронно-обчислювальної техніки: аналіз судової практики. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 1. С. 159–160. DOI: <https://doi.org/10.32782/2311-8040/2024-1-19>.

правова кваліфікація несанкціонованих транзакцій безготівкових коштів.

4.1. «Комп'ютерне» шахрайство

Відправною точкою вважатимемо обґрунтовану позицію В. О. Навроцького, який зазначає, що шахрайство, учинене шляхом незаконних операцій із використанням ЕОТ (ч. 4 ст. 190 КК), належить до тих випадків, коли стаття Особливої частини передбачає незаконність учинення діянь, що входять до об'єктивної сторони відповідного злочину, водночас злочинність цих діянь «впливає не з інших нормативно-правових актів, а з самого КК, оскільки в диспозиціях використані інші терміни, які однозначно свідчать про те, що відповідне діяння завжди є кримінально караним»¹. Саме тому вказівка в диспозиції на незаконні операції є зайвою², використання в процесі шахрайства електронно-обчислюваної техніки слід завжди вважати незаконним, оскільки це прямо передбачено ст. 190 КК.

Отже, тлумачення ч. 4 ст. 190 КК свідчить про невідале, тавтологічне формулювання, що фактично означає використання засобів комп'ютерної техніки в процесі шахрайства.

Далі виникають цілком справедливі питання. Наскільки обґрунтованим є положення чинного законодавства щодо розгляду шахрайства з використанням електронно-обчислювальної техніки як тяжкого злочину (санкція ч. 4 ст. 190 передбачає покарання до 8(!) років позбавлення волі)? Чи справедливо стверджувати, що використання комп'ютерної техніки в процесі простого (за розміром заподіяної шкоди) шахрайства прирівнює його до шахрайства у великих розмірах?

На момент включення цієї норми до КК (2001 рік) застосування комп'ютерної техніки для здійснення шахрайства справді могло свідчити про підвищену суспільну небезпечність посягання. Поширеність

¹ Навроцький В. О. Наскрізнi кримінально-правові поняття : навч. посіб. Київ : Юрінком Інтер, 2023. С. 151.

² Навроцький В. О. Наскрізнi кримінально-правові поняття. С. 148.

засобів електронної комерції, систем дистанційного банківського обслуговування була незначною. Користувалися ними великі господарюючі суб'єкти. Тому положення КК доволі чітко окреслювали коло діянь, які обґрунтовано було розглядати як особливо кваліфікований вид шахрайства, близький за ступенем суспільної небезпечності до шахрайства у великих розмірах.

Проте стрімкі темпи проникнення інформаційних технологій у фінансову сферу зумовили якісну зміну цього виду шахрайства. У сучасних умовах немає підстав стверджувати, що використання електронно-обчислювальної техніки в процесі здійснення шахрайства настільки підвищує рівень суспільної небезпечності вчиненого діяння. Формалізовані в цій нормі уявлення законодавця про суспільну небезпечність шахрайства, учинюваного шляхом незаконних операцій із використанням електронно-обчислювальної техніки, не відповідають фактичному рівню відносин інформатизації. Унаслідок цього законодавча оцінка суспільної небезпечності посягань (покарання до 8 років позбавлення волі) не відповідає рівню їх фактичної суспільної небезпечності. Означена кваліфікуюча ознака шахрайства має бути скасована¹.

Водночас у разі шахрайства, «обтяженого» кримінальними правопорушеннями у сфері використання інформаційних технологій (наприклад, отримання несанкціонованого доступу до облікового запису в системі дистанційного банківського обслуговування або використання шкідливого програмного забезпечення для отримання авторизаційних даних), учинене слід кваліфікувати за сукупністю.

Повертаючись до питання про причини суперечливої судової практики, зазначимо, що вона є відображенням кримінального закону, який не відображає небезпечності передбачених діянь, є нечітким, тавтологічним.

Кримінально-правова кваліфікація несанкціонованих транзакцій безготівкових коштів. Визначимо ознаки складу кримінального право-

¹ Карчевський М. В. Особливості кваліфікації шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2014. Вип. 1. С. 272–281. URL: http://nbuv.gov.ua/UJRN/Nvlduvs_2014_1_30 (дата звернення: 21.09.2025).

порушення для випадків протиправного використання електронних платіжних систем, що полягають у так званому «списанні» безготівкових коштів із чужих розрахункових рахунків.

Об'єктом шахрайства з використанням платіжних карток або їх реквізитів є суспільні відносини щодо реалізації держателем платіжної картки права власності, обумовленого відповідними угодами банківського обслуговування. Суспільні відносини, що виникають у сфері використання платіжних систем, охоплюють взаємодію між фізичними особами, суб'єктами господарювання, банківськими установами, емітентами платіжних інструментів, еквайрами й іншими учасниками фінансової інфраструктури з метою здійснення безготівкових розрахунків.

Зміст цих відносин полягає в тому, що:

- 1) особа, яка уклала з банком договір банківського обслуговування, отримує право розпоряджатися грошовими коштами, облікованими на рахунок;
- 2) банки зобов'язані зараховувати кошти на рахунки, здійснювати перерахування згідно з інструкціями клієнтів, а також забезпечувати технічну підтримку платіжних операцій.

Такі відносини регулюються нормами Цивільного кодексу України, Законів України «Про банки і банківську діяльність», «Про платіжні послуги», іншими нормативними документами.

Ініціювання платіжних операцій та ідентифікація учасників забезпечуються технічними рішеннями щодо використання платіжних карток, мобільних застосунків, банкоматів, POS-терміналів тощо.

Можливість здійснювати операції з коштами, облікованими на банківських рахунках, забезпечується банківськими платіжними інструментами, засобами, що містять реквізити, які ідентифікують емітента, платіжну систему, у якій він використовується, та, зазвичай, держателя цього банківського платіжного інструмента¹.

Платіжним інструментом є персоналізований засіб, пристрій та/або набір процедур, що відповідають вимогам законодавства й по-

¹ Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III. URL: <https://zakon.rada.gov.ua/laws/show/2121-14> (дата звернення: 21.09.2025).

годжені користувачем і надавачем платіжних послуг для надання платіжної інструкції¹.

Електронний платіжний засіб є платіжним інструментом, реалізованим на будь-якому носії, що містить в електронній формі дані, необхідні для ініціювання платіжної операції та/або здійснення інших операцій, визначених договором з емітентом². Найбільш поширеними електронними платіжними інструментами є платіжні карти й мобільні банківські застосунки.

Безготівкові кошти існують у вигляді електронних записів. Вони не є речами в контексті понять, які використовує диспозиція ст. 190 КК, безготівкові гроші є правом на майно. Банківська діяльність є «залученням у вклади грошових коштів фізичних і юридичних осіб та розміщенням зазначених коштів від свого імені, на власних умовах та на власний ризик, відкриттям і веденням банківських рахунків фізичних та юридичних осіб»³. Відповідно, банківські рахунки – це «рахунки, на яких обліковуються власні кошти, вимоги, зобов'язання банку стосовно його клієнтів і контрагентів та які дають можливість здійснювати переказ коштів за допомогою банківських платіжних інструментів»⁴. Отже, наявність коштів на банківському рахунку з юридичного погляду означає наявність права розпоряджатися певною сумою коштів і наявність відповідного обов'язку банківської установи. Саме тому безготівкові гроші слід розглядати як предмет злочинного впливу.

Варто погодитися з Р. А. Усмановим у тому, що «безготівкові гроші як предмет злочинного впливу шахрайства являють собою права потерпілої особи вимагати від банку певної суми коштів, а також зобов'язання банку виконати цю вимогу, зменшити обсяг яких намагається винна особа»⁵. Безпосереднім об'єктом шахрайства, яке здійснюється щодо безготівкових грошей, є суспільні відносини

¹ Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20> (дата звернення: 21.09.2025).

² Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX.

³ Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III.

⁴ Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III.

⁵ Усманов Р. А. Кримінальна відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням комп'ютерної техніки : дис. ... д-ра філософії : 081. Кропивницький, 2024. С. 93.

власності, опосередковані використанням банківських рахунків та електронних платіжних систем. «Означена специфіка об'єкта посягання та предмета злочинного впливу робить необхідним встановлення в процесі досудового слідства таких даних, як: реквізити договору банківського обслуговування (на відкриття рахунку потерпілої особи), реквізити банківського рахунку потерпілої особи, реквізити договору на отримання платіжних послуг, реквізити платіжної картки потерпілої особи, дані щодо ініційованих винною особою транзакцій із рахунку потерпілої особи»¹.

Зазвичай посягання на власність із використанням платіжних карток поділяють на три групи: 1) із застосуванням справжніх карток; 2) із використанням підроблених карток; 3) із використанням лише їх реквізитів (без фізичного пред'явлення картки).

До першої групи належать злочини, учинювані за допомогою викрадених або загублених карток, а також недобросовісне використання карток, добровільно переданих законними держателями (так зване «дружнє шахрайство»). Верховний Суд України зазначав, що платіжні картки як платіжні інструменти – засоби доступу до банківських рахунків – відповідають визначенню «офіційний документ» і є його різновидом, а тому можуть бути предметом злочинів, передбачених ч. 1, 2 ст. 357 КК. Отже, викрадення платіжної картки з подальшою несанкціонованою транзакцією кваліфікується за сукупністю ст. 190, 357 КК.

Посягання із застосуванням підроблених карток означають отримання готівки або оплату товарів / послуг шляхом ініціювання платежів із карткових рахунків клієнтів, чиї картки підроблено, що потребує додаткової кваліфікації за ст. 200 КК.

Використання реквізитів карток найчастіше пов'язано з оплатою товарів і послуг в інтернеті за чужий рахунок. У таких випадках зловмисник ініціює платіж шляхом уведення реквізитів (номер, П. І. Б. держателя, строк дії тощо) на сайті платіжної системи або інтернет-магазину. Отримання реквізитів може утворювати окремий склад злочину (ст. 361, 361-1, 362 КК) у разі застосування «скімерів», зламу банківських мереж чи інсайдерського витоку даних.

¹ Усанов Р. А. Кримінальна відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням комп'ютерної техніки : дис. С. 97.

У всіх трьох випадках об'єктивна сторона характеризується спільними ознаками. По-перше, діяння полягає в тому, що, надсилаючи несанкціонований запит на платіж і використовуючи платіжну систему з автоматизованою обробкою запитів, зловмисник вводить в оману банк-емітент щодо необхідності виконання зобов'язань перед держателем картки. По-друге, наслідки полягають у тому, що через учинене діяння банк-емітент безпідставно списує безготівкові кошти з рахунку держателя, спричиняючи збитки у вигляді зменшення безготівкових коштів, облікованих на картрахунку. По-третє, ініціювання переказу (діяння) та наслідки перебувають у причинному зв'язку.

Зрозуміло, що не всі посягання у сфері використання платіжних систем і банкоматів підлягають кваліфікації як шахрайство. Маємо приклад відомої істини про те, що виключення з правила підтверджують його істинність. Відносно поширеним є заволодіння готівкою, що зберігається в банкоматі, із застосуванням спеціального пристрою («вилки») або клейкої стрічки. У професійній класифікації банківської безпеки такі випадки отримання коштів із банкоматів без ініціювання несанкціонованого платежу позначаються терміном «Cash Trapping» (від англ. *cash* – готівка, *trapping* – захоплення). Визначальною ознакою цих посягань у контексті кримінально-правової кваліфікації є відсутність несанкціонованого ініціювання платежу. Саме тому подібні випадки є крадіжкою, а не шахрайством. Водночас дії з Cash Trapping обґрунтовано додатково кваліфікують як несанкціоноване втручання в роботу автоматизованої системи. Під час функціонування банкомат зі встановленим трепінговим пристроєм формує код помилки роботи, що становить «несанкціоноване втручання в роботу АС, яке призвело до спотворення процесу обробки інформації» (ст. 361 КК).

4.2. Кримінальні правопорушення щодо віртуальних активів

У сфері обігу криптовалют виникає особливий тип суспільних відносин. За своєю структурою та функціонуванням вони суттєво

відрізняються від традиційних фінансових відносин. Основна відмінність полягає в децентралізованому характері взаємодії між учасниками, що усуває необхідність існування центрального посередника, такого, як банк чи інша фінансова установа.

До основних учасників правовідносин, що виникають під час здійснення транзакцій із криптовалютами, належать:

1) особа, яка передає актив (відправник) – власник віртуального активу, що ініціює його передачу іншій особі; така особа створює транзакцію, підписує її своїм приватним ключем і надсилає в мережу для підтвердження;

2) особа, яка отримує актив (одержувач) – суб'єкт, на адресу якого передається віртуальний актив; отримання відбувається шляхом фіксації в розподіленому реєстрі запису про транзакцію (блокчейн криптовалюти);

3) «майнери» (або валідатори) – учасники мережі, які забезпечують перевірку й підтвердження транзакцій, формування нових блоків у блокчейні та підтримання цілісності реєстру.

Усі зазначені суб'єкти діють, використовуючи єдину розподілену систему, де немає органу, який централізовано керує, санкціонує або блокує операції. Технічно ця система існує у вигляді мережі серверів («вузлів»), яку підтримують «майнери» і яка функціонує на основі програмного забезпечення з відкритим кодом.

Як зазначалося, відносини щодо реалізації права власності на віртуальні активи є децентралізованими. Цю ознаку можна пояснити шляхом порівняння з відносинами в централізованій банківській системі. Так, інформація про банківські рахунки і транзакції зберігається на серверах банку, контроль, перевірка й підтвердження операцій здійснюються вповноваженими працівниками, без санкції банку клієнт не може виконати жодної операції, можливим є обмеження операцій із боку регуляторів.

Натомість децентралізовані відносини у сфері використання криптовалюти характеризуються: відсутністю єдиного центру зберігання даних – синхронізовані копії реєстру транзакцій зберігає кожен «вузол» мережі; автоматизованим здійсненням підтвердження операцій за допомогою алгоритмів консенсусу; безпосередньою взаємоді-

єю учасників, коли функції перевірки й фіксації операцій виконує кожен «вузол», який автоматизовано «узгоджує» результати власної перевірки транзакцій з іншими «вузлами» децентралізованої мережі.

Тобто відносини між учасниками обігу криптовалюти за своєю природою є горизонтальними, на відміну від вертикально підпорядкованих централізованих відносин у банківській сфері.

Технологічним фундаментом таких відносин є блокчейн – розподілений реєстр транзакцій, який зберігається у вигляді синхронізованих копій та актуалізується мережею «вузлів». Процес його формування відбувається в кілька етапів:

- 1) ініціювання транзакції – відправник створює транзакцію, підписує її своїм приватним ключем і надсилає до мережі «вузлів»;
- 2) перевірка ініційованої транзакції «вузлами» мережі – транзакція поширюється серед учасників мережі, які перевіряють її коректність;
- 3) формування нового блоку – майнери збирають визнані коректними транзакції в новий блок;
- 4) додавання до нового блоку блокчейну – за допомогою алгоритму консенсусу сформований новий блок визнається як підтверджений і додається до реєстру транзакцій (блокчейну) як наступний.

Також важливою ознакою відносин у сфері реалізації права власності на віртуальні активи слід визнати технологічний характер довіри. Традиційні відносини власності гарантуються переважно організаційними та правовими засобами. Довіра до цих відносин підтримується існуванням законів, правоохоронних і судових органів, наявністю фізичної інфраструктури (відділення банків, офісів компаній) тощо. Надійність відносин у сфері використання віртуальних активів ґрунтується на використанні криптографічних алгоритмів. Асиметричне шифрування забезпечує створення пари ключів (публічного та приватного), де публічний ключ використовується як адреса для отримання активів, а приватний – для підтвердження транзакцій. Криптографічні хеш-функції забезпечують унікальну ідентифікацію кожної транзакції, кожного блоку та зв'язок між блоками в блокчейні. Автоматизовані механізми консенсусу гарантують, що додавання

нового блоку потребує значних обчислювальних витрат, що внаслідок цього викликає масові фальсифікації.

Як предмет кримінального правопорушення віртуальні активи характеризуються фізичною, соціальною та юридичною ознаками.

Фізична ознака полягає в тому, що криптовалюта є інформацією про стан певної публічної адреси платіжної системи, яка додана до реєстру транзакцій за допомогою криптографічних методів і розподілено зберігається в достатній кількості учасників системи («майнерів»).

Економічну ознаку криптовалюти визначає ціна, яку за неї можуть заплатити зацікавлені особи. Ключова позиція тут полягає в тому, що вартість криптовалюти нічим не забезпечена й визначається ситуативно на підставі попиту та пропозиції; єдиного органу, що встановлює курс до національних валют, немає. Проте властивості криптовалюти (захищеність, конфіденційність, децентралізація, майже миттєвий переказ у будь-яку частину світу) забезпечують стабільний попит на неї. Приклади визначення ціни на криптовалюту можна побачити на таких майданчиках, як «Bitfinex», «Bitstamp», «Coinbase». Типовий підхід до визначення ціни криптовалюти полягає в тому, що вона дорівнює ціні останньої за часом біржової операції. Також ціна криптовалюти може обчислюватися як середнє арифметичне операцій, проведених за певний період на одному або кількох майданчиках (наприклад, «Bitcoin Liquid Index»¹).

Юридична ознака. Національна специфіка протидії злочинному використанню віртуальних активів полягає в тому, що незавершене правове регулювання використання віртуальних активів супроводжується фактичним використанням віртуальних активів для вчинення кримінальних правопорушень. Прийнято Закон України «Про віртуальні активи», але відповідно до перехідних положень він набере чинності після внесення змін до Податкового кодексу. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» визначає поняття

¹ Brave New Coin : вебсайт. URL: <https://bravenewcoin.com> (дата звернення: 21.09.2025).

«віртуальний актив». Відповідно до цього закону віртуальні активи є «цифровим вираженням вартості, яким можна торгувати у цифровому форматі або переказувати, і яке може бути використаним для платіжних або інвестиційних цілей». Нарешті 10 серпня 2023 р. Законом № 3320-IX Цивільний кодекс України доповнено ст. 179-1, яка визначає поняття «цифрова річ» і відносить до таких об'єктів права, зокрема, віртуальні активи.

З урахуванням указанного, несанкціонована транзакція криптовалюти через, наприклад, компрометацію приватного ключа, є шахрайством. Лінія аргументація тут подібна до аналогічних посягань щодо безготівкових грошей. Варто погодитися з Р. А. Усмановим, що в таких випадках:

1) безпосереднім об'єктом посягання будуть суспільні відносини власності, що опосередковуються функціонуванням платіжних систем віртуальних активів;

2) предметом злочинного впливу є віртуальні активи, нематеріальні блага, які належать потерпілій особі на праві власності, мають визначену вартість і виражені у вигляді сукупності даних в електронній формі;

3) специфіка об'єкта посягання та предмета злочинного впливу зумовлює необхідність установлювати під час досудового розслідування:

- публічні адреси потерпілої та винної осіб;
- реквізити транзакцій (геш, дата й час, входи, виходи, розмір комісії, номер блоку), за якими потерпіла особа отримала віртуальний актив;
- реквізити транзакцій, ініційованих винною особою;

4) особливості об'єктивної сторони полягають у наявності опосередкованого обману учасників відповідної платіжної системи; винна особа транслює в систему забезпечення функціонування віртуальних активів (мережу «вузлів», *М. К.*) неправдиві відомості про те, що нібито власник віртуального активу ініціює його передачу; через цей обман децентралізована платіжна система віртуальних активів (мережа вузлів) вносить інформацію про ініційовану винним транзакцію до реєстру (блокчейну); унаслідок цієї несанкціонованої транзакції

кількість віртуального активу, що належить потерпілому, зменшується, що й становить заподіяну шкоду¹.

Утім, шахрайство не єдине кримінальне правопорушення, яке може бути вчинене з використанням віртуальних активів. Поява технологій розподіленого зберігання даних (блокчейн) й основаних на таких технологіях криптовалютних платіжних систем істотно змінює процес протидії злочинності. Трансформуються форми корупції, з'являються нові види неправомірної вигоди, оновлюються методи легалізації злочинних доходів, принципово змінюється фінансова складова незаконного обігу наркотиків, зброї тощо. Водночас як будь-який соціальний процес розширення сфери використання криптовалют має діалектичні наслідки. З одного боку, віртуальні активи стали новим інструментом злочинців. З іншого, – наявність у відкритому доступі всієї бази даних транзакцій дає правоохоронцям принципово нові інструменти боротьби зі злочинністю².

За даними «The 2025 Crypto Crime Report від Chainalysis», у 2024 році криптовалюти були інструментом різноманітних кримінальних правопорушень. Важливо зазначити, як «Chainalysis» та подібні аналітичні організації розробляють звіти про злочинне використання віртуальних активів. Зважаючи на те, що блокчейни більшості криптовалют перебувають у відкритому доступі, дослідники збирають дані про публічні адреси, задіяні в злочинній діяльності, та здійснюють моніторинг потоку транзакцій через них. Наприклад, злочинці вимагають віртуальні активи шляхом використання шкідливого програмного забезпечення, що шифрує дані потерпілих. Вони повідомляють публічну адресу для отримання винагороди за розблокування даних. Ця адреса маркується як така, що використовується в криптозлочинах, пов'язаних із використанням шкідливого програмного забезпечення. Сума транзакцій, що проходить через неї, додається до відповідного сегмента кримінально-протиправних транзакцій.

¹ Усманов Р. А. Кримінальна відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням комп'ютерної техніки : дис. С. 137–163.

² Sedgwick K. Bitcoin is Great for Criminals. It's Even Better for Law Enforcement. *Bitcoin.com*. 2018, July 16. URL: <https://news.bitcoin.com/bitcoin-is-great-for-criminals-its-even-better-for-law-enforcement/> (дата звернення: 21.09.2025).

Використовуючи таку методологію, встановлено, що в 2024 році загальний обсяг криптовалюти, отриманої злочинним шляхом, становив щонайменше 40,9 млрд USD. Найбільш поширені види кримінозлочинності:

- несанкціоновані транзакції (компрометація приватних ключів, атаки на DeFi й централізовані сервіси; 2,2 млрд USD, 5,4%);
- традиційне шахрайство (інвестиційні афери, фішинг, у т. ч. з персоналізацією сценаріїв на основі оцінки потерпілих осіб із використанням ШІ; 9,9 млрд USD, 24,2%);
- шкідливе програмне забезпечення (розвиток адаптивних методів вимагання; 0,81 млрд USD, 2%);
- даркмаркети (торгівля наркотиками, психотропними речовинами; 2,0 млрд USD, 4,9%);
- порушення санкцій (використання стейблкоїнів для обходу обмежень, відмивання коштів, фінансування незаконних операцій)¹.

Національний вимір проблеми злочинного використання віртуальних активів ми досліджували в спосіб формулювання запитів до Єдиного державного реєстру судових рішень (ЄДРСР) із подальшим аналізом отриманих обвинувальних вироків. За нашими оцінками, станом на вересень 2021 року в ЄДРСР обліковано 52 обвинувальні вирoki, що стосувалися використання криптовалюти. 36 – використання криптовалюти для незаконного обігу наркотиків; 15 – «комп'ютерні» злочини, розповсюдження шкідливого програмного забезпечення для прихованого майнінгу криптовалюти, продаж даних; 1 – шахрайство.

У лютому 2023 року реєстр містив 100 обвинувальних вироків. 59 – пов'язані з функціонуванням онлайн-мереж розповсюдження наркотиків (28 – «end users»); 19 – «комп'ютерні» злочини; 9 – посягання на власність; 5 – підробка документів; по 2 – незаконний обіг електронних грошей, збут порнографічних матеріалів; по 1 – злочини проти національної безпеки, легалізація доходів, незаконний обіг зброї, службовий злочин.

¹ The 2025 Crypto Crime Report. *Chainalysis*. 2025, February. URL: <https://www.chainalysis.com/crypto-crime-2025-report> (дата звернення: 25.08.2025).

Аналогічний моніторинг ми провели й у серпні 2025 року. Реєстр містив 214 судових рішень. 88 (41,1%) – незаконний обіг наркотиків; 32 (15%) – посягання на власність; 33 (15,4%) – правопорушення у сфері використання ІТ (ст. 361–362 КК), 25 (11,7%) – національна безпека; 14 (6,5%) – у сфері господарської діяльності (переважно ст. 200 та 209 КК); 15 (7%) – громадська безпека (переважно ст. 301 КК).

Очевидно, що така кількість судових рішень є вкрай незначною і сама собою не може свідчити про значний рівень використання криптовалют злочинцями в Україні. Водночас очевидною є тенденція розширення злочинного використання віртуальних активів в Україні. Можна зазначити, що відбуваються зміни і кількісні – збільшення випадків злочинного використання віртуальних активів, і якісні – збільшення видів злочинного використання віртуальних активів.

У таких умовах необхідно зауважити на системні недоліки чинного законодавства.

По-перше, фрагментарність і неповнота національного правового регулювання використання віртуальних активів суттєво обмежує можливості розслідування. Насамперед це стосується визначення вартості віртуального активу для цілей кримінальних проваджень. Наприклад, особа вимагає певну суму в Bitcoin. Як установити ознаки предмета посягання? Чи можна розглядати відомості інтернет-джерел щодо курсу Bitcoin як достатній доказ для встановлення економічної ознаки відповідного предмета? На сьогодні чіткої відповіді на ці запитання немає.

По-друге, є певний вакуум щодо визначеності дій правоохоронців у разі вилучення віртуальних активів, збереження після вилучення тощо. Доцільно розробити порядок (настанову, інструкцію), у якому передбачити тактичні аспекти фіксації з використанням комплексу НС(Р)Д й алгоритм дій щодо вилучення криптовалют та її збереження до прийняття рішення у справі. Є сенс уведення в правоохоронних органах посад розпорядників віртуальних активів (вилучених, арештованих). Адже сьогодні факти вчинення злочинів із використанням криптовалют не отримують належного реагування через відсутність організаційно-технічного забезпечення вказаного процесу. Зокрема навіть у разі фіксації операції з криптовалютою під час учинення зло-

чину та її документального підтвердження технічно немає змоги вилучення криптовалюти та блокування електронного гаманця. Єдиним виходом у цій ситуації є створення окремого електронного гаманця, розпорядником якого буде правоохоронний орган в особі окремого співробітника й на якому зберігатиметься вилучена криптовалюта до відповідного рішення у справі. Власне, вилучення криптовалюти пропонується організовувати як транзакцію на електронний гаманець, що контролюється правоохоронними органами.

Тут зазначимо, що ми говоримо про «класичне» децентралізоване використання віртуальних активів. Водночас на практиці важливу роль відіграють і централізовані послуги, що функціонують як надбудови над децентралізованими мережами, наприклад, криптовалютні біржі «Binance», «Bitfinex» тощо. Такі суб'єкти на відміну від децентралізованої інфраструктури мають організаційно-правову форму, персоніфікують користувачів (вимагаючи, зокрема, проходження процедур ідентифікації та верифікації), здійснюють контроль за проведенням транзакцій, можуть їх блокувати й заморожувати активи за вимогою регуляторів чи правоохоронних органів. Фактично вони діють у межах звичайних юрисдикцій і підпорядковуються національному законодавству країн, де зареєстровані або надають послуги, що істотно впливає і на правовий статус таких операцій, і на можливості правоохоронців щодо їх контролю.

Дослідження показують, що централізовані біржі (CEX)¹ і децентралізовані (DEX)² платформи суттєво відрізняються за структурою довіри й регуляторним контекстом: DEX забезпечують децентралізований контроль і стійкість до цензури, тоді як CEX пропонують вищу ліквідність, зручність користування та інфраструктурну підтримку, але водночас підпадають під регуляторний нагляд³ і зобов'язані ви-

¹ CEX (Centralized Exchange, централізована біржа) – платформа для купівлі, продажу й обміну криптовалют, яка має централізоване управління і контролюється конкретною юридичною особою. Приклади: Binance, Bitfinex.

² DEX (Decentralized Exchange, децентралізована біржа) – платформа для обміну криптовалютою, яка працює без централізованого посередника, транзакції виконуються напряму між користувачами (peer-to-peer). Приклади: Uniswap, SushiSwap, PancakeSwap.

³ Hägele S. Centralized exchanges vs. decentralized exchanges in cryptocurrency

конувати вимоги KYC та AML¹. На відміну від традиційного децентралізованого підходу СЕХ створюють нову форму «неособистої довіри», коли користувачі змушені покладатися на юридичну особу з централізованим управлінням, що є принципово відмінним від взаємодії в межах відкритого блокчейну².

Як можна побачити, криміногенний вплив появи й розширення сфери застосування віртуальних активів розглядається нами як такий, що меншою мірою потребує змін кримінального законодавства, але актуалізує завдання правового регулювання обігу віртуальних активів.

Також варто розглянути й міжнародні ініціативи. Важливим елементом міжнародного регуляторного середовища є Регламент Європейського Союзу «Про ринки криптоактивів» («Markets in Crypto-Assets Regulation», MiCA), ухвалений 20 квітня 2023 року. Цей нормативний акт установлює єдині правила для емітентів криптоактивів і постачальників послуг, пов'язаних із ними, у межах усіх держав-членів ЄС. Регламент стосується ліцензування постачальників послуг («Crypto-asset service providers», CASPs), регулювання централізованих послуг, захисту споживачів тощо. Для України значення MiCA полягає ще й у тому, що його імплементація в національне законодавство забезпечить гармонізацію з правом ЄС, сприятиме правовій визначеності у сфері протидії злочинному використанню віртуальних активів³.

Окремої уваги заслуговує щорічна конференція Робочої групи з протидії злочинному використанню фінансів і криптовалют, яка

markets: A systematic literature review. *Electron Markets*. 2024. Vol. 34. Art. 33. 22 p. DOI: <https://doi.org/10.1007/s12525-024-00714-2>; Zhou Z., Shen B. Toward understanding the use of centralized exchanges for decentralized cryptocurrency. *arXiv*. 2022. DOI: <https://doi.org/10.48550/arXiv.2204.08664>.

¹ KYC і AML – це два ключові регуляторні стандарти, яким зобов'язані підпорядковуватися централізовані фінансові та криптовалютні сервіси. KYC (Know Your Customer – «Знай свого клієнта») – процедура ідентифікації та верифікації особи клієнта перед наданням фінансових послуг. AML (Anti-Money Laundering – «Протидія відмиванню коштів»).

² Vidal-Tomás D. Centralised exchanges & proof-of-solvency: The guardians of trust. *SSRN*. 2024, February 15. 49 p. DOI: <https://doi.org/10.2139/ssrn.4761565>.

³ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj> (дата звернення: 21.09.2025).

є тристоронньою ініціативою Базельського інституту урядування, Інтерполу та Європолу¹. Рекомендації цих конференцій є зрізом найбільш актуальних проблем протидії злочинному використанню віртуальних активів і безсумнівно є важливими для побудови відповідної системи в Україні.

Так, рекомендації конференції 2021 року² фокусуються на таких аспектах організації протидії злочинному використанню віртуальних активів:

1. Міжнародне співробітництво. Усвідомлюючи гіперглобальність індустрії віртуальних активів, відзначається необхідність прискорення обміну інформацією між правоохоронними органами, важливість обміну ресурсами, новими розробками, призначеними для розслідування фактів злочинного використання віртуальних активів.

2. Викриття віртуальних активів. Брак правового регулювання віртуальних активів призводить до втрати національними правоохоронними органами змоги протидіяти «криптозлочинності», виявляти незаконні фінансові потоки. Оскільки кількість незаконних активів, які зберігаються у вигляді криптовалют, зростає, то ця неспроможність ставатиме дедалі більшою перешкодою для зусиль країн у боротьбі з фінансовими злочинами.

3. Державно-приватне партнерство. Необхідність довіри й ефективних механізмів співпраці між державним і приватним секторами для боротьби з відмиванням грошей у вигляді віртуальних активів.

4. Необхідність міжнародної гармонізації нормативного регулювання віртуальних активів.

5. Важливість постійного вдосконалення діяльності правоохоронців, їх технічної оснащеності, актуалізації професійних знань і навичок.

Окрім підтвердження значення державно-приватного партнерства й розвитку можливостей правоохоронних органів протидіяти зло-

¹ 7th Global Conference on Criminal Finances and Cryptocurrencies. *Basel Institute on Governance*. URL: <https://baselgovernance.org/node/2446> (дата звернення: 21.09.2025).

² Combating virtual assets-based money laundering and crypto-enabled crime: 2021 Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies / Basel Institute on Governance ; Interpol ; Europol. *Basel Institute on Governance*. URL: <https://baselgovernance.org/publications/combating-virtual-assets-based-money-laundering-and-crypto-enabled-crime> (дата звернення: 21.09.2025).

чинному використанню віртуальних активів, рекомендації конференції 2022 року¹ починаються з положення про те, що необхідно усунути бар'єри між традиційною та «криптозлочинністю». Йдеться про те, що подальше проникнення віртуальних активів до сфер, де зазвичай використовувалися традиційні фінанси, властиве й звичайній злочинній діяльності, зокрема відмиванню коштів. Тому пропонується обмежити практику створення спеціалізованих підрозділів правоохоронних органів як неефективну. Як більш раціональний підхід розглядається включення фахівців зі знаннями у сфері віртуальних активів до підрозділів, які здійснюють протидію традиційній злочинності.

Уважаємо такі пропозиції обґрунтованими при розробці нового законодавства про злочини проти власності або перегляді наявних законів, є сенс не виокремлювати криптовалюти, а використовувати достатньо широкі формулювання, щоб охоплювати і віртуальні активи, і можливі майбутні зміни криптоіндустрії. Такий підхід забезпечить подолання давно відомої проблеми «хронічного відставання кримінального законодавства», проблеми невідповідності законодавства формам і способам злочинної діяльності у сфері використання технологій.

Висновки

Дослідження судової практики демонструє, що межа між «звичайним» шахрайством і шахрайством із використанням електронно-обчислювальної техніки є розмитою. Це спричиняє несталість підходів до кваліфікації: одні й ті самі діяння можуть оцінюватися судами по-різному – як шахрайство, крадіжка або шахрайство, вчинене

¹ Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering: 2022 Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies / Basel Institute on Governance ; Europol. *Basel Institute on Governance*. URL: <https://baselgovernance.org/publications/seizing-opportunity-5-recommendations-crypto-assets-related-crime-and-money-laundering> (дата звернення: 21.09.2025).

шляхом незаконних операцій із використанням ЕОТ. Конструкція ч. 4 ст. 190 КК потребує критичного переосмислення: її тавтологічність і завищений рівень суворості покарання не відповідають сучасним реаліям інформатизації.

Поширені випадки несанкціонованих транзакцій із використанням електронних платіжних систем є шахрайством. Безготівкові гроші – право на майно. Повідомлення через платіжну систему неправдивої інформації про ініціювання платежу – обман.

Поява й поширення віртуальних активів створює нові виклики. Національне законодавство є фрагментарним, не забезпечує ефективної нормативної бази для протидії злочинному використанню криптовалют. Міжнародна спільнота (Регламент ЄС МіСА, рекомендації міжнародних робочих груп) прямує до гармонізації. Результати аналізу національної судової практики свідчать про поступове зростання кількості й різноманітності злочинів із використанням криптовалют. Хоча загальний масштаб наразі невеликий, простежується чітка тенденція до зростання і кількісних, і якісних характеристик таких посягань. Це вимагає розробки процедур щодо виявлення, вилучення та збереження віртуальних активів у межах кримінального провадження.

Отже, «комп'ютерні» злочини проти власності виявляють складну діалектику взаємодії між традиційними інститутами кримінального права й новітніми технологіями. Не кожна технологічна інновація потребує створення нового складу злочину, проте окремі сфери – зокрема шахрайство з використанням ІТ та злочини, пов'язані з віртуальними активами – потребують глибшого осмислення та корекції правових підходів. Подолання «хронічного відставання кримінального законодавства» має відбуватися не шляхом нескінченного множення норм, а завдяки використанню універсальних категорій, здатних охоплювати і сучасні, і майбутні технологічні форми протиправної поведінки.

Розділ 5

«НЕКОМП'ЮТЕРНІ» ПОСЯГАННЯ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

Кримінально-правова охорона інформаційної безпеки не обмежується лише «комп'ютерними» злочинами, що безпосередньо пов'язані з використанням інформаційних технологій. Вона охоплює ширше коло посягань, до яких належать посягання у сфері обмеженого доступу до інформації та правопорушення, що впливають на формування інформаційного простору. Перші характеризуються надмірною фрагментацією кримінально-правових заборон. Другі стосуються спроб кримінально-правового законодавчого реагування на загрози дезінформації, маніпулятивних впливів і гібридних інформаційних операцій.

5.1. Порухення обмеженого доступу до інформації

Ключова проблема кримінально-правової охорони відносин інформаційної безпеки у *сфері забезпечення доступу до інформації* полягає в надмірній кількості заборон.

Інформація з обмеженим доступом є предметом значної кількості різноманітних кримінальних правопорушень: державна зрада (ст. 111); шпигунство (ст. 114); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунodefіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132); незаконне розголошення лікарської таємниці (ст. 145); порушення таємниці голосування (ст. 159); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); розголошення таємниці усиновлення (удочеріння) (ст. 168); порушення недоторканності при-

ватного життя (ст. 182); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231); розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу й організованих товарних ринках (ст. 232); незаконне використання інсайдерської інформації (ст. 233); розголошення державної таємниці (ст. 328); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2) КК тощо.

Показовою буде спроба визначити випадки, коли відповідальність може наставати за ст. 361-2 КК:

1) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає державну таємницю, здійснює особа, якій ці відомості довірені не були й це не пов'язано з передачею її іноземній державі, іноземній організації або їх представникам;

2) коли розповсюдження або збут комп'ютерної інформації, зміст якої складають: відомості про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби; лікарська таємниця; комерційна, банківська таємниця, професійна таємниця на ринках капіталу й організованих товарних ринках; відомості про заходи безпеки щодо особи, взятої під захист; дані оперативно-розшукової діяльності досудового слідства чи дізнання, – здійснює особа, якій ці відомості довірені не були, тобто вона не мала спеціальних зобов'язань щодо збереження їх у таємниці;

3) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає лікарську, комерційну, банківську таємницю, професійну таємницю на ринках капіталу й організованих товарних ринках здійснює особа, якій вони були довірені, але наслідків, зазначених у ст. 145 чи 232, не настало;

4) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складає таємницю усиновлення (ст. 168) або приватного життя (ст. 182), але до умислу суб'єкта не включається усвідомлення та бажання чи свідоме допущення заподіяння шкоди

конкретній особі або чітко визначеній групі осіб, тобто відсутні ознаки складу злочину проти конституційних прав і свобод;

5) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складають відомості з обмеженим доступом інших видів.

Щоб не перевантажувати запропоновану схему, «за дужки» ми внесли такі ознаки комп'ютерної інформації, предмета кримінального правопорушення, передбаченого ст. 361-2 КК, як «створена та захищена відповідно до чинного законодавства». Однак видається, що й без цього запропонований перелік випадків, коли можливим є застосування ст. 361-2 КК, яскраво демонструє очевидну надлишковість кримінально-правової заборони, передбаченої досліджуваною нормою. Дійсно, крім випадків шпигунства, не можна погодитися з тим, що слід уважати злочином розповсюдження відомостей, які складають певну таємницю, вчинене особою, якій вони не були довірені. Ситуація з відповідальністю за порушення лікарської, комерційної або банківської таємниці є ще більш наочною. Чи обґрунтовано вважати певні дії кримінальним правопорушенням, коли наслідки, що зумовлюють кримінальну відповідальність за них, не настали? Єдиним аргументом, який може бути використаний для обґрунтування доцільності такої відповідальності, можна вважати лише те, що кримінальна відповідальність обумовлена формою цих відомостей, тим, що вони є комп'ютерною інформацією. Однак окрім того, що він спірний, цього аргументу явно недостатньо для обґрунтування кримінальної відповідальності за подібні дії. Форма інформації в жодному разі не може обґрунтовувати підвищену суспільну небезпечність її розповсюдження або збуту.

Існування такої кількості окремих норм для різних видів інформації з обмеженим доступом є невиправданим, таким, що потребує оптимізації. Способом вирішення цієї проблеми може бути заміна наявних у КК спеціальних заборон однією загальною. Інтенсивність покарання в цьому разі доцільно визначати не за видом інформації з обмеженим доступом, а за спричиненою шкодою. Наприклад, цілком очевидно, що шкода навіть від розголошення відомостей, що становлять державну таємницю, не завжди є значно більшою, ніж шкода від розголошення таємниці усяновлення або удочеріння.

5.2. Кримінально-правова охорона формування інформаційного простору

Фотограф К. Адельман 2003 року проводив звичайну роботу щодо візуального аналізу ерозії узбережжя Каліфорнії. У межах проєкту «California Coastal Records Project» він зробив понад 12 тис. аерофотографій берегової лінії, призначених для наукових і природоохоронних цілей. Серед цих тисяч зображень був один кадр, що випадково зафіксував приватний маєток американської акторки та співачки Барбари Стрейзанд у Малібу¹. Саме цей знімок став підставою для судового позову, який назавжди ввійшов в історію.

Б. Стрейзанд вимагала видалення фотографії з сайту й компенсацію в розмірі 10 млн доларів, стверджуючи, що оприлюднення зображення порушує її право на приватність. До подачі позову фото завантажили лише шість разів, причому двічі це зробили її адвокати. Після судового розголосу знімок набув небувалої популярності – його переглянули сотні тисяч, а згодом і мільйони людей у світі. Суд визнав позов безпідставним, а Б. Стрейзанд зобов'язали відшкодувати адвокатські витрати К. Адельмана на суму понад 155 тис. доларів США².

Цей випадок демонструє неоднозначність спроб правовими чи адміністративними методами заборонити поширення інформації. Заборона може перетворити малопомітний контент на всесвітньовідомий. У науковій літературі цей феномен назвали «ефект Стрейзанд».

Основне питання кримінально-правової охорони відносин інформаційної безпеки у *сфері формування інформаційного ресурсу* полягає в чіткому й послідовному визначенні межі можливостей ефективного впливу кримінального права. Небезпеки інформаційних впливів

¹ Weiss K. R. Barbra Streisand sues to keep Malibu home photos off web site. *Los Angeles Times*. 2003, May 30. URL: <https://www.latimes.com/archives/la-xpm-2003-may-30-me-barbra30-story.html> (дата звернення: 25.08.2025).

² Masnick M. Twenty years ago today: Barbra Streisand sued a photographer, and the Streisand effect was born. *Techdirt*. 2023, May 20. URL: <https://www.techdirt.com/2023/05/20/twenty-years-ago-today-barbra-streisand-sued-a-photographer-and-the-streisand-effect-was-born> (дата звернення: 25.08.2025).

і зловживань обговорюються доволі широко. Багатомірність і масштабність шкоди від неконтрольованого інформаційного простору є безсумнівною. Водночас вирішення означених проблем шляхом доповнення КК новими нормами навряд чи є доцільним. Неодноразово пропонувалося встановлювати покарання за різноманітні форми маніпуляції суспільною свідомістю¹. Такі пропозиції є спірними через прогнозовану неефективність і декларативність, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації. Крім того, поширення глобальних інформаційних технологій узагалі робить методи обмеження або заборони контенту менш ефективними². Вирішення проблеми є поза межами кримінально-правового регулювання і, на нашу думку, передбачає насамперед системну роботу в системі освіти й формування конкурентних інформаційних продуктів.

Саме така позиція переважає в міжнародному юридичному дискурсі. У спільній декларації Спеціальних доповідачів ООН з питань свободи думки та вираження, Організації американських держав з питань свободи вираження, Африканської комісії з прав людини та народів з питань свободи вираження і доступу до інформації та Представника ОБСЄ з питань свободи ЗМІ від 30 квітня 2020 року під назвою «Joint declaration on freedom of expression and elections in the digital age» зазначається, що держави повинні підтримувати позитивні заходи боротьби з онлайн-дезінформацією, такі як незалежний фактчекінг та інформаційні кампанії для суспільства, а також уникати ухвалення норм, що криміналізують дезінформацію³.

¹ Див.: Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія. Київ : ДКС, 2012. 340 с.

² Див., наприклад: Кушнір І. П., Адамчук С. В. Протидія дезінформації: організаційно-правовий аспект. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 470–475. DOI: <https://doi.org/10.24144/2788-6018.2025.01.78>.

³ Joint declaration [of the United Nations Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression] on freedom of expression and elections in the digital age. 2020, 30 April. URL: https://www.ohchr.org/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf (дата звернення: 21.09.2025).

Центром міжнародної медіадопомоги (СІМА) проаналізовано 105 законів, ухвалених у 78 країнах у 2011–2022 рр., спрямованих на боротьбу з дезінформацією, маніпулятивною та неправдивою інформацією (MDM). Застосування таких заходів має тенденцію обмежувати свободу преси та стимулювати самоцензуру журналістів. Відомо, що станом на 2022 рік приблизно 10% усіх ув'язнених журналістів у світі перебували в місцях несвободи саме за «поширення фейків». Водночас фіксується відсутність чітких визначень «неправдивої інформації» чи «фейкових новин», що створює умови для довільного трактування й переслідування незалежних медіа. Звіт підкреслює, що не всі регуляторні заходи є небезпечними. Позитивним вважається розвиток медіаграмотності, прозорості онлайн-платформ і механізмів саморегуляції ЗМІ. Водночас саме криміналізація поширення неправдивої інформації становить найбільші ризики, оскільки легітимізує практики цензури й використовується як інструмент цифрового авторитаризму навіть у демократичних країнах¹.

У означеному контексті неможливо не звернути уваги на доповнення КК новими заборонами у 2022 році. Усвідомлення небезпек гібридної агресії рф зумовило доповнення КК (березень 2022 року) ст. 436-2, яка передбачає відповідальність за виправдовування, визнання правомірною, заперечення збройної агресії російської федерації проти України, глорифікацію її учасників.

Відповідно до пояснювальної записки мета доповнення КК ст. 436-2 визначалася як протидія засобами кримінально-правового впливу ворожим інформаційним впливам в умовах триваючої гібридної війни рф з Україною. Прогноз соціально-економічних та інших результатів прийняття проекту передбачав посилення ефективної протидії гібридній інформаційній війні, що її веде держава-агресор проти України, захист державного суверенітету й територіальної ці-

¹ Lim G., Bradshaw S. Chilling legislation: Tracking the impact of «fake news» laws on press freedom internationally. *Center for International Media Assistance*. 2023, July 23. URL: <https://www.cima.ned.org/publication/chilling-legislation> (дата звернення: 21.09.2025).

лісності України, зміцнення патріотичних настроїв у ЗСУ та загалом в українському суспільстві¹.

З-поміж приблизно 1 тис. засуджених за глорифікацію дій агресора (ст. 436-2 КК): 42% учинили злочин у віці від 50 до 65 років, 30% – у віці понад 65 років; 39% жінок; 81% звільнено від покарання.

Серед усіх засуджених: частка засуджених за вчинення правопорушення у віці від 50 до 65 років перебуває в межах 9–13%, 65 – у межах 1–2%(!); частка жінок дорівнює приблизно 12%; частка звільнених від покарання від 36 до 44%.

Цілком очевидно, що притягнення до відповідальності літніх людей, серед яких значною є частка жінок, для того, щоб 80% засуджених звільнити від покарання, не може розглядатися як ефективна відповідь гібридній агресії в інформаційному просторі².

Наведені дані промовисто свідчать, що задекларовані цілі доповнення КК ст. 436-2 не досягнуто. Рівень застосування звільнення від покарання свідчить, що імовірно в судах зазвичай опиняються справи щодо обвинувачення у найменш небезпечних проявах глорифікації. Це додатково підтверджується аномальними, у контексті загальних показників протидії злочинності, даними, що характеризують вік, стать, освіту й заняття засуджених за вчинення кримінальних правопорушень, передбачених ст. 436-2 КК. Можна стверджувати, що спостерігається примітивізація кримінально-правової протидії виправдовуванню, визнанню правомірною, запереченню збройної агресії РФ проти України, глорифікації її учасників.

Необхідність ефективного кримінально-правового регулювання в умовах протидії військовій агресії РФ і в процесі відновлення після перемоги над агресором є очевидною. Невідповідність цілей і прогнозів соціальних ефектів криміналізації тенденціям практичного

¹ Проект Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції) реєстр. № 5102 від 18.02.2021. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5102&conv=9> (дата звернення: 21.09.2025).

² Інститутом вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України за підтримки Національного фонду досліджень України був реалізований науковий проект «Кримінально-правові та кримінологічні засади протидії глорифікації збройної агресії РФ в Україні» (реєстраційний номер 2022.01/0060).

кримінально-правового регулювання потребує розгляду проблеми в контексті прагматичної парадигми кримінального права й підтверджує висловлені зауваження щодо необхідності визначення меж ефективного кримінально-правового впливу на відносини інформаційної безпеки у сфері формування інформаційного ресурсу. Крім того, наявний досвід вкотре актуалізує проблематику нечітких формулювань заборон і необхідності законодавчої визначеності.

Висновки

Аналіз «некомп'ютерних» посягань на інформаційну безпеку засвідчує дві ключові проблеми.

По-перше, надмірна кількість спеціальних кримінально-правових заборон щодо обмеженого доступу до інформації створює ефект дублювання та ускладнює правозастосування. Доцільнішим видається консолідований підхід, коли інтенсивність кримінально-правової реакції визначається не видом таємниці, а фактичними наслідками й завданою шкодою. Аналогічний підхід був реалізований у кримінальному законодавстві стосовно власності. Законодавець відмовився від окремих норм для державної і приватної власності, визнавши, що ключовими є факт посягання на власність і заподіяна шкода, а не форма її належності. Сучасні соціальні трансформації породжують схожу ситуацію. Норми, орієнтовані на захист окремих видів інформації, втрачають сенс, адже визначальною стає не форма чи носій відомостей, а реальний масштаб негативних наслідків їх незаконного розповсюдження чи використання.

По-друге, у сфері формування інформаційного простору кримінально-правові засоби повинні застосовуватися лише як *ultima ratio*. Досвід криміналізації дезінформації та глорифікації агресора демонструє значні розриви між декларованими цілями й фактичними результатами, а також ризик примітивізації кримінальної політики. Реальний захист інформаційної безпеки тут полягає не так у кримінально-правових заборонах, як у розвитку механізмів освіти, медіаграмотності й конкурентних інформаційних продуктах, що формують стійкість суспільства до інформаційних загроз.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА АНАЛІЗ ЗЛОЧИННОСТІ

Інформаційні технології у сфері протидії злочинності застосовуються доволі давно. Традиційно вони використовувалися для вирішення прикладних завдань: ідентифікації осіб за біометричними ознаками, пошуку викраденого майна, порівняння відбитків пальців чи ДНК, розпізнавання голосу, побудови криміналістичних обліків і баз даних. Ці інструменти є важливою частиною повсякденної роботи правоохоронних органів і значно підвищили ефективність оперативно-розшукової та слідчої діяльності.

Проте всі наведені приклади демонструють використання ІТ переважно як допоміжних інструментів у кримінальному процесі. Суто кримінально-правове застосування інформаційних технологій, на нашу думку, пов'язане з новим рівнем дослідження злочинності – рівнем, на якому ключовим стає автоматизоване опрацювання значних масивів даних.

Сьогодні інформатизація не лише створює нові загрози у вигляді комп'ютерних злочинів, а й відкриває безпрецедентні можливості для підвищення ефективності кримінального права. Автоматизована обробка даних уможливорює виявлення тенденцій злочинності, критичну оцінку результативності кримінально-правових заборон, прогнозування ризиків і формування науково обґрунтованих рекомендацій для законодавця та практики.

Саме в цьому контексті ми пропонуємо поняття «обчислювального кримінологічного аргументування» – методології, яка поєднує потенціал інформаційних технологій і правової науки для обґрунтування положень про злочинність й ефективність заходів протидії.

6.1. Обчислювальне кримінологічне аргументування

У 1930-х рр. у Бостонській міській лікарні працював молодий інтерн Л. Томас, який згодом став відомим лікарем й автором книги «The Youngest Science: Notes of a Medicine-Watcher»¹. Тоді, коли він розпочав свою практику, лікарі відверто визнавали ефективність лише трьох видів ліків – проносних, паліативних і плацебо – й говорили про необхідність визнавати терапевтичний нігілізм.

Прийняття терапевтичного нігілізму вимагало від лікаря чесності з собою та пацієнтом: визнавати, що зазвичай хвороба йде своїм шляхом, а роль медицини полягає в підтримці й ретельному спостереженні. Тому в лікарнях на перший план виходили систематичний збір й аналіз даних про перебіг захворювань, що дало змогу поступово відрізнити випадкові одужання від результатів медичного втручання. Така практика за кілька років створила підґрунтя для впевненого лікування низки серцевих хвороб, а згодом і для впровадження перших ефективних протимікробних засобів.

Схожу ситуацію ми спостерігаємо зараз у суспільствознавчих науках. Складно не погодитись із Б. Розовським: «Давайте на час охолодимо емоції та поміркуємо: чи могли б називатися наукою фізика або механіка, якщо б їх досягнення обмежувалися геніальним винаходом колеса?»². Сьогодні фізика здатна зробити вражаючі точні розрахунки. Якщо потрібно запустити супутник на орбіту, інженери визначають масу апарата, вид і кількість пального, траєкторію та інші параметри й отримують рішення, яке спрацює в будь-який момент і в будь-якій точці планети. Змінюйте вихідні дані, формули однаково дадуть правильний результат.

А тепер уявімо подібну впевненість у кримінології чи кримінальному праві. Чи можемо ми розрахувати «оптимальну» норму закону

¹ Thomas L. The youngest science : Notes of a medicine-watcher. Penguin Books, 1995. 272 p.

² Розовський Б. Г. Карному кодексу слід надати нагадування-епіграф: «Багато розстріляних було помертно реабілітовано!». *Актуальні проблеми права: теорія і практика*. 2020. № 2 (40). С. 38–39.

чи модель правозастосування так, щоб вона з однаковим успіхом діяла в різних країнах, культурах, історичних контекстах? Досвід показує – ні. Те, що ефективно стримує злочинність в одному середовищі, може бути майже безсилим в іншому. Рекомендації, отримані навіть із найретельніших соціальних досліджень, часто мають суто локальну цінність.

Це ставить перед нами незручні, але важливі запитання: чи можна суспільствознавство вважати наукою? Наскільки воно здатне виявляти сталі закономірності розвитку суспільства, а не лише описувати його окремі фрагменти?

Очевидно, що опис суспільних процесів із математичною точністю значно складніший, аніж моделювання руху тіла в просторі. Проте нині технологічний прогрес відкриває новий рівень пізнання соціальної сфери: інформатизація забезпечує величезні масиви даних, а сучасні методи їх аналізу дають змогу суттєво оновити методологію та результати суспільних наук.

«Зростаюча інтеграція технологій у наше життя надає доступ до безпрецедентних обсягів даних про повсякденну поведінку суспільства. Такі дані відкривають нові можливості для роботи в напрямі розуміння наших складних соціальних систем у межах нової дисципліни, відомої як обчислювальна соціальна наука (Computational Social Science)». Це зазначено в Маніфесті обчислювальної соціальної науки¹. А. Манн влучно називає результати, що отримує ця наука, «поглядом на суспільство у великій розподільчій здатності (in high resolution)»².

Інтеграція інформатики й соціальних наук дає доволі цікаві результати. Методи обробки інформації ефективно застосовуються для вирішення складних соціальних проблем. З-поміж них: установлення особливостей внутрішньої структури соціальних груп на основі ме-

¹ Manifesto of computational social science / R. Conte, N. Gilbert, G. Bonelli et al. *European Physical Journal Special Topics*. 2012. 22 p. URL: <http://www.everyaware.eu/resources/publications/Conte-2012.pdf> (дата звернення: 19.09.2025).

² Mann A. Core concept: Computational social science. *Proceedings of the National Academy of Sciences*. 2016, January 19. Vol. 113, No. 3. P. 468–470. DOI: <https://doi.org/10.1073/pnas.1524881113>.

режевого аналізу¹, автоматизована обробка звернень у системах електронного урядування (e-government)², алгоритмізація визначення фейкових новин³, вирішення проблем оптимізації оборони⁴ тощо.

Використання обчислювальної соціальної науки для вирішення завдань, що стоять перед юриспруденцією, також є достатньо перспективним. Дослідники отримали змогу працювати з надвеликими обсягами інформації, ставити завдання, які раніше неможливо було вирішити. Комплекс питань щодо дослідження злочинності з використанням інформаційних технологій нами об'єднано поняттям «*обчислювальне кримінологічне аргументування*»⁵.

Аргументування визначається як «процес обґрунтування людиною певного положення (твердження, гіпотези, концепції) з метою переконання в його істинності, слушності»⁶. Правове аргументування є однією з актуальних проблем сучасної юридичної науки⁷. Криміно-

¹ Fotoohi S., Saeidi S. Discovering the maximum clique in social networks using artificial bee colony optimization method. *International Journal of Information Technology and Computer Science*. 2019. Vol. 11, No. 10. P. 1–11. DOI: <https://doi.org/10.5815/ijitcs.2019.10.01>.

² Iskandarli G. Y. Applying clustering and topic modeling to automatic analysis of citizens' comments in e-government. *International Journal of Information Technology and Computer Science*. 2020. Vol. 12, No. 6. P. 1–10. DOI: <https://doi.org/10.5815/ijitcs.2020.06.01>.

³ Akinyemi B., Adewusi O., Oyeade A. An improved classification model for fake news detection in social media. *International Journal of Information Technology and Computer Science*. 2020. Vol. 12, No. 1. P. 34–43. DOI: <https://doi.org/10.5815/ijitcs.2020.01.05>.

⁴ Hazra T., Kumar C. R. S., Nene M. J. Strategies for searching targets using mobile sensors in defense scenarios. *International Journal of Information Technology and Computer Science*. 2017. Vol. 9, No. 5. P. 61–70. DOI: <https://doi.org/10.5815/ijitcs.2017.05.08>.

⁵ Карчевський М. В. Обчислювальне кримінологічне аргументування: поняття, можливості та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2022. № 4 (100). С. 112–126. DOI: <https://doi.org/10.33766/2524-0323.100.112-126>.

⁶ Філософський енциклопедичний словник / НАН України, Ін-т філософії ім. Г. С. Сковороди ; редкол.: В. І. Шинкарук (голова) та ін. ; наук. ред. Л. В. Озадовська, Н. П. Поліщук. Київ : Абрис, 2002. С. 36.

⁷ Рабінович П. М., Дудаш Т. І. Правова аргументація: терміно-поняттєвий інструментарій дослідження. *Вісник Національної академії правових наук України*. 2016. № 2. С. 8–20. URL: http://nbuv.gov.ua/UJRN/vapny_2016_2_3 (дата звернення: 21.09.2025) ; Дудаш Т. Особливості аргументування рішень Європейського

логічне аргументування є видом правового та стосується злочинності, її причин, особистості злочинця, заходів запобігання. Кримінологічне аргументування оперує положеннями, що належать і до кримінально-правового регулювання, і до пов'язаних зі злочинністю соціальних процесів.

Соціальна динаміка є необхідним контекстом аналізу даних про використання права. Так, стрімке зростання з 2014 року злочинів проти основ національної безпеки пояснюється саме контекстом – військовою агресією РФ проти України. Падіння облікованих правопорушень у сфері обігу наркотиків 2016 року не свідчить про те, що в цей рік стало менше відповідних посягань, а відображає складні процеси реформування Національної поліції України. Тлумачення зростання кількості облікованих зґвалтувань і кількості осіб, засуджених за цей злочин, потребує розгляду цих процесів у контексті ратифікації Україною Стамбульської конвенції.

Обчислювальне аргументування здійснюється шляхом використання інформаційних технологій для збирання, обробки, аналізу й візуалізації даних. Використання інформаційних технологій для дослідження соціальних процесів вивчається обчислювальною соціальною наукою («computational social science»). Методи цієї науки поділяються на такі групи, як: автоматизація збору даних, аналіз соціальних систем, соціальні геоінформаційні системи, моделювання соціальних систем тощо¹. Обчислювальна соціальна наука розгляда-

суду з прав людини (до характеристики методологічних підходів). *Право України*. 2017. № 4. С. 86–95 ; Feteris E. T. Fundamentals of legal argumentation : A survey of theories on justification of judicial decisions. 2nd ed. Dordrecht : Springer, 2017. 225 p. (Argumentation Library ; Vol. 1) ; Щербина О. Ю. До питання про розуміння аргументації у логіко-юридичних дослідженнях. *Гуманітарні студії*. 2014. Вип. 21. С. 45–53 ; Stelmach J., Brożek B. Methods of legal reasoning. Springer, 2006. 236 p. (Law and Philosophy Library ; Vol. 78) ; Козюбра М. І. Моделі (типи) юридичної аргументації. *Наукові записки НаУКМА. Серія «Юридичні науки»*. 2013. Т. 144–145. С. 3–8 ; Кістяник В. І. Правова аргументація: сучасні підходи до її розуміння в зарубіжних дослідженнях. *Наукові записки НаУКМА. Серія «Юридичні науки»*. 2012. Т. 129. С. 20–22.

¹ Cioffi-Revilla C. Computational social science. *Wiley Interdisciplinary Reviews Computational Statistics*. 2010. Vol. 2, Iss. 3. P. 259–271. DOI: <https://doi.org/10.1002/wics.95>.

ється як міждисциплінарне поле, яке включає математику, статистику, науку про дані (data science) та, звичайно ж, науку про суспільство (social science)¹. Своєю чергою data science визначається як набір фундаментальних принципів вилучення інформації та знань із даних².

Логіка розглядає аргумент як «думку, істинність якої уже встановлена раніше і яка може бути використана для обґрунтування істинності довільного положення»³. Дані, отримані з використанням сучасних технологій, розглядаються як аргументи тоді, коли вони одержані з дотриманням відповідної методології. Такою, зокрема, є методологія проведення відтворюваного дослідження (reproducible research). Аналіз даних вважається відтворюваним, якщо набори аналітичних даних і комп'ютерний код, використаний для створення аналізу даних, надаються іншим для незалежного вивчення та аналізу⁴. У такий спосіб досягається відкритість дослідження та значно збільшується довіра до його результатів.

Отже, обчислювальне аргументування полягає в методологічно послідовному отриманні нових знань із даних, що збираються та обробляються автоматизовано. Варто зазначити, що розвиток логічних моделей правового аргументування натеper відбувається саме на перетині сучасних інформаційних технологій, зокрема штучного інтелекту, та права⁵.

Таким чином, обчислювальне кримінологічне аргументування визначимо як *процес обґрунтування положень про злочинність, її причини, особистість злочинця, заходи запобігання, який здійснюється шляхом методологічно послідовного отримання нових знань із даних, що збираються та обробляються автоматизовано.*

¹ Hox J. J. Computational social science methodology, anyone? *Methodology*. 2017. Vol. 13, Iss. suppl. 1. P. 3–12. DOI: <https://doi.org/10.1027/1614-2241/a000127>.

² Provost F., Fawcett T. Data science and its relationship to big data and data-driven decision making. *Big Data*. 2013. Vol. 1, No. 1. P. 51–59. DOI: <https://doi.org/10.1089/big.2013.1508>.

³ Конверський А. С. Логіка : підручник. 2-ге вид., випр. Київ : Київ. ун-т, 2017. С. 365.

⁴ Peng R. D. Reproducible research in computational science. *Science*. 2011. Vol. 334, Iss. 6060. P. 1226–1227. DOI: <https://doi.org/10.1126/science.1213847>.

⁵ Prakken H., Sartor G. Law and logic: A review from an argumentation perspective. *Artificial Intelligence*. 2015. Vol. 227. P. 214–245. DOI: <https://doi.org/10.1016/j.art-int.2015.06.005>.

6.2. «CrimeDataLab»: сучасний аналіз відкритих даних щодо протидії злочинності в Україні

Застосовуючи методи обчислювального кримінологічного аргументування, ми створили аналітичну платформу «CrimeDataLab» (<https://crimedatalab.org/>). Її розробка ґрунтувалася на переконанні, що невід’ємною частиною сучасного демократичного процесу є громадський контроль за діяльністю правоохоронних і судових органів. Залучення громадян до оцінки й моніторингу роботи державних структур відбувається завдяки відкритим даним, які систематично публікуються у вигляді статистики та звітів. Такий підхід підвищує прозорість, об’єктивність і підзвітність роботи правоохоронної та судової систем, зміцнює суспільну довіру до державних інституцій і посилює ефективність заходів із запобігання та протидії злочинності.

В Україні відчувається брак інструментів для глибокого аналізу публічних даних у сфері протидії злочинності. Це ускладнює проведення якісних досліджень на основі статистики, обмежує можливість об’єктивно оцінювати результативність правоохоронної діяльності, зумовлює дисбаланс у змінах кримінального законодавства й ускладнює контроль за реформою кримінальної юстиції.

Базові показники кримінально-правового регулювання нині публікуються в періодичних звітах у форматі електронних таблиць, доступних для завантаження з вебсайтів ОГП та ДСА України. Проте такий формат значно ускладнює обробку даних. Щоб отримати уявлення про ефективність протидії злочинності, доводиться виконувати складні технічні операції. У підсумку діяльність правоохоронних та судових органів і надалі є недостатньо прозорою, а демократичний контроль – обмеженим.

Розроблена нами аналітична платформа «CrimeDataLab» пропонує інноваційне рішення, яке робить дані у сфері протидії злочинності в Україні доступними та зрозумілими для широкої аудиторії. Вона забезпечує швидкий аналіз великих масивів кримінальної статистики й надає інструменти для інтерактивної роботи з даними, візуалізації складних закономірностей і виявлення тенденцій.

Головні характеристики платформи: 1) період охоплення – два-надцять років (2013–2024 рр.); 2) понад 300 параметрів для аналізу застосування кримінального законодавства; 3) понад 14 млн показників роботи системи кримінальної юстиції; 4) режим створення власних візуалізацій і наборів даних із можливістю комбінувати параметри, визначати часові межі, рівень узагальнення та розраховувати відносні величини; 5) режим побудови фонових картограм на основі регіональної статистики.

Особливості платформи можна узагальнити в трьох вимірах: юридичному, алгоритмічному й технічному.

Юридичний вимір полягає в тому, що вхідні дані розглядаються крізь призму усталених у правовій науці підходів. Це стосується, зокрема, змісту таких понять, як «кримінальне правопорушення», «обліковане правопорушення», «вирок, що набрав чинності» тощо. Логіка відображення процесу протидії злочинності визначається структурою та змістом аналізованих статистичних звітів. У спрощеному виді цей процес виглядає так: правоохоронні органи обліковують певні події як такі, що підлягають дослідженню в межах кримінальних проваджень. За результатами досудового розслідування може бути ухвалено рішення про скерування матеріалів до суду в одній із чотирьох форм: з обвинувальним актом, із клопотанням про звільнення від кримінальної відповідальності, із клопотанням про застосування примусових заходів медичного чи виховного характеру. Судовий розгляд завершується набранням чинності рішенням, яке може бути чотирьох типів: про засудження, виправдання, застосування примусових заходів медичного характеру або закриття провадження. Якщо особа визнається винною, кримінальна відповідальність реалізується в репресивній (призначення покарання) чи ліберальній (звільнення від покарання) формах.

Як вхідні дані використовуються річні звіти ОГП і ДСА, що перебувають у відкритому доступі, збираються й оприлюднюються на виконання відповідних нормативно-правових актів¹.

¹ Про затвердження річних форм звітів щодо здійснення правосуддя місцевими та апеляційними судами : наказ Держ. суд. адміністрації України від 23.06.2018 № 325.

Алгоритмічний аспект охоплює специфіку реалізації відтвореного дослідження (reproducible research). Збір даних відбувається шляхом завантаження звітів, оприлюднених на офіційних вебресурсах ОГП і ДСА. Посилання на ці звіти інтегровані безпосередньо в програмні скрипти, виконання яких забезпечує створення локальних копій вхідних даних. Наступний крок – їх трансформація у формат, придатний для автоматизованої обробки («чисті» дані). На основі аналізу структури звітів були розроблені скрипти очищення, що дали змогу сформувати файли лише з показниками кримінально-правового регулювання, прив'язаними до конкретних статей Особливої частини КК. Із цих файлів вилучені всі елементи, які перешкоджають автоматизованій роботі (розмітка таблиць, підсумкові рядки, заголовки тощо). Подальше виконання скриптів передбачає формування з очищених даних добірок і узагальнень, необхідних для подальшої візуалізації. Представлення результатів також відбувається автоматизовано – через виконання скриптів, що використовують отримані добірки та стандартні бібліотеки для графічного відображення даних.

Технічний аспект визначається характеристиками використаного програмного забезпечення. Для виконання завдань дослідження використовувалася мова програмування R¹, середовище розробки програмного забезпечення з відкритим вихідним кодом RStudio². Розробку оболонки вебзастосунку здійснено з використанням «Shiny R» – програмного середовища для створення інтерактивних програмних продуктів із графічним інтерфейсом на основі мови програмування R. Використано такі бібліотеки (libraries)

URL: <https://zakon.rada.gov.ua/rada/show/v0325750-18> (дата звернення: 21.09.2025) ; Про затвердження форм єдиної звітності про стан кримінальної протиправності : наказ Офісу Ген. прокурора України від 30.06.2020 № 299. URL: <https://zakon.rada.gov.ua/laws/show/v0299905-20> (дата звернення: 21.09.2025).

¹ The R Project for Statistical Computing : вебсайт / R Core Team ; R. Foundation for Statistical Computing, Vienna, Austria. URL: <https://www.r-project.org/> (дата звернення: 21.09.2025).

² Positron : The data science code editor / Posit Software, PBC formerly RStudio, PBC. URL: <https://posit.co/> (дата звернення: 21.09.2025).

R: «shiny»¹, «readxl»², «readr»³, «DT»⁴, «xlsx»⁵, «tidyverse»⁶, «textreadr»⁷, «stringr»⁸.

Основні функції платформи наступні.

«CrimeTracer» – інструмент для швидкого аналізу окремих кримінальних правопорушень: динаміка злочинів за статтями КК, порівняння кількості матеріалів, переданих до суду, із кількістю засуджених осіб, візуалізація тенденцій реального покарання.

«CrimeExplorer» – аналіз регіональних особливостей кримінальної статистики: вибір регіону й перегляд ключових показників щодо злочинності, взаємодія з інтерактивною картою, динаміка змін у різних регіонах за окремими статтями КК.

«CrimeScale AI» – інтелектуальний асистент для аналітики: автоматизований аналіз великих обсягів даних; генерація детальних таблиць, графіків і прогнозних моделей; відповіді на специфічні запити щодо кримінальної статистики (подано тестовий варіант, робота над остаточним триває).

¹ shiny: Web Application Framework for R / W. Chang, J. Cheng, J. J. Allaire et al. R package version 1.11.1. 2025. URL: <https://CRAN.R-project.org/package=shiny> (дата звернення: 21.09.2025).

² Wickham H., Bryan J. readxl: Read Excel Files. R package version 1.4.5. 2025. URL: <https://CRAN.R-project.org/package=readxl> (дата звернення: 21.09.2025).

³ Wickham H., Hester J., Bryan J. readr: Read Rectangular Text Data. R package version 2.1.5. 2024. URL: <https://CRAN.R-project.org/package=readr> (дата звернення: 21.09.2025).

⁴ Xie Y., Cheng J., Tan X., Aden-Buie G. DT: A Wrapper of the JavaScript Library 'DataTables'. R package version 0.34.0. 2025. URL: <https://CRAN.R-project.org/package=DT> (дата звернення: 21.09.2025).

⁵ Dragulescu A., Arendt C. xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files. R package version 0.6.5. 2020. URL: <https://CRAN.R-project.org/package=xlsx> (дата звернення: 21.09.2025).

⁶ Welcome to the tidyverse / Wickham H., Averick M., Bryan J. et al. *Journal of Open Source Software*. 2019. Vol. 4, Iss. 43. Art. 1686. 6 p. DOI: <https://doi.org/10.21105/joss.01686>.

⁷ Textreadr. *GitHub*. URL: <https://github.com/trinker/textreadr> (дата звернення: 21.09.2025).

⁸ Wickham H. stringr: Simple, Consistent Wrappers for Common String Operations. R package version 1.5.2. 2025. URL: <https://CRAN.R-project.org/package=stringr> (дата звернення: 21.09.2025).

Інструменти наукового дослідження злочинності: глибокий аналіз злочинності за різними параметрами, підготовка аналітичних вибірок, порівняння даних щодо правоохоронної та судової статистики.

Отже, «CrimeDataLab» реалізує комплексний підхід до аналізу кримінальної статистики. Завдяки комбінації бібліотек автоматизованої обробки даних і вбудованому інструменту для роботи з базами даних SQLite платформа забезпечує гнучкість, ефективність і зручність використання для дослідників, аналітиків, правоохоронних органів, організацій громадянського суспільства тощо¹.

Окремо варто зазначити, що і створена аналітична платформа, і всі використані програмні продукти й дані є у вільному доступі, що додатково гарантує відтворення здійсненого дослідження.

Офіційна статистика є важливим індикатором соціальної стабільності й ефективності функціонування правоохоронної системи держави. Україна зіткнулася з численними викликами, зумовленими і внутрішніми соціально-економічними чинниками, і зовнішньою військовою агресією. Аналіз цих викликів на основі статистичних даних має певні методологічні обмеження, про які йтиметься далі. Водночас саме такий підхід дає змогу сформулювати гострі, але необхідні для суспільної дискусії питання. Використання створеної нами аналітичної платформи забезпечує можливість усебічного розгляду масивів статистики за останні дванадцять років, що дає змогу ідентифікувати актуальні проблеми кримінально-правового регулювання.

У період з 2013 по 2024 рік простежується суттєве коливання кількості облікованих кримінальних правопорушень і поступове зменшення кількості засуджених осіб. У 2013 році обліковано 563 558 кримінальних правопорушень, засуджено 122 973 осіб. У 2024 році обліковано 492 479 правопорушень (на ~71 тис. менше, ніж у 2013 році). У 2024 році засуджено 61 434 особи (менше майже вдвічі) (рис. 1).

¹ Прикладом використання платформи журналістами може слугувати аналітична стаття Олега Гебури «Члени наркобанд майже не потрапляють за ґрати. Аналіз судових рішень» на [Texty.org.ua](https://texty.org.ua), див.: Гебура О. Члени наркобанд майже не потрапляють за ґрати. Аналіз судових рішень. *Texty.org.ua*. 17.07.2025. URL: <https://texty.org.ua/projects/115496/imitaciya-narkoborotby-chomu-pravoohoronna-systema-karaye-spozhyvachiv-a-ne-prodavciv/> (дата звернення: 21.09.2025).

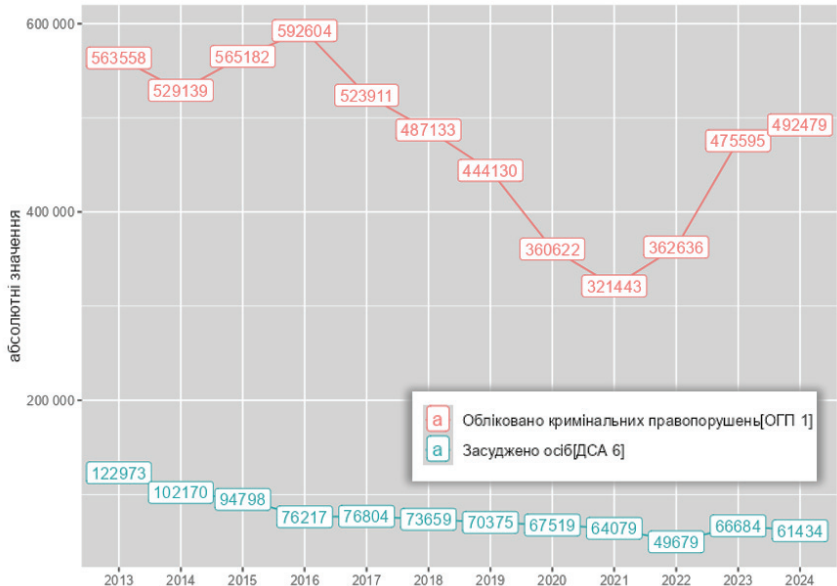


Рис. 1. Кількість облікованих проваджень і засуджених осіб

Навіть враховуючи різні підходи до статистичного обліку кримінальних проваджень (ОГП) і засуджених осіб (ДСА)¹, слід зазначити, що відбулися суттєві трансформації як у кількісному обсязі злочинності, так і в ефективності реагування на неї (рис. 2).

Як маркер діяльності правоохоронних і судових органів доцільно розглядати співвідношення між кількістю осіб, стосовно яких судові рішення набрали законної сили, та загальною кількістю облікованих проваджень. Динаміка цього показника демонструє кілька важливих тенденцій:

- зниження в 2016 році до 15,9% збігається з початком реформи поліції та формуванням нових організаційно-правових структур,

¹ Карчевський М. В. Протидія злочинності в умовах війни: аналіз статистичних даних (2013–2023). *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 2. С. 80–90. DOI: <https://doi.org/10.32782/2311-8040/2024-2-12>.

що на стартових етапах зумовило істотні коливання в роботі правоохоронної системи;



Рис. 2. Відношення кількості осіб, судові рішення стосовно яких набрали законної сили, до кількості облікованих проваджень

– зростання до 27,5% у 2021 році можна інтерпретувати як тимчасове підвищення результативності кримінального переслідування, пов’язане з адаптацією системи до оновлених умов;

– різке падіння у 2022 році до 18,1% безпосередньо зумовлене початком повномасштабного вторгнення рф, яке спричинило дестабілізацію судової системи, евакуацію установ та масову реєстрацію воєнних злочинів. Тимчасово доступ національної юстиції до виконавців цих посягань обмежений. Надалі показник продовжив знижуватись і досяг рівня 17% у 2024 році.

У підсумку система кримінальної юстиції демонструє стійку тенденцію до зменшення ймовірності того, що обліковане правопорушення завершиться судовим розглядом.

У воєнний час це частково пояснюється об’єктивними обставинами: значна частина кримінальних проваджень після 2022 року стосується воєнних злочинів рф – обстрілів цивільної інфраструктури, убивств мирного населення, знищення житла й об’єктів критичної інфраструктури. Такі події обліковуються як кримінальні правопорушення, проте зазвичай вони наразі не мають установлених виконавців.

Додатковим чинником є поступова лібералізація реєстрації проваджень: зменшення адміністративного тиску сприяє обліку більшої їх кількості, а практика відмов у реєстрації мінімізується.

Слід визнати, що процедура обліку кримінальних правопорушень в Україні поєднує процесуальну, адміністративну й політичну логіку.

Вона не є прямим відображенням рівня злочинності, а тому потребує глибокого аналізу під час досліджень чи оцінки ефективності правоохоронної системи.

Водночас наявна тенденція зростання формальної активності правоохоронних органів при одночасному скороченні кількості осіб, притягнутих до відповідальності, є очевидною. У таких умовах зростає ризик зміщення зусиль із розслідування небезпечних, але складних правопорушень на так звані «легкі цілі» – справи, які легко облікувати, швидко передати до суду й завершити вироком. Цю тенденцію ми називаємо примітивізацією протидії злочинності.

Примітивізація виникає тоді, коли система кримінальної юстиції переорієнтовується на прості справи, що не завжди відповідають реальним загрозам, але дають змогу підтримувати формальну статистичну «ефективність».

Примітивізацією правозастосовного рівня кримінально-правового регулювання називатимемо ситуацію, коли значна частина судових рішень, пов'язаних із засудженням осіб за певні кримінальні правопорушення, стосується найменш небезпечних форм таких правопорушень за умови фактичної відносної поширеності більш небезпечних форм цих правопорушень. Зрозуміло, що примітивізація є небезпечним явищем, оскільки свідчить про зниження ефективності кримінально-правового регулювання.

Використання створеної платформи дало змогу ідентифікувати вияви примітивізації в таких сферах правозастосовного кримінально-правового регулювання, як: протидія корупції, протидія незаконному обігу наркотиків, протидія глорифікації дій ворога.

Протидія корупції

Якщо до 2017 року більшість осіб засуджували за отримання неправомірної вигоди, то з 2018 року – за пропозицію неправомірної вигоди. Абсолютні значення ще більш промовисті: у 2013 році за отримання неправомірної вигоди засуджено 731 особу, за пропозицію – 80; у 2024 році за отримання неправомірної вигоди засуджено 80 осіб, за пропозицію – 1286 (рис. 3).

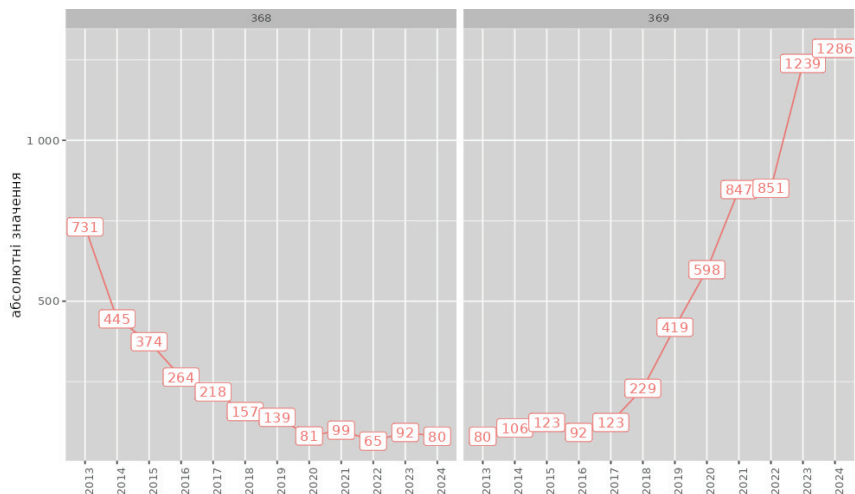


Рис. 3. Кількість засуджених за отримання неправомірної вигоди (ст. 368 КК) та пропозицію неправомірної вигоди (ст. 369 КК)

Процес був поступовим, відповідні тенденції зменшення / збільшення кількості засуджених осіб прослідковувалися впродовж усього періоду спостережень. Із 2018 по 2024 рік частка засуджених за пропозицію неправомірної вигоди (ст. 369 КК) серед усіх засуджених за так звані «службові злочини» (розділ XVII Особливої частини КК) збільшилася з 29 до 77% (рис. 4).

Чи означає це, що головною проблемою протидії корупції в Україні є пропозиція неправомірної вигоди? Чи відповідають результати функціонування кримінальної юстиції реальній соціальній ситуації? Чи можна стверджувати, що соціальні ресурси, які виділяються на протидію корупції, використовуються раціонально?

Для відповіді на ці запитання ми провели розвідувальний контент-аналіз обвинувальних вироків за ст. 369 КК, які було постановлено в Єдиному державному реєстрі судових рішень. Більшість вироків стосується майже тотожних обставин: пропозиція неправомірної вигоди поліцейським (прикордонникам) під час виконання ними служ-

бових обов'язків у складі добових нарядів (охорона громадського порядку, виконання обов'язків на пункті пропуску через державний кордон тощо). У більшості судових рішень ішлося про угоду щодо визнання винуватості.

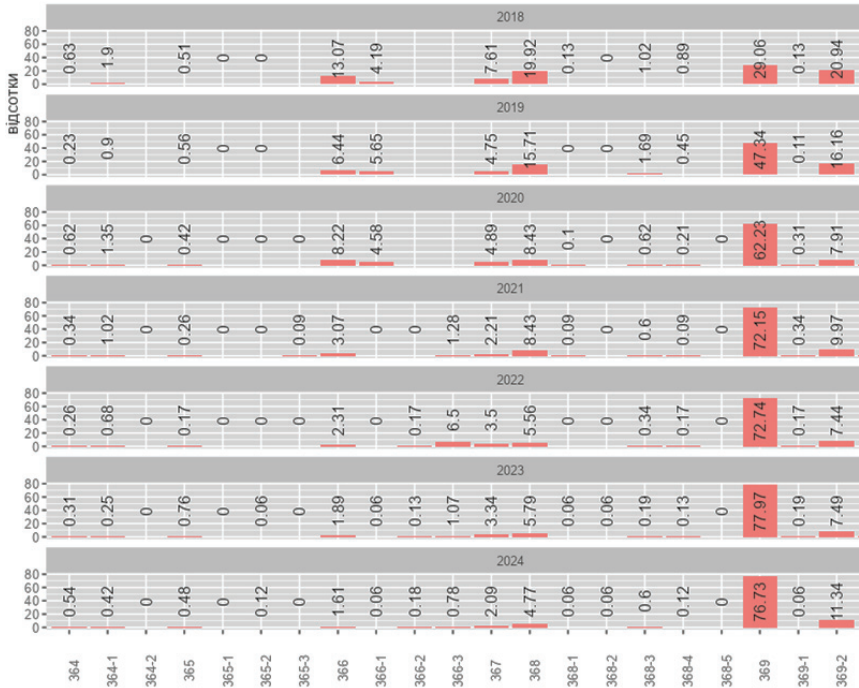


Рис. 4. Відносні значення. Розподіл кількості засуджених за статтями розділу XVII Особливої частини КК

Стосовно сформульованих запитань про відповідність фактичної судової практики соціальному запиту протидії корупції вважаємо, що відповідь має бути негативною. Навряд чи сукупність актів застосування кримінального права щодо протидії корупції, майже 3/4 якої є засудженням по угоді за пропозицією правоохоронцеві у складі добового наряду незначної неправомірної вигоди є такою, що відповідає соціальній потребі (рис. 5).

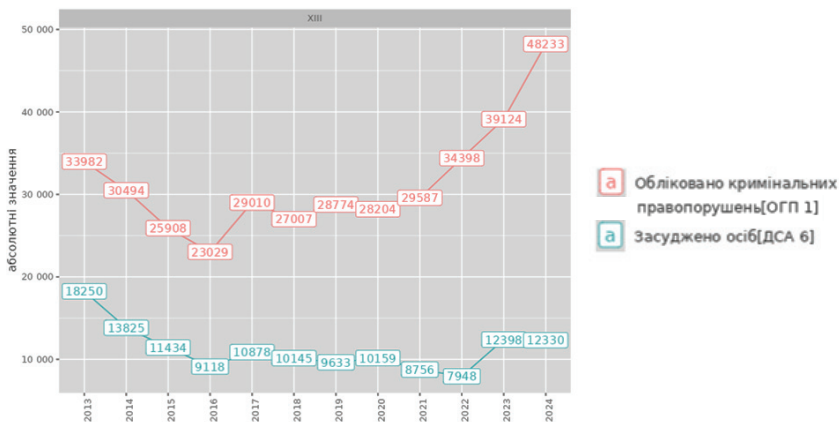
Протидія незаконному обігу наркотиків

Рис. 5. Кількість облікованих проваджень і засуджених осіб за статтями розділу XIII КК «Кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші кримінальні правопорушення проти здоров'я населення»

У 2013–2016 рр. в Україні відбулося суттєве зменшення і кількості облікованих кримінальних правопорушень (із 33 982 до 23 029), і кількості засуджених осіб (із 18 250 до 9118). Ключовим чинником цього спаду є масштабна інституційна реформа правоохоронних органів, у межах якої здійснювалося переформатування організаційних структур, створення нової патрульної поліції, ліквідація міліції, оновлення керівного складу й перерозподіл повноважень. У цей період система перебувала в стані організаційної дестабілізації, що спричинило тимчасове зниження спроможності обліковувати й ефективно розслідувати злочини.

Додатковим наслідком реформи є масштабне «вимивання» кадрів: значна кількість досвідчених працівників залишила службу. Це негативно позначилося на збереженні інституційної пам'яті, якості досудового розслідування та здатності виявляти складні форми злочинності, зокрема організований збут наркотичних засобів.

Отже, падіння показників у 2016 році слід розглядати не як ознаку зростання ефективності кримінально-правової політики, а як свідчення тимчасової дезорганізації правоохоронної системи. Така ситуація додатково підтверджує тезу про багатофакторність статистики кримінальних правопорушень, яка потребує глибокого контекстуального тлумачення. У цьому випадку вона вказує на іншу системну проблему – вразливість кримінальної політики до адміністративних реформ, що здійснюються без належного кадрового супроводу й аналітичного моніторингу їхніх наслідків.

У 2017–2021 рр. кількість облікованих правопорушень стабілізувалася (від 27 000 до 29 000 щороку), тоді як число засуджених осіб продовжувало поступово знижуватися.

У 2023–2024 рр. зафіксовано різке зростання кількості облікованих злочинів у сфері обігу наркотиків: у 2023 році – 39 124 випадки, у 2024 році – уже 48 233 (найвищий показник із 2013 року). Водночас кількість засуджених у 2024 році (12 330) залишилася на рівні попереднього року: стрімке зростання облікованих проваджень не супроводжувалося пропорційним збільшенням кількості винесених вироків. Це знову виводить нас на проблему формального підвищення активності правоохоронних органів за умови одночасного зниження ймовірності доведення облікованих злочинів до стадії судового розгляду (рис. 6).

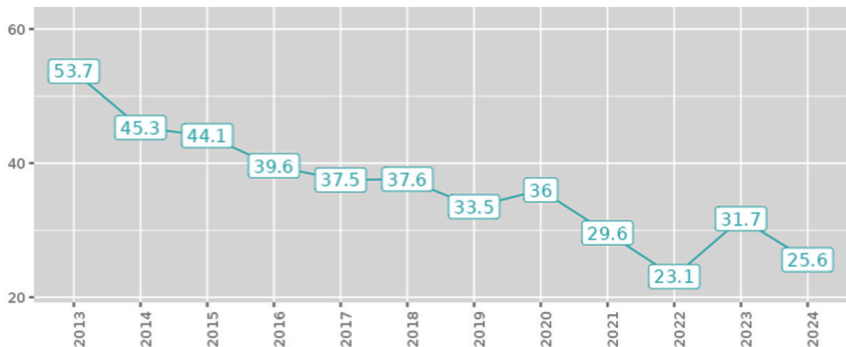


Рис. 6. Відношення кількості засуджених до кількості облікованих проваджень. Розділ XIII Особливої частини КК

Промовистою є й динаміка відношення кількості засуджених осіб до кількості облікованих кримінальних проваджень: у 2013 році цей показник становив 53,7% – тобто понад половина справ завершувалася вироком; надалі коефіцієнт стабільно знижувався: 39,6% у 2016; 33,5% у 2019; 29,6% у 2021; у 2022 році він досяг мінімуму – 23,1%, після чого у 2023 році піднявся до 31,7%, але вже у 2024 знову знизився до 25,6%.

Тенденція примітивізації проявляється особливо виразно у сфері протидії наркозлочинності. Відбувається зміщення фокусу з протидії збуту на дрібне зберігання.

Серед умовної тисячі засуджених за незаконні дії з наркотиками (ст. 307 і 309 КК) у 2013 році було б 212 осіб, пов'язаних зі збутом (ст. 307 КК), у 2024 – 80 (рис. 7). Отже, частка засуджених за зберігання наркотиків без мети збуту збільшується, що ставить під сумнів фокус професійної діяльності правоохоронців і судів. Така динаміка з усією очевидністю не відповідає тенденціям незаконного обігу наркотичних засобів. Зрозуміло, що основна проблема протидії наркотизації – це зовсім не засудження осіб, які зберігають наркотики без мети збуту.

Примітивізація у сфері протидії незаконному обігу наркотиків призводить до: концентрації зусиль на споживачах наркотиків, а не на збуті; надмірній увазі до дрібних дій «видимих» суб'єктів замість фокусування на структурних загрозах; тенденції до збільшення статистичних показників через «легкі цілі».

Отже, кримінально-правова протидія наркозлочинності в Україні демонструє нестабільність і чутливість до організаційних змін. Різке зростання кількості облікованих проваджень у 2023–2024 рр. указує на загострення проблеми. Водночас установлені тенденції примітивізації разом із негативними наслідками реформ є чинниками, що істотно зменшують ефективність протидії.

Тут слід зауважити на особливо небезпечний прояв такої неефективності в умовах війни: істотне збільшення військовослужбовців, засуджених за незаконний обіг наркотиків. Якщо за даними ДСА у 2022 році засуджено 2138 військовослужбовців, то у 2024 – 6532. Водночас частка військовослужбовців, засуджених за кримінальні

правопорушення у сфері незаконного обігу наркотиків, зросла з 9,73 % у 2022 році до 24,72 % у 2024. За ст. 307 КК (збут наркотиків) до 2022 року в середньому засуджувалося 10 військовослужбовців щороку, у 2024 році – 35. За ст. 309 КК (зберігання без мети збуту) до 2022 року в середньому засуджувалося 67 військовослужбовців щороку, у 2024 році – 1571(!).

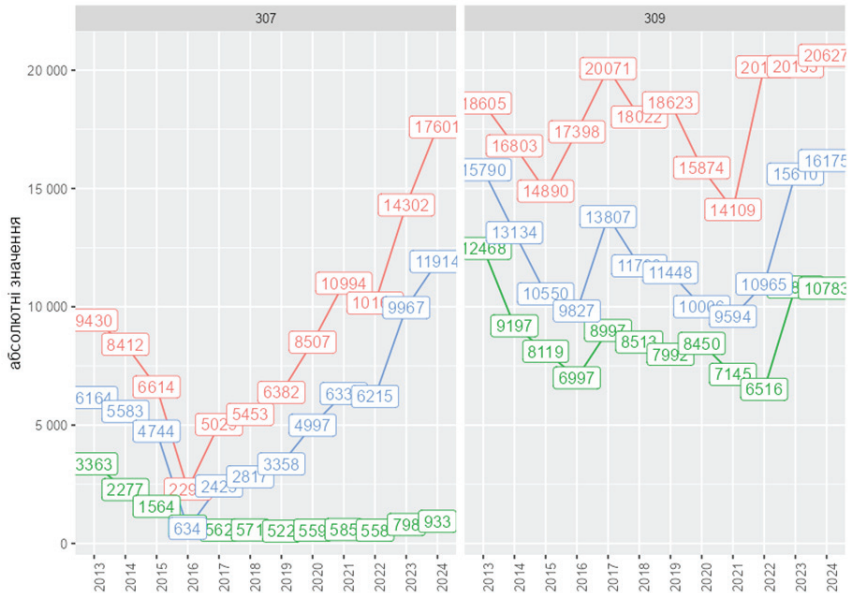


Рис. 7. Статті 307 і 309 КК. Річний розподіл облікованих проваджень (червоний), скерованих до суду обвинувальних матеріалів (синій) і кількості засуджених осіб (зелений)

Якщо розглядати кількість усіх осіб, засуджених за кримінальні правопорушення, передбачені ст. 307 і 309 КК, як 100%, то частка засуджених за ст. 307 КК у 2023 та 2024 роках буде в межах 7–8%, відповідно ст. 309 КК – 93–92%. Аналогічний розподіл для засуджених військовослужбовців: ст. 307 – 2%, ст. 309 – 98%. Отже, багаторазове збільшення військовослужбовців, засуджених за кримінальні

правопорушення у сфері незаконного обігу, стосується діянь, які не пов'язані зі збутом наркотиків.

Збереження чинного підходу, орієнтованого на репресивне переслідування споживачів наркотиків, а не на профілактику, лікування та ресоціалізацію, не вирішує проблему, а лише перетворює її на джерело нових ризиків. Наприклад, криміналізація військовослужбовців за дії, що є радше наслідком бойової травми, породжує зайві бар'єри для їхнього повернення до мирного життя. Судимість обмежує можливості працевлаштування, навчання, соціальної інтеграції.

У підсумку, проблема, яка могла б залишатись у площині медичної, психологічної або соціальної відповіді, перетворюється на юридичну пастку, яка не тільки не вирішує суть питання, а й посилює вторинну маргіналізацію, формує передумови для повторного правопорушення, посилення недовіри до держави.

Протидія глорифікації дій ворога, статистичні дані щодо протидії якої наводились у попередньому розділі, також є очевидним прикладом примітивізації.

Отже, сучасна система кримінальної юстиції в Україні демонструє ознаки примітивізації – тенденції до зосередження на простих, процедурно зручних справах, які не потребують тривалого слідства або складної доказової бази. Така логіка правозастосування дає змогу органам досудового розслідування та судам підтримувати видимість активності й ефективності, проте віддаляє систему від реагування на справжні загрози.

На прикладі протидії корупції ми бачимо, як відбулося зміщення фокусу з отримання неправомірної вигоди на пропозицію вигоди. Це супроводжується укладанням угод про визнання винуватості, що спрощує процедуру, але нівелює зміст боротьби з корупцією як системним злом.

Примітивізована протидія незаконному обігу наркотиків не вирішує проблему наркотизації суспільства.

Так само реагування на публічні прояви глорифікації дій агресора попри свою формальну відповідність кримінальному закону виявляється переважно спрямованим проти літніх людей, жінок і мар-

гіналізованих осіб – категорій, які не становлять реальної інформаційної загрози, але є зручними для статистичного обліку.

Ці приклади підтверджують трансформацію практики застосування кримінального закону від змістовної до формалізованої, де пріоритет надається не усуненню джерел небезпеки, а підтриманню статистичних показників через спрощене правозастосування.

Якщо примітивізація, на нашу думку, є найбільш небезпечною тенденцією кримінально-правового регулювання, то злочини проти власності – найпоширеніші кримінальні правопорушення. Їх найбільше обліковують (2013 рік – 59% серед облікованих, 2024 рік – 27%), за них найчастіше засуджують (2013 рік – 48% серед усіх засуджених, 2024 рік – 28%).

Із 2023 року найбільш поширеним посяганням на власність було шахрайство. У 2024 році таких посягань обліковано приблизно 65 тис., це 49% від усіх облікованих посягань на власність.

Водночас на підставі Закону України «Про внесення змін до Кодексу України про адміністративні правопорушення та деяких інших законів України щодо посилення відповідальності за дрібне викрадення чужого майна та врегулювання деяких інших питань діяльності правоохоронних органів» від 18 липня 2024 р. № 3886-IX, який набув чинності в серпні 2024 року, відбулася декриміналізація крадіжок, шахрайства та привласнення в розмірі до 3028 грн. Попередня редакція передбачала відповідальність за ці посягання, починаючи з 302,8 грн. Як результат: у 2024 році порівняно з попереднім роком відбулося зменшення облікованих крадіжок на 32% та зменшення облікованих випадків шахрайства на 21%.

Із використанням «CrimeDataLab» нами встановлено, що крадіжка (ст. 185 КК), шахрайство (ст. 190 КК) та привласнення (ст. 191 КК) за даними останніх 12 років (2013–2024) становить 50% облікованих проваджень (39% – крадіжка, 9% – шахрайство, 2% – привласнення).

Протягом останніх 12 років частка засуджених за положеннями ст. 185, 190 та 191 КК, які межують із дрібним викраденням (ст. 51 Кодексу України про адміністративні правопорушення (КУпАП)), становить 42,3%.

Прийняте рішення більш ніж суттєво вплинуло на стан протидії злочинності. Можна сказати, що у 2024 році держава відмовилася реагувати кримінально-правовими засобами на щонайменше кожен третю крадіжку та кожне п'яте шахрайство. Водночас аргументація пояснювальної записки законопроекту зводиться до того, що в актуальних умовах кваліфікація, наприклад, простої крадіжки має відбуватися як особливо кваліфікованої (в умовах воєнного стану). Далі цитата: «Таким чином, при призначенні покарання за крадіжку, вчинену в умовах воєнного стану, відбувається порушення принципу домірності...». Не перший випадок, коли законодавець більше піклується про осіб, що вчинили правопорушення, ніж про потерпілих. Видається, що рішення, які роблять тектонічні зміни, мають бути предметом більш широкої професійної дискусії.

Отже, прийняте Верховною Радою рішення можна було б характеризувати як позитивне, оскільки воно актуалізує питання раціонального використання ресурсів країни для протидії злочинності. Водночас спосіб аргументації та відсутність належних розрахунків зводить оцінку прийнятого рішення до негативної.

Тож статистично зафіксоване падіння кількості облікованих посягань на власність у 2024 році відбулося не через оздоровлення криміногенної обстановки, а через істотне збільшення порогу кримінальної відповідальності. На цьому тлі загострюється проблема ефективного захисту власності, особливої небезпеки набувають посягання на власність із використанням інтернету й соціальних мереж.

Проблема кримінально-правового регулювання, яка потребує вирішення, може бути сформульована так: чи сприяло більш ефективному захисту власності десятикратне збільшення межі адміністративно-протиправного дрібного викрадення (ст. 51 КпАП)?

Нарешті третя група проблем кримінально-правового регулювання, яка, на нашу думку, є актуальною – відповідальність військово-вслужбовців. Найбільш очевидно вона виявляється при дослідженні статистичних даних щодо самовільного залишення частини (СЗЧ) (ст. 407 КК) й дезертирства (ст. 408 КК) (рис. 8).

У 2024 році кількість облікованих фактів СЗЧ зросла в чотири рази, облікованих фактів дезертирства – у три.

Чи можна розглядати кримінально-правове регулювання як засіб вирішення цієї проблеми? Така ситуація порушує проблему ресоціалізації захисників і захисниць України. Збільшення числа засуджених військовослужбовців може бути наслідком посттравматичних розладів, соціальної дезадаптації, відсутності належної психологічної підтримки й реабілітаційних програм. Поточна система кримінального правосуддя не враховує специфіку пережитого бойового досвіду, що може призводити до криміналізації ветеранів замість їхньої ефективної ресоціалізації. Тому важливо розробити та впровадити комплексні реабілітаційні програми для демобілізованих військових, що включатимуть психологічну підтримку, соціальну адаптацію, профілактику залежностей; розширити програми працевлаштування ветеранів.

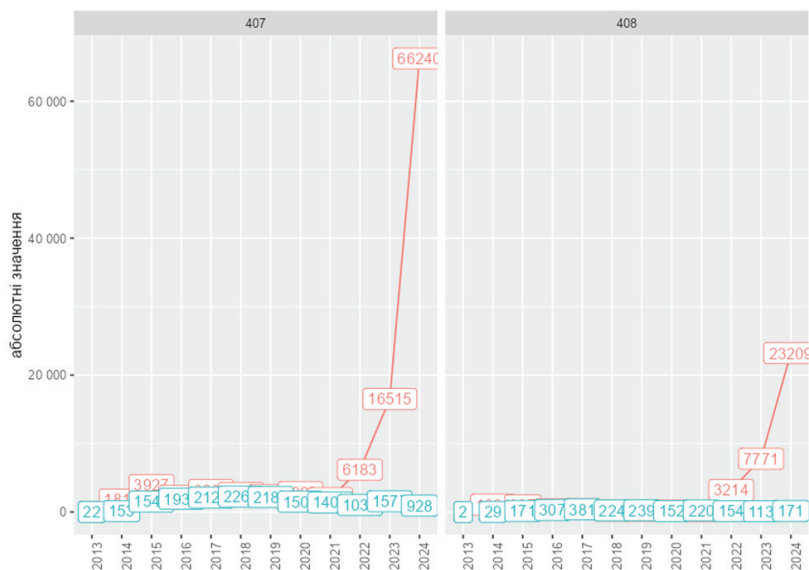


Рис. 8. Кількість облікованих проваджень і засуджених осіб за ст. 407 і 408 КК

Отже, застосування обчислювального кримінологічного аргументування та аналітичної платформи «CrimeDataLab» дало змогу встановити такі напрями подальшого аналізу.

1. Щодо посягань на власність – найпоширеніших кримінальних правопорушень. Аналіз наслідків декриміналізації дрібних крадіжок і шахрайства. Для повноцінної відповіді на питання, чи забезпечило збільшення кримінально-правового порогу підвищення ефективності протидії злочинам проти власності, потрібні додаткові дослідження. У будь-якому разі необхідно розвивати ідею запобіжників необґрунтованої (недостатньо обґрунтованої) кримінальної нормотворчості. В умовах, коли найбільш поширеним кримінальним правопорушенням стає шахрайство з використанням інформаційних технологій та активно розвиваються злочинні техніки, орієнтовані на значну кількість потерпілих, зміни до ст. 51 КУпАП можуть призвести до ефекту безкарності дрібних, але системних правопорушень.

2. Щодо тенденцій примітивізації. Небезпека подальшого розвитку примітивізації протидії злочинності потребує розробки і законодавчих, і організаційних запобіжників. Важливою є корекція пріоритетів кримінальної юстиції у сфері протидії корупції. Потребує змін антинаркотична політика. Зусилля та ресурси слід фокусувати на боротьбі зі збутом наркотиків, а не лише зі споживачами. Уточнення кримінально-правових заборон, зокрема ст. 436-2 КК, має сприяти мінімізації практики «легких цілей».

3. Проблеми ресоціалізації військовослужбовців. Перегляд меж кримінально-правового реагування на СЗЧ і дезертирство. Цілком очевидно, що зафіксоване збільшення кількості СЗЧ і дезертирства вимагає пошуку нових рішень. Збереження традиційних підходів призведе тільки до появи нових корупційних схем і криміналізації захисників країни.

6.3. Обмеженість обчислювального кримінологічного аргументування та шляхи її подолання

Водночас необхідно наголосити, що робота зі статистичними даними у сфері кримінальної юстиції має свої істотні обмеження.

Статистика не є «чистим» відображенням соціальної реальності: вона формується в межах конкретних адміністративних процедур, залежить від якості збору й обробки даних, відображає упередженість інституцій, які їх генерують. Додатково самі собою кількісні методи мають обмежений пояснювальний потенціал, адже за цифрами нерідко приховуються складні соціальні процеси, які неможливо звести лише до числових показників. Тому інтерпретація статистики завжди потребує критичного підходу та врахування методологічних ризиків, про які йтиметься далі.

Маємо зазначити, що в процесі створення платформи виявлено істотні недоліки чинної системи збирання та аналізу статистики протидії злочинності. М. Хавронюк і Р. Шехавцов розглядали це питання в контексті статистичних стандартів ООН і Європейського Союзу. У підготовленому дослідниками звіті містяться важливі пропозиції. Слід підтримати ідею створення Державного агентства кримінальної статистики як центрального органу виконавчої влади. Важливою є пропозиція науково обґрунтованих методичних рекомендацій, які забезпечують процес збирання, опрацювання, аналізу, поширення, збереження, захисту й використання кримінальної статистики. На позитивну оцінку заслуговують висновки щодо змін нормативно-правового регулювання кримінальної статистики¹. Висловлені нами положення – результат отриманого досвіду роботи з національною статистикою за методологією обчислювального кримінологічного аргументування. Ми формулюємо проблемні аспекти, які обмежують цінність наявних статистичних даних, та пропозиції, що дають змогу змінити ситуацію.

По-перше, недоліки чинної системи збирання та аналізу даних щодо протидії злочинності. Головна проблема тут – обмежений обсяг відкритих даних. У публічному інформаційному просторі є тільки агреговані звіти. Потік первинних даних і надалі є закритим, що не дає змоги використовувати відкриті дані максимально ефективно.

Окрім того, ОГП і ДСА представляють дані, зібрані під кутом їх професійної діяльності, тому їх зведення в єдиний масив часто

¹ Шехавцов Р. М., Хавронюк М. І. Звіт щодо кримінальної статистики в Україні / Центр політико-прав. реформ. Київ, 2019. 80 с. URL: <https://pravo.org.ua/books/zvit-shhodo-kryminalnoyi-statystyky-v-ukrayini/> (дата звернення: 21.09.2025).

є проблематичним. Наприклад, ОГП веде облік осіб, яким повідомлено про підозру, й матеріалів щодо вчинення кримінального правопорушення, які направлено до суду. ДСА, своєю чергою, веде облік осіб, вирoki стосовно яких набрали чинності. Однак порівняння кількості осіб, матеріали щодо яких було направлено до суду, та кількості осіб, стосовно яких існують вирoki, що набрали чинності, буде не зовсім послідовним із методологічного погляду. Річ у тім, що ОГП обліковує всі обвинувачення, а ДСА, у разі вчинення кількох правопорушень, – лише ті, що належать до статті КК з найбільш суворою санкцією.

Також слід зауважити на особливості термінології, що використовується для нормативного регулювання кримінальної статистики. Так, відповідно до Положення про порядок ведення Єдиного реєстру досудових розслідувань (ЄРДР), до загальної кількості облікованих у звітності кримінальних правопорушень не включаються правопорушення, кримінальні провадження за якими закрито через відсутність події кримінального правопорушення або відсутність у діянні складу кримінального правопорушення (пп. 1 або 2 ч. 1 ст. 284 Кримінально-процесуального кодексу України (КПК)). Отже, є різниця між «облікованим» кримінальним провадженням і «зареєстрованим». Через те що річні звіти ОГП щодо облікованих кримінальних правопорушень не дають змоги отримати уявлення про структуру рішень щодо всіх зареєстрованих проваджень, неможливо дати відповідь на надважливі питання. Головні з них такі: яким є відображення злочинності в повідомленнях до правоохоронних органів про вчинені правопорушення? Які особливості структури рішень, що приймаються правоохоронними органами залежно від первинної кваліфікації? Як впливає реформа правоохоронних органів на розподіл рішень по зареєстрованих провадженнях?

Обмежено результативними будуть і спроби прослідити інтенсивність призначених покарань. Як можна пояснити призначення за злочин, передбачений ч. 2 ст. 185 КК, покарання терміном у понад 5 років? Аналогічні питання щодо покарань, призначених за шахрайство. Відповідь у недосконалому обліку даних про покарання, призначені за сукупністю злочинів і сукупністю вироків. Водночас просто від-

кинути дані про покарання, що перевищують максимум санкцій, теж неможливо. Отже, маємо ситуацію, коли дані про покарання, призначені за одиничний злочин, додаються до покарань, призначених за сукупністю. Чітко виокремити останні не видається можливим. У результаті неможливо оцінити, наскільки інтенсивне покарання призначається за вчинення конкретного одиничного злочину. Крім того, обмежена користь статистичних даних щодо призначених покарань пов'язана також із формою звіту. Так, за окремими позиціями накопичуються дані про призначення позбавлення волі терміном на 1 рік, понад 1 рік – до 2 років, понад 2 роки – до 3 років, понад 3 роки – до 5 років, понад 5 років – до 10 років, понад 10 років – до 15 років, понад 15 років – до 25 років. За таких умов якщо санкція, наприклад, передбачає покарання від 5 до 10 років, дослідити розподіл інтенсивності призначеного покарання неможливо.

У підсумку якість збирання та узагальнення статистики проти-дії злочинності в Україні слід визнати недостатньою.

По-друге, є і класична проблема довіри до офіційної статистики. Е. Гідденс сформулював її так: «Статистика злочинності та правопорушень є, мабуть, найменш достовірною з усіх офіційно опублікованих даних із соціальних питань»¹. Така ситуація виникає через залежність змісту офіційної статистики від суб'єктів її збирання, що з необхідністю призводить до неможливості об'єктивного відображення стану речей. Статистичні дані щодо протидії злочинності збирають і надають у відкритий доступ ті органи державної влади, ефективність яких оцінюється на підставі цих даних.

Наприклад, прийняття у Великій Британії Національного стандарту реєстрації злочинів (NCRS) у квітні 2002 року з акцентом на «орієнтованому на жертв» підході до реєстрації злочинів оголошено засобом забезпечення «рівних умов гри» для всіх підрозділів поліції. На думку експертів, NCRS має фундаментальний недолік, поліцейські підрозділи змогли скористатися ним і створити ілюзію ефективного зменшення злочинності².

¹ Giddens A., Griffiths S. Sociology. Cambridge : Polity Press, 2006. 5th ed., fully rev. and updt. P. 812.

² Patrock R. 'Reading tea leaves': An assessment of the reliability of police recorded crime statistics. *The Police Journal*. 2011. Vol. 84, Iss. 1. P. 47–67. DOI: <https://doi.org/10.1350/POJO.2011.84.1.512>.

Крім питань стосовно якості процесів збирання статистичної інформації щодо протидії злочинності, маємо проблему упередженості змісту таких даних.

Нарешті, по-третє, є і проблема методологічного плану. У кримінологічній науці широко представлено думку про обмеженість кількісних методів. Небезпідставно наголошується, що кількісні методи часто не дають змоги глибоко дослідити складну поведінку людей. Ігноруються відхилення або унікальні випадки, «аутсайтери», чий досвід виходить за межі середньостатистичних даних. Натомість якісні методи дають змогу зануритися в соціальні й емоційні контексти поведінки людей, краще розуміти обставини, які формують злочинну поведінку або досвід жертв.

Зрештою складно не погодитися з висновком про те, що коли кількісні дослідження дають важливу статистичну інформацію про тенденції злочинності, якісні, своєю чергою, висвітлюють людські історії, що стоять за цифрами¹.

Отже, отримані результати аналізу статистики необхідно розглядати крізь призму таких проблемних аспектів, як: недостатня якість процесів збирання офіційних даних щодо протидії злочинності, упередженість таких даних, обмеженість кількісних методів дослідження.

Виявлені обмеження визначають напрями оптимізації кримінально-правового регулювання, зокрема створення комплексної системи інформаційного забезпечення та впровадження альтернативних критеріїв оцінки результативності діяльності правоохоронних і судових органів.

Комплексна система інформаційного забезпечення кримінально-правового регулювання. Її умовними складовими є: законодавство, наукові джерела, реєстри кримінальних проваджень, судових рішень, засуджених осіб, а також дані щодо адміністративно-правового регулювання.

Законодавство. Це структуровані й класифіковані відомості про всі закони, що передбачають кримінальну відповідальність, із поділом

¹ Ranaweera N. Beyond numbers: Embracing the depth of qualitative research in criminology affiliations. *International Journal of Qualitative Research*. 2024. Vol. 3, Iss. 3. P. 315–325. DOI: <https://doi.org/10.47540/ijqr.v3i3.1346>.

за редакціями, зазначенням строків чинності, перехресними посиланнями на позиції Верховного Суду тощо.

Наукові джерела. Йдеться про постійно актуалізовану наукову інформацію, пов'язану з окремими нормами кримінального законодавства. Через слабку взаємодію науки та практики результати досліджень використовуються обмежено; забезпечення «одноклікового» доступу до систематизованих матеріалів, прив'язаних до правових норм, сприятиме підвищенню ефективності регулювання.

Кримінальні провадження. Ключовим напрямом оновлення має стати відмова від суто агрегованих звітів. Для науковців й інститутів громадянського суспільства слід відкрити доступ до деперсоніфікованого потоку даних із ЄРДР. Це дасть змогу проводити складний аналіз і забезпечить реальну взаємодію громадськості з правоохоронними органами, виходячи за межі формальних процедур.

Подібна модель діє у сфері охорони здоров'я в країнах ЄС і Північної Америки. Усі дані про пацієнтів, включно з призначеннями й медичними показниками, зберігаються в єдиній базі; лікарі мають доступ до персональних відомостей, а науковці, контролюючі органи й фармацевтичні компанії працюють зі знеособленими даними. Це дає змогу контролювати якість препаратів, відслідковувати ефективність лікування та вдосконалювати медичне забезпечення на основі аналізу великих масивів даних. Як наслідок, система охорони здоров'я стає ефективнішою та прозорішою¹.

Реєстр судових рішень. Державний реєстр судових рішень є одним із ключових і найпотужніших інструментів сучасних наукових досліджень. Водночас його інтеграція з обліком кримінальних правопорушень необхідна для забезпечення можливості відстеження подальшої долі кожного зафіксованого провадження.

Реєстр осіб, притягнутих до кримінальної відповідальності. Нині вивчення ефективності кримінально-правових заходів із урахуванням подальшої поведінки засуджених є надзвичайно складним завданням.

¹ Schulte T., Bohnet-Joschko S. How can big data analytics support people-centred and integrated health services: A scoping review. *International Journal of Integrated Care*. Jun 16, 2022. Vol. 22. Art. 23. DOI: <https://doi.org/10.5334/ijic.5543>. PMID: 35756337; PMCID: PMC9205381.

Для оперативного здійснення таких досліджень цей реєстр повинен бути інтегрований і з обліком кримінальних правопорушень, і з реєстром судових рішень.

Система інформаційного забезпечення адміністративно-правового регулювання. Аналіз результативності кримінально-правового регулювання потребує врахування суміжних видів правового впливу. Показовим прикладом є визначення меж дрібного викрадення чужого майна. Значна частина професійної діяльності у сфері кримінальної юстиції пов'язана саме з протидією крадіжкам. Водночас офіційна статистика не містить чітких, прозорих і обґрунтованих критеріїв відмежування цього кримінального правопорушення від адміністративного, передбаченого ст. 51 КУпАП. На підставі яких розрахунків межу дрібного викрадення було збільшено в десять разів? Яка частка облікованих крадіжок становить 2,1 неоподатковуваного мінімуму доходів громадян (НМДГ), а яка – 1,8 чи менше? За таких умов показник 2,0 фактично виконує функцію «регулятора» злочинності, який може бути використаний як інструмент політичних маніпуляцій. Натомість відкритий доступ до відповідної статистики дав би змогу знаходити більш раціональні рішення цієї проблеми¹.

Створення альтернативної системи оцінки ефективності діяльності правоохоронних і судових органів, яка не ґрунтується на аналізі даних офіційної статистики. Одним із можливих варіантів вирішення проблем упередженості даних статистики й обмеженості кількісних методів оцінки злочинності є розвиток альтернативних методів.

В означеному контексті на позитивну оцінку заслуговує Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки й оборони України на 2023–2027 рр., схвалений Указом Президента України від 11 травня 2023 р. № 273/2023, який передбачає «запровадження періодичного анонімного віктимологічного опитування населення (victimology survey, crime survey) з метою

¹ В'юник М. В., Карчевський М. В., Арланова О. Д. Кримінально-правове регулювання в Україні: реалії та перспективи (аналітичні матеріали) / упоряд. Ю. В. Баулін ; Коміс. з питань прав. реформи, Робоча група з розвитку кримін. права. Харків : Право, 2020. 212 с. URL: <https://dspace.nlu.edu.ua/handle/123456789/18398> (дата звернення: 21.09.2025).

встановлення кількості осіб, які стали потерпілими від кримінальних правопорушень певного виду, а також використання методу самозвіту (self-report survey) для анонімного з'ясування кола осіб, які вчиняли будь-які кримінальні правопорушення протягом певного періоду, складання за їх результатами віктимологічних карт».

Дослідження у сфері віктимології є й у вітчизняній науці. Так, В. Туляковим розроблено основи віктимологічної теорії, уточнено зміст і характеристики процесу віктимізації, описано основні поняття, принципи й науковий апарат віктимологічної теорії, наведено результати віктимологічних досліджень¹. За редакцією Б. Головкіна й В. Голіни підготовлено навчальний посібник, у якому на основі сучасних досліджень системно викладено знання щодо сутності віктимології як науки, основних її понять, віктимізації окремих категорій жертв, соціальних та особистісних детермінант віктимності й ролі її в механізмі злочинної поведінки, шляхів і заходів віктимологічного запобігання злочинності².

Х. Курі й В. Поклад представляли результати міжнародного віктимологічного дослідження за участі Інституту зарубіжного та міжнародного кримінального права імені Макса Планка й Луганського державного університету внутрішніх справ³. А. Бова обґрунтовував необхідність і демонстрував результати оцінки даних офіційної статистики в контексті результатів віктимологічних досліджень⁴. Представлено результати багатьох інших змістовних досліджень.

Водночас вимірювання громадської довіри та впевненості в здатності правоохоронних органів протидіяти злочинності має істотні обмеження, пов'язані з джерелами формування досвіду громадян.

¹ Туляков В. О. Вчення про жертву злочину: соціальні та правові основи : автореф. дис. ... д-ра. юрид. наук : 12.00.08. Одеса, 2001. 36 с.

² Віктимологія : навч. посіб. / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін. ; за ред. В. В. Голіни, Б. М. Головкіна. Харків : Право, 2017. 308 с.

³ Поклад В., Курі Х. Віктимологические исследования в криминологии. *Віктимологічні аспекти злочинності. Кримінологічні дослідження*. 2006. Вип. 1. Луганськ : РВВ ЛДУВС. С. 6–12.

⁴ Бова А. А. Методичні аспекти крос-національних соціологічних опитувань щодо віктимізації та безпеки. *Наука і правоохорона*. 2017. № 1. С. 143–148 ; Бова А. А. Соціологічні опитування потерпілих від злочинів в Україні. *Український соціум*. 2006. № 1 (12). С. 33–41.

Навіть за умови вирішення організаційних, методологічних і фінансових питань віктимологічних моніторингів зберігається проблема упередженості результатів. Показник довіри до соціальних інститутів, що «зчитується» опитуваннями, ґрунтується на особистому досвіді й контенті ЗМІ. Оскільки більшість людей має мінімальний досвід безпосередньої взаємодії з правоохоронцями в межах кримінальних проваджень, визначальним чинником є саме медійний вплив. Це формує додаткове джерело викривлених результатів.

У цьому контексті заслуговує на увагу метод оцінки ефективності протидії злочинності шляхом аналізу витрат і прибутків. Його результати відображають економічну оцінку програм протидії¹. Так, «Perry Preschool Program» – експериментальна ініціатива дошкільного виховання, реалізована в 1960-х роках у місті Іпсіланті (штат Мічиган, США) для дітей із малозабезпечених сімей – передбачала щоденні заняття в класі й щотижневі візити вихователя з акцентом на розвиток когнітивних і соціальних навичок. Первинною метою було підвищення життєвих шансів дітей, однак довгострокове спостереження до 27-річного віку показало зниження рівня злочинності, зростання освітніх і трудових досягнень, а також зменшення залежності від соціальної допомоги. Аналіз витрат і прибутків засвідчив, що кожен інвестований долар приніс понад 7 доларів соціального ефекту (коефіцієнт 7,16:1), а у сфері запобігання злочинності й витрат на правосуддя – 2,16:1².

Іншим прикладом є «Kirkholt Burglary Prevention Project» – комплексна програма ситуаційної профілактики злочинів, реалізована в середині 1980-х у житловому масиві Кірхолт (Рочдейл, Велика Британія), що налічував приблизно 2280 помешкань і характеризувався високим рівнем крадіжок із житла. Перша фаза передбачала заходи, спрямовані на потенційних жертв (укріплення помешкань, усунення можливостей для злочину), друга – роботу з громадою та по-

¹ Manning M. Cost-Benefit Analysis. *Encyclopedia of Criminology and Criminal Justice* / Eds.: G. Bruinsma, D. Weisburd. New York : Springer, 2014. P. 641–651. DOI: https://doi.org/10.1007/978-1-4614-5690-2_176.

² Chisholm J. Benefit-cost analysis and crime prevention. Canberra : Australian Institute of Criminology, 2000. 6 p. (Trends & issues in crime and criminal justice ; no. 147). URL: <https://www.aic.gov.au/publications/tandi/tandi147> (дата звернення: 21.09.2025).

тенційними правопорушниками, включно із системою «сусідського нагляду». Оцінка витрат і вигод показала, що кожен фунт стерлінг приносив приблизно п'ять фунтів економії завдяки скороченню збитків від крадіжок (коефіцієнт 5,04:1). Програма продемонструвала швидкий ефект завдяки фокусуванню на конкретному злочинному ризику в чітко визначеному середовищі¹.

Показовими є й результати «Communities That Care» (CTC) – програми первинної профілактики підліткової злочинності, що реалізовувалася у 24 невеликих містах і селищах США з 2003 по 2012 рік. Вона базувалася на ресурсах місцевих громад і охоплювала п'ятифазний процес: мобілізацію громади, оцінку локальних ризиків і захисних факторів, розробку стратегії, упровадження доказових інтервенцій і постійний моніторинг. Ключовою особливістю є адаптивність до локальних потреб і використання виключно науково підтверджених практик. Довготривалі дослідження засвідчили істотне зниження зловживання психоактивними речовинами й насильства серед молоді. За результатами аналізу витрат і вигод, проведеного «Washington State Institute for Public Policy», кожен долар інвестицій приносив приблизно 8 доларів соціального ефекту (коефіцієнт 8,22:1)².

Звісно, спектр методів оцінювання ефективності протидії злочинності значно ширший: якісні дослідження, експертні опитування, порівняльно-правовий аналіз тощо. Проте всі вони деталізують три ключові напрями – аналіз діяльності органів правопорядку, дослідження рівня відчуття безпеки й баланс соціальних витрат і прибутків.

Отже, отримання об'єктивної, збалансованої та придатної для формування державної політики оцінки потребує поєднання різних

¹ Forrester D., Frenz S., O'Connell M., Pease K. The Kirkholt burglary prevention project: Phase II : Crime prevention unit paper 23. London : Home Office, 1990. VI, 50 p. (Crime Prevention Unit Papers). URL: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0503146df6dfaa3c65ffd4247e84ffa0783b2ba0> (дата звернення: 21.09.2025).

² Benefit-cost analysis of a randomized evaluation of Communities That Care: Monetizing intervention effects on the initiation of delinquency and substance use through grade 12 / M. R. Kuklinski, A. A. Fagan, J. D. Hawkins et al. *Journal of Experimental Criminology*. 2015. Vol. 11, Iss. 2. P. 165–192. DOI: <https://doi.org/10.1007/s11292-014-9226-3>. PMID: 26213527; PMCID: PMC4512954.

методів. Результати обчислювального кримінологічного аргументування необхідно інтерпретувати в контексті даних, отриманих альтернативними методами.

Висновки

Розвиток обчислювального кримінологічного аргументування слід розглядати як етап модернізації кримінально-правової науки в умовах цифрової трансформації. Використання інформаційних технологій для обробки великих масивів даних дає змогу перейти від описового рівня дослідження злочинності до рівня аналітичного. Це означає не лише фіксацію статистичних показників, а й можливість виявлення глибинних закономірностей, оцінки ефективності кримінально-правових заборон, прогнозування ризиків і формування науково обґрунтованих рекомендацій для законодавця та практики.

Застосування цієї методології до українських реалій показало, що результати її використання є не просто аналітично цікавими, а й суспільно значущими. Обчислювальний підхід дав змогу виявити небезпечну тенденцію примітивізації кримінально-правового регулювання, коли правоохоронна система концентрується на простих і процедурно зручних справах, уникаючи складних, але соціально небезпечних викликів. Він також засвідчив, що наймасовішими правопорушеннями є злочини проти власності, структура яких зазнала істотних змін у зв'язку з декриміналізацією. Було виявлено масштабну проблему відповідальності військовослужбовців: зростання кількості засуджених за зберігання наркотиків актуалізує проблему ресоціалізації та психологічної підтримки захисників держави.

Водночас метод має істотні обмеження, які не дають змоги розглядати його як універсальний засіб аналізу злочинності. По-перше, офіційна статистика, що є основним джерелом даних, формується органами, ефективність яких вона ж і відображає, що створює ризик упередженості й викривлень. По-друге, обмежений доступ до пер-

винних даних не дає змоги проводити повноцінні дослідження: для аналізу доступні лише агреговані звіти. По-третє, кількісні методи самі собою не пояснюють соціальної реальності, адже за цифрами приховані складні процеси, що потребують якісного аналізу. Подолати ці обмеження можливо шляхом відкриття доступу до деперсонфікованих первинних даних, удосконалення процесів формування статистики, а також поєднання кількісних досліджень із якісними методами, соціологічними опитуваннями й економічним аналізом ефективності кримінальної політики.

Розділ 7

ШТУЧНИЙ ІНТЕЛЕКТ І КРИМІНАЛЬНЕ ПРАВО

Після завершення Другої світової війни військова авіація США перейшла на реактивні двигуни, що різко підвищило кількість аварій. Причиною виявився проєкт кабіни, створений на основі усереднених параметрів пілотів. На високих швидкостях і під час катапультивання таке рішення ставало фатальним. Звіт для Міністерства оборони США починався питанням: «Чи існує та сама «середня людина»?»¹. У ньому наголошувалося: будь-яка технологія, розрахована на середні розміри, неминуче приречена на провал. Саме так з'явилася концепція індивідуальних налаштувань. Злочин як аварія. Кримінально-правовими засобами ми прагнемо вирвати людину з асоціального падіння. Та через дію закону, що орієнтується на умовного «середнього» суб'єкта, маємо значний ризик, що наші кримінальні «катапульти» ламатимуть людей, а не повертатимуть їх до суспільства.

Сьогодні складно уявити торгівлю без персональних програм лояльності. «Netflix» чи «YouTube» пропонують контент на основі індивідуальних уподобань. Це – приклади аналізу великого масиву даних, які стають основою персоналізації та запорукою результативності.

То чи може застосування кримінального закону в світі персоналізації бути грубим і базуватися на середньостатистичних орієнтирах? Відкритість даних, їх збір і ретельний аналіз можуть наблизити вирішення проблеми. Кардинальне збільшення обсягів інформації, що накопичується під час протидії злочинності, її всебічний аналіз здатні зробити цей процес персоналізованим і сучасним. Це і є головним завданням цифровізації правосуддя. Нині цей процес найчастіше пов'язують зі штучним інтелектом (ШІ).

¹ Daniels G. The «Average Man»? : technical report, accession number AD0010203 / Air Force Aerospace Medical Research Lab. 1977, April 25. URL: <https://apps.dtic.mil/sti/citations/tr/AD0010203> (дата звернення: 21.09.2025).

7.1. Можливості й ризики, які створює штучний інтелект у сфері кримінальної юстиції

За останні два десятиліття ШІ пройшов шлях від абстрактних концептів до прикладних інструментів, що стали буденністю. Системи штучного інтелекту використовуються майже в усіх сферах діяльності людини. Відбулися зміни в науковій рефлексії та правовому регулюванні соціалізації штучного інтелекту.

Сучасні наукові підходи розглядають штучний інтелект як програму, що імітує інтелектуальні функції людини. Така імітація ґрунтується на статистичних методах, відомих як машинне навчання. Загалом воно означає програмування без класичного кодування, а шляхом завантаження великих масивів навчальних даних із правильними прикладами. Система виявляє закономірності й формує моделі, здатні прогнозувати чи приймати рішення в схожих випадках.

Нині великі мовні моделі (LLM) досягають видатних результатів у роботі з текстами, розпізнаванні образів, створенні контенту тощо. Однак попри здатність імітувати людину, вони є лише інструментами для вирішення конкретних завдань.

Тому правове регулювання зосереджується на питаннях застосування, мінімізації ризиків і встановлення меж використання. Для України ця дискусія надактуальна у зв'язку з інтеграцією в глобальні процеси регулювання нових технологій.

Правове врегулювання ШІ перебуває на етапі становлення, розвивається паралельно з активним упровадженням цих систем у різні сфери. Дослідження в Україні та світі охоплюють чимало аспектів, зокрема й використання штучного інтелекту судами та правоохоронцями.

У зарубіжних країнах реалізовані ШІ-проекти, пов'язані з класифікацією та розпізнаванням об'єктів, розпізнаванням звукових сигналів (мови або, наприклад, системи визначення пострілів). Запропоновані технічні рішення для аналізу великих об'ємів даних на основі алгоритмів машинного навчання. Це включає обробку інформації про

телефонні й інтернет-з'єднання, платіжні системи, віртуальні активи. Такі інструменти використовуються під час розслідувань. Додатково створюються системи прогнозування злочинності й оцінки ризику індивідуальної протиправної поведінки.

Розглянемо, які є найбільш поширені практики використання ІІ на правозастосовному й законодавчому рівнях кримінально-правового регулювання. Інтеграція ІІ в судові процеси, зокрема для правової оцінки вчиненого, оцінки ризиків і призначення покарань, а також планування діяльності правоохоронних органів на основі прогнозів злочинності (правозастосовний рівень). Аналіз якості кримінального законодавства, формування пропозицій щодо його вдосконалення на основі оцінки надвеликих обсягів даних щодо соціальних й економічних процесів, діяльності правоохоронних і судових органів (законодавчий рівень).

Оцінка ризиків є ключовим напрямом застосування ІІ на правозастосовному рівні кримінально-правового регулювання. Алгоритми оцінки кримінального ризику використовуються судами для визначення запобіжного заходу чи покарання. Теоретично це знижує упередженість, адже рішення ухвалюються на основі даних, а не лише суддівських переконань.

За даними дослідження Гарвардського університету, понад 20 штатів США використовують алгоритмічні моделі для оцінки ймовірності рецидиву обвинувачених на різних етапах кримінального процесу. Найвідоміший приклад – система COMPAS, що прогнозує ризик повторного злочину й рекомендована судам для обґрунтування рішень про ув'язнення чи реабілітаційні програми. Алгоритми також можуть виявляти потреби засуджених (наприклад, лікування від наркозалежності або психологічна допомога) й рекомендувати відповідні реабілітаційні заходи¹.

Проте застосування ІІ не усуває суб'єктивності, а переносить її в цифрову форму. Відтак разом з очікуваною об'єктивністю виникає

¹ Constitutional dimensions of predictive algorithms in criminal justice / M. Brenner, J. Suk Gersen, M. Haley et al. *Harvard Civil Rights-Civil Liberties Law Review*. 2020. Vol. 55. P. 267–310. URL: <https://journals.law.harvard.edu/crcl/wp-content/uploads/sites/80/2020/09/Brenner-et-al.pdf> (дата звернення: 21.09.2025).

нова складність – упередження, закладені у вихідні дані чи алгоритм. Вони не зникають, а переходять у технологічну площину й можуть посилюватися.

Оскільки алгоритми ґрунтуються на попередніх рішеннях, вони здатні закріплювати й відтворювати упередженість, генеруючи ще більшу кількість викривлених даних для наступних циклів рішень¹. Наприклад, якщо перед суддею особа з невеликим доходом, алгоритм із дуже великою імовірністю радитиме застосувати ув'язнення до суду. Наступного разу в подібній ситуації алгоритм буде ще категоричніший, наступного – ще й ще... Така небезпека зумовлює критичну необхідність прозорості й можливості незалежної перевірки ШІ-систем². Алгоритми, навчені на історичних даних, можуть успадковувати структурну упередженість кримінальної статистики, де непропорційно високий рівень арештів окремих меншин призводить до хибних прогнозів щодо них у майбутньому³.

Для зниження ризиків алгоритмічної упередженості використовується пояснюваний ШІ (explainable AI), який дає змогу не лише отримати прогноз, а й зрозуміти, на яких факторах та ознаках він базується. Так, було представлено модель передбачення строків ув'язнення у справах про напад у судах Нової Зеландії. Система продемонструвала середню похибку менш ніж рік і водночас дала змогу виокремити ключові слова та фрази, що найбільше впливали на тривалість покарання. Подібне пояснюване представлення дає змогу судді бачити, які параметри система вважає релевантними, виявляти потенційно помилкові зв'язки й уникати ефекту «чорної скриньки» під час ухвалення рішень. Дослідники підкреслюють: штучний інтелект не повинен автоматизувати винесення вироків, проте може ви-

¹ Hao K. AI is sending people to jail – and getting it wrong. *MIT Technology Review*. 2019, January 21. URL: <https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/> (дата звернення: 21.09.2025).

² Sanger R. Artificial intelligence and criminal law. *The Colleges of Law*. 2024, January 12. URL: <https://www.collegesoflaw.edu/blog/2024/01/12/artificial-intelligence-and-criminal-law/> (дата звернення: 08.08.2025).

³ Faulkner A. From case law to code: Evaluating AI's role in the justice system. *Montreal AI Ethics Institute*. 2025, May 26. URL: <https://montrealethics.ai/from-case-law-to-code-evaluating-ais-role-in-the-justice-system/> (дата звернення: 19.08.2025).

користуватися як допоміжний інструмент для перевірки та вдосконалення судових рішень¹.

Ще одним напрямом використання ШІ в судах є забезпечення єдності практики. ШІ може підвищити якість судових рішень, аналізуючи великі обсяги судової практики й наявні правові позиції. Це допоможе суддям приймати обґрунтовані рішення та скорочувати час розгляду справ. Публічно представлені плани створення судів, де значну частину рутинних судових процедур буде автоматизовано. Звичайно, повна автоматизація правосуддя наразі є радше теоретичною можливістю; на практиці підхід полягає у використанні ШІ під наглядом людини. Найбільш реалістичним є використання алгоритмів як допоміжного інструменту для суддів².

Водночас у сучасній дискусії наголошується, що однаковість вироків (як результат алгоритмізації) не завжди має однозначно позитивне значення. Як підкреслює Й. Рюберг, принцип «подібні випадки – подібні вирoki» може бути етично небезспірним: з погляду консеквенціалізму відмінність у вироків іноді здатна забезпечити кращі соціальні наслідки, а з погляду ретрибутивізму важливим є не лише відносна, а й абсолютна пропорційність покарання. Якщо правова система загалом схильна до надмірного покарання, то відхилення від усталених практик у бік пом'якшення може виявитися більш справедливим, аніж суворе дотримання формальної однаковості³.

Окрім того, єдність практики через використання ШІ може бути проявом нових системних упереджень. Статистична «природа» ШІ вимагає постійної критичної оцінки результатів через небезпеку так званих конфабуляцій (галюцинацій) ШІ, випадків, коли відповідь генерується на помилкових статистичних припущеннях.

¹ Rodger H., Lensen A., Betkier M. Explainable artificial intelligence for assault sentence prediction in New Zealand. *Journal of the Royal Society of New Zealand*. 2022. Vol. 53, Iss. 1. P. 133–147. DOI: <https://doi.org/10.1080/03036758.2022.2114506>. PMID: 39439993; PMCID: PMC11459755.

² Ryberg J. Criminal sentencing and artificial intelligence: What is the input problem? *Criminal Law and Philosophy*. 2025. Vol. 19. P. 203–220. DOI: <https://doi.org/10.1007/s11572-024-09739-2>.

³ Ryberg J. Criminal sentencing and artificial intelligence: What is the input problem?

Наприклад, дослідження «Stanford RegLab» та «Stanford HAI» показало, що навіть провідні спеціалізовані юридичні ШІ-інструменти, побудовані на технології «retrieval-augmented generation» (RAG), не гарантують відсутності помилок. Аналіз роботи Lexis + AI, Westlaw AI-Assisted Research та Ask Practical Law AI продемонстрував, що від 17 до понад 34% відповідей містили помилки – від створення вигаданих судових прецедентів і норм права до некоректної інтерпретації чинного законодавства й помилкових цитувань. Особливо небезпечним виявилося явище підлаштування під помилкові припущення користувача (sysorphanancy), коли система не лише не спростовує хибну передумову, а й підкріплює її додатковою, але недостовірною аргументацією¹.

Ще однією проблемою використання ШІ при розгляді справ у суді є так звана «input problem» – складності адекватного введення всієї релевантної інформації про злочин в алгоритм. Для винесення справедливих вироків часто важливі тонкощі справи й особи обвинуваченого, які складно структурувати у формальних параметрах. Дослідники застерігають, що спрощене кодування реальності злочину може призвести до втрати контексту й індивідуальної справедливості. Тобто навіть якщо алгоритм позбавлений людських упереджень, він може помилитися через обмежені або неправильно інтерпретовані вхідні дані².

Тому використання ШІ для забезпечення єдності судової практики слід розглядати в контексті питання, чи ШІ забезпечує справжню справедливість, чи алгоритмізація лише стандартизує рішення на основі потенційно недосконалих даних.

Подібні проблеми існують і під час упровадження систем прогнозування злочинності³. Наприклад, досвід британської поліції

¹ Hallucination-free? Assessing the reliability of leading AI legal research tools / V. Magesh, F. Surani, M. Dahl et al. *Journal of Empirical Legal Studies*. 2025. Vol. 22, Iss. 2. P. 216–242. DOI: <https://doi.org/10.1111/jels.12413>.

² Ryberg J. Criminal sentencing and artificial intelligence: What is the input problem?

³ Trejo O. What is Bias in machine learning? Real-world examples that show the impact of AI Bias. *Scalable Path*. Originally published on May 4, 2020, last updated on August 28, 2024. URL: <https://www.scalablepath.com/machine-learning/bias-machine-learning> (дата звернення: 21.09.2025).

свідчить, що алгоритмічні інструменти прогнозування повторної злочинності інституціоналізують індивідуально орієнтовану стратегію «загроза-школа-ризик» і стають обов'язковою точкою проходження в прийнятті управлінських рішень¹. Ідея полягає в тому, що на підставі аналізу даних про зареєстровані кримінальні правопорушення системи визначають райони, що потребують посиленої уваги правоохоронців. У ці райони направляється більша кількість патрулів, чим має забезпечуватися ефективніше використання ресурсів і досягатися необхідний рівень безпеки громадян.

Результати впровадження таких системи показали зворотний бік проблеми. Що більше поліцейських направлялося в заданий район, то більшою була кількість виявлених у цьому районі правопорушень. Алгоритм фіксував прийняте рішення як правильне та продовжував рекомендувати посилені наряди для визначених районів². У такий спосіб увічнювався «кримінальний» статус таких районів, але загальне використання ресурсів поліції не ставало більш ефективним, загальний рівень безпеки громадян не підвищувався. Так званий ефект «зворотної петлі» (feedback loop) є тоді, коли підвищена увага поліції до «прогнозованих» районів призводить до ще більшої реєстрації там злочинів і, як наслідок, подальшого укріплення хибного прогнозу³.

Щоб оцінити упередженість поліцейського прогнозування, Група аналізу даних з прав людини (HRDAG) проаналізувала зареєстровані поліцейським управлінням Окленду злочини, пов'язані з наркотиками. Управління використовувало спеціальний алгоритм обробки великих

¹ Marciniak D. Algorithmic policing: an exploratory study of the algorithmically mediated construction of individual risk in a UK police force. *Policing and Society*. 2023. Vol. 33, Iss. 4. P. 449–463. DOI: <https://doi.org/10.1080/10439463.2022.2144305>.

² Див.: Runaway feedback loops in predictive policing / D. Ensign, S. A. Friedler, S. Neville et al. *Proceedings of Machine Learning Research*. 2018. Vol. 81 : Proceedings of the 1st Conference on Fairness, Accountability and Transparency. P. 160–171. URL: <https://proceedings.mlr.press/v81/ensign18a.html> (дата звернення: 21.09.2025) ; Hung T. W., Yen C. P. Predictive policing and algorithmic fairness. *Synthese*. 2023. Vol. 201, Iss. 3. P. 1–25. DOI: <https://doi.org/10.1007/s11229-023-04189-0>.

³ Joh E. E. The new surveillance discretion: Automated suspicion, big data, and policing. *Harvard Law & Policy Review*. 2016. Vol. 10. P. 15–42 ; Ferguson A. G. The rise of big data policing : Surveillance, race, and the future of Law enforcement. New York : New York University Press, 2017. DOI: <https://doi.org/10.2307/j.ctt1pwtb27>.

даних для прогнозування наркозлочинів. Звичайно, HRDAG виявила, що прогностична модель майже виключно зосередилася на неспроєднаних спільнотах із низьким рівнем доходу. Але дані громадської охорони здоров'я щодо споживачів наркотиків у поєднанні з даними перепису населення США показали, що розподіл споживачів наркотиків не корелює з прогнозами програми, демонструючи, що прогноз алгоритму ґрунтувався на упередженості, а не на реальності¹.

Показовим є те, що в червні 2020 року міська рада Санта Круз, американського міста, яке одним із перших почало застосовувати для потреб поліції технології розпізнавання обличчя та прогнозування злочинів, відмовилася від використання таких систем, зважаючи на численні прояви упередженості їх роботи й недостатню ефективність. Рішення полягало в забороні використовувати обидві технології, за винятком схвалення міською радою на основі «висновків про те, що технологія і дані, які використовуються для цієї технології, відповідають науково підтвердженим та рецензованим дослідженням, захищають і охороняють цивільне населення, права і свободи всіх людей і не увічнюють упередженість»².

Перспективи використання ШІ на законодавчому рівні кримінально-правового регулювання пов'язані насамперед з інформаційним супроводженням удосконалення кримінального законодавства. ШІ тут не «ламає» традиційний підхід, а масштабує та поглиблює звичайні аналітичні задачі законотворчості. Використання ШІ в процесі вдосконалення законодавства є не так революційним проривом, як логічним розвитком традиційних інформаційних технологій (ІТ), які застосовувалися протягом десятиліть.³ Як і раніше, під час підготовки проєктів законів оцінюють статистику злочинності, економічні й демографічні тренди, ефективність правозастосування. Різниця в тому,

¹ Lum K., Isaac W. To predict and serve? *Significance*. 2016. Vol. 13, Iss. 5. P. 14–19. DOI: <https://doi.org/10.1111/j.1740-9713.2016.00960.x>.

² Ibarra N. Santa Cruz becomes first U. S. city to approve ban on predictive policing. *Santa Cruz Sentinel*. 2020, June 25. URL: <https://www.santacruzsentinel.com/2020/06/23/santa-cruz-becomes-first-u-s-city-to-approve-ban-on-predictive-policing/> (дата звернення: 21.09.2025).

³ Berk R. Demystifying AI in criminal justice. *arXiv*. 2025, July 28. 25 p. DOI: <https://doi.org/10.48550/arXiv.2507.19305>.

що ШІ дає змогу робити це на якісно іншому рівні – опрацьовувати масиви даних, які раніше були фактично непідйомними, і швидко зводити їх у релевантні висновки для законодавця.

Автори дослідження Європейської комісії «Drafting legislation in the era of AI and digitisation» наголошують, що використання штучного інтелекту в нормопроектванні здатне забезпечити якісніші тексти законів, швидший процес підготовки й вищий рівень узгодженості нормативних актів, однак воно можливе лише за умови гібридного підходу зі збереженням людського контролю. Використання концепції «машиночитаного права» (machine-consumable law) у сфері кримінального законодавства дає змогу проводити автоматизовану перевірку узгодженості між статтями КК. Завдяки інструментам аналізу великих масивів даних ШІ може моделювати наслідки криміналізації або декриміналізації певних діянь, урахуовуючи статистику правозастосування, соціальні й економічні фактори. Це забезпечує більш обґрунтоване прийняття рішень у процесі внесення змін до кримінального законодавства¹.

Сучасні дослідження підкреслюють, що впровадження штучного інтелекту в державному управлінні пов'язане не лише з технологічними можливостями, а й з організаційними та етичними чинниками. Як показують результати аналізу кейсів публічного сектору в різних країнах, найбільш поширеними є застосування ШІ для автоматизації процесів, предиктивної аналітики, обробки великих масивів документів й аналізу громадських настроїв. Водночас дослідники наголошують на необхідності балансування між ефективністю, прозорістю та дотриманням прав людини, що вимагає розбудови належних механізмів управління даними й алгоритмів, що відповідають вимогам пояснювальних ШІ².

¹ Palmirani M., Vitali F., Van Puymbroeck W., Durango F. N. Drafting legislation in the era of AI and digitisation. Brussels : European Commission, Directorate-General for Informatics, 2022. 96 p. URL: <https://interoperable-europe.ec.europa.eu/sites/default/files/document/2022-06/Drafting%20legislation%20in%20the%20era%20of%20AI%20and%20digitisation%20-%20study.pdf> (дата звернення: 21.09.2025).

² Noordt C. van, Misuraca G. Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union. *Government Information Quarterly*. 2022. Vol. 39, Iss. 3. Art. 101714. DOI: <https://doi.org/10.1016/j.giq.2022.101714>.

Отже, системи ШІ мають значні перспективи для раціоналізації кримінально-правового регулювання. Ці перспективи супроводжуються не менш небезпечними ризиками. Розмову про ШІ в кримінальній юстиції ми почали з історії про «середню людину» й найочевиднішу задачу кримінального права – індивідуалізацію впливу. ШІ здатен бути інструментом її розв’язання. Водночас від людей, політиків, законодавців залежить, чи буде ШІ використовуватися для підвищення ефективності кримінальної юстиції шляхом персоналізації впливу, чи відбуватиметься подальше алгоритмічне усереднення рішень, орієнтованих на «середніх» людей.

Саме алгоритмічне усереднення у сфері кримінальної юстиції становить, на нашу думку, найсерйознішу небезпеку застосування ШІ. Коли система починає орієнтуватися не на конкретну особу з її унікальними обставинами, а на «усереднений» профіль злочинця, відбувається тотальне вирівнювання правосуддя. Таке правосуддя втрачає сенс індивідуалізації покарання та перетворюється на механічне застосування шаблонів. У цьому полягає ризик зведення складної правової реальності до статистичної формули: людина починає сприйматися не як індивід, а як представник певної статистичної групи.

Як слушно застерігає Р. Йоргенсен, відбувається перетворення провини на «злочин належності до референтного класу», що суперечить фундаментальному праву кожного бути розглянутим як особистість, а не як середньостатистичний носій характеристик групи¹. Подібна «усереднена справедливість» фактично руйнує базові принципи кримінального права: покарання перестає бути результатом індивідуальної оцінки та стає лише математичною функцією.

Дослідження студентів Гарвардської школи права про використання відомого ШІ-інструмента оцінки ризиків у сфері кримінального правосуддя COMPAS показало, що його стандартизовані алгоритмічні оцінки відтворювали приховані расові упередження. У результаті «вирівнювання» не лише нівелює індивідуальні обставини, а й

¹ Jorgensen R. Algorithms and the individual in criminal law. *Canadian Journal of Philosophy*. 2022. Vol. 52, Iss. 1. P. 61–77. DOI: <https://doi.org/10.1017/can.2021.28>.

поглиблює соціальну несправедливість, закріплюючи дискримінаційні практики¹.

На думку Р. Тітах, ще небезпечніше, коли судді починають беззастережно довіряти інструментам ШІ, «зрікаючись власної відповідальності» й підмінюючи людське судження алгоритмом². Такий підхід формує систему, де індивідуалізація зникає, а рішення уніфікуються за логікою машинної «справедливості», яка не враховує багатовимірність людської поведінки. Це призводить до ситуації, яку можна назвати «алгоритмічним конвеєром покарання» – системи, здатної швидко ухвалювати рішення, але нездатної бути справедливою.

7.2. Правове регулювання використання штучного інтелекту

Значущість використання ШІ, його потенційні можливості, але водночас і масштаб ризиків зумовлюють питання щодо правового регулювання використання технологій ШІ.

Як правильно зазначає Р. Берк, прогнозування злочинів за допомогою ШІ за належного використання здатне зробити правоохоронну діяльність «більш точковою» і раціональною. Водночас абсолютно уникнути компромісів між точністю прогнозу, справедливістю і прозорістю неможливо – «не можна мати все й одразу», тож оптимальний баланс між безпекою і правами має вироблятися політичними та правовими рішеннями³.

¹ Hua R. AI and racial Bias in legal decision-making: A student fellow project. *Harvard Law School*. 2025, March 19. URL: <https://clp.law.harvard.edu/knowledge-hub/insights/ai-and-racial-bias-in-legal-decision-making-a-student-fellow-project/> (дата звернення: 21.09.2025).

² Titah R. How AI skews our sense of responsibility. *MIT Sloan Management Review*. 2024, May 13. URL: <https://sloanreview.mit.edu/article/how-ai-skews-our-sense-of-responsibility/> (дата звернення: 21.09.2025).

³ Berk R. A. Artificial intelligence, predictive policing, risk assessment for law enforcement. *Annual Review of Criminology*. 2021. Vol. 4. P. 209–237. DOI: <https://doi.org/10.1146/annurev-criminol-051520-012342>.

Збройна агресія росії пришвидшила впровадження технологій штучного інтелекту в діяльність національних правоохоронних структур. Розслідування воєнних злочинів, виявлення колаборантів, боротьба з пропагандою на користь агресора потребують швидкої обробки значних масивів даних. Для цього активно застосовуються системи розпізнавання, відеоаналітика, транскрибування аудіо- й відеозаписів. Водночас відсутність належного правового регулювання та організаційно-технічних механізмів дотримання нормативних приписів під час використання штучного інтелекту правоохоронними органами може спричинити масштабні порушення прав людини й ускладнити євроінтеграційні процеси та взаємодію України з міжнародними партнерами.

Як рівні сучасної системи правового регулювання штучного інтелекту, на нашу думку, слід розглядати: метарівень, стратегічний рівень, тактичний рівень. Якщо стратегічний рівень окреслює довгострокові напрями розвитку ШІ, а тактичний забезпечує нормативне реагування на поточні ризики, то метарівень відповідає за осмислення цілей, соціального призначення та відповідності ШІ-систем людським цінностям¹.

Метарівень пов'язаний із проблемою невизначеності (alignment problem) і нечіткості людських цінностей. Ми намагаємося регулювати технологію, якій теоретично доведеться приймати рішення на основі наших суспільних цінностей і пріоритетів, але водночас:

- 1) ми часто не можемо досягти консенсусу щодо цих цінностей і пріоритетів у суспільстві;
- 2) чимало наших соціальних норм є неявними, фрагментарними, складно формалізуються;
- 3) наші уявлення про «ідеальне суспільство», про те, як має «працювати» той або інший соціальний інститут, містять внутрішні суперечності.

Це породжує парадокс: ми вимагаємо від ШІ дотримуватися «людських цінностей», але самі не можемо чітко артикулювати, що це

¹ Карчевський М. В., Карчевська О. В. Структурний вимір правового регулювання ШІ. *Український політико-правовий дискурс*. 2025. № 12. DOI: <https://doi.org/10.5281/zenodo.15782211>.

означає в кожному конкретному контексті. Крім того, дані, на яких навчається ШІ, – це дзеркало нашого недосконалого суспільства з усіма його упередженнями й суперечностями.

С. Рассел стверджує, що традиційна – так звана стандартна модель ШІ – базується на припущенні про наявність чітко визначеної мети, якої має досягати система. Проте в реальному світі таке припущення є хибним: люди рідко можуть формалізувати свої цілі повністю, послідовно й без суперечностей. Людські орієнтири змінюються, часто є багатозначними або навіть несвідомими. За таких умов застосування потужних ШІ-систем, орієнтованих на фіксовані цілі, може не тільки не допомогти, а й спричинити втрату контролю. Машини, що впевнено переслідують неправильно задані цілі, можуть завдати значної шкоди. Тому модель ототожнення інтелекту зі здатністю обирати дії, які призведуть до досягнення цілей, С. Рассел називає непрацездатною для подальшого прогресу технологій ШІ. Він пропонує нову модель, у якій невпевненість машини щодо справжньої мети призводить до якісно нових способів поведінки, які є більш надійними¹.

Проблемою узгодженості (alignment problem) називає Б. Крістіан концептуальну та практичну невідповідність між тим, що насправді хоче людина, і тим, що система машинного навчання виконує на основі заданої мети або формалізованих інструкцій. Як слушно зазначає дослідник, зі зростанням складності й автономності ШІ-систем критично важливо забезпечити, щоб вони «вловлювали наші норми та цінності, розуміли те, що ми маємо на увазі, і насамперед робили те, чого ми насправді хочемо»². Ця проблема стає актуальнішою через те, що люди не здатні чітко сформулювати свої цілі, норми або критерії справедливості. Так з'являються рекомендаційні алгоритми, що підсилюють стереотипи й поляризацію, системи розпізнавання зображень, які демонструють расову упередженість тощо³. Дослідник

¹ Russell S. Artificial intelligence and the problem of control. *Perspectives on digital humanism* / Eds.: H. Werthner, E. Prem, E. A. Lee, C. Ghezzi. Springer, 2022. P. 19–24. DOI: https://doi.org/10.1007/978-3-030-86144-5_3.

² Christian B. The alignment problem : How can machines learn human values? Atlantic Books, 2021. P. 20.

³ Christian B. The alignment problem : How can machines learn human values? P. 31–32.

небезпідставно наполягає на тому, що проблема узгодженості не лише технічна, а насамперед ціннісна. Вона вимагає переосмислення взаємодії між алгоритмами та суспільством і передбачає міждисциплінарний підхід, що об'єднує юриспруденцію, етику, соціальні науки й інформатику.

На проблемі відсутності чіткості, стабільності та внутрішньої узгодженості людських цілей наголошує і Н. Бостром. Він зазначає, що навіть у гіпотетично ідеальному суспільстві з необмеженими ресурсами, досконалою координацією та автоматизованими засобами досягнення будь-яких результатів ми все одно стикнемося з «аксіологічними контурами». Це внутрішні обмеження, які випливають із самої структури людських цінностей. Наприклад, частина наших прагнень є позиційними за своєю природою, вони визначаються не абсолютними результатами, а положенням у соціальній ієрархії (наприклад, бажання бути найкращим чи єдиним у чиемусь житті). Жодна система, навіть досконала, не зможе одночасно задовольнити всіх у таких бажаннях, бо вони суперечать одне одному за своєю суттю. Моральні переконання можуть самі собою забороняти певні дії, навіть якщо вони технічно можливі й мали б принести бажані результати. Н. Бостром переконливо показує, що не тільки технології мають бути узгоджені з людськими цілями, а й самі цілі – вивчені, усвідомлені та структуровані. Поки цього не досягнуто, ризик дезорієнтації і навіть екзистенційної кризи від використання ШІ є надзвичайно високим¹.

Тому на метарівні має здійснюватися аналіз того, для чого в кінцевому рахунку створюється та впроваджується конкретна технологія ШІ, яку проблему вона має вирішити, яким цінностям сприяти, і які ризики для суспільних пріоритетів вона може генерувати. В умовах, коли навіть самі людські цілі часто є неявними, суперечливими або нефіксованими у правових інститутах, метарівень виконує функцію узгодження змісту правового регулювання з реальними потребами людини й суспільства.

¹ Bostrom N. Deep Utopia: Life and meaning in a solved world. Ideapress Publishing, 2024. 525 p.

Потреба в метарівні актуалізується в практичних кейсах упровадження ШІ. Як показує приклад розробки системи «CrimeDataLab», недосконалість, фрагментарність та упередженість масивів даних (у нашому випадку – різні цілі статистичного спостереження ОГП і ДСА) може не лише знецінити потенціал технологій, а й створити хибне уявлення про ситуацію, яку ці технології мають відображати. У такому випадку питання не зводиться лише до правових дозволів і заборон, а потребує глибшої перевірки на відповідність соціальному сенсу, етичним орієнтирам і справедливості.

Отже, метарівень є ключовим для забезпечення інтегрованого, людиноцентричного підходу до правового регулювання ШІ, адже саме він дає змогу встановлювати взаємозв'язок між технологічним рішенням і його фактичним внеском у суспільне благо. Стосовно правового регулювання ШІ у сфері кримінальної юстиції метарівень, на нашу думку, необхідно визначати так: *використання ШІ у сфері кримінальної юстиції здійснюється для максимальної індивідуалізації кримінально-правового впливу на основі аналізу великих обсягів релевантних даних.*

Індивідуальний підхід, підкріплений даними ШІ, дає змогу забезпечити справедливіше ставлення до кожного злочинця та цільове витрачання ресурсів на заходи, які дійсно необхідні саме цій особі, замість застосування усереднених санкцій. Як показують дослідження, правильно налаштовані алгоритми можуть допомогти сконцентрувати зусилля там, де це дасть найбільший суспільний ефект, уникаючи ситуації, коли когось карають суворіше лише через належність до певної статистичної групи¹.

Стратегічний рівень зосереджується на довгострокових викликах і гіпотетичних сценаріях розвитку ШІ, таких як поява автономного інтелекту, трансгуманізм, формування нових форм юридичної відповідальності та «юстиції штучного інтелекту». Основна мета цього рівня – визначення загальних координат для правового осмислення

¹ Jorgensen R. Algorithms and the individual in criminal law ; DOJ report on AI in criminal justice: key takeaways. *Council on Criminal Justice*. 2025, April. URL: <https://counciloncj.org/doj-report-on-ai-in-criminal-justice-key-takeaways/> (дата звернення: 21.09.2025).

соціалізації технологій, зокрема з урахуванням технологічної нейтральності, необхідності конвергенції технічних і юридичних наук, а також переосмислення правового статусу і людей, і машин.

Можливо, найбільше дискусій тут викликає проблема суб'єктності. Ш. О. Баранов зазначав, що теоретичні погляди на юридичний статус штучного інтелекту загалом поділяються на негативну теорію, позитивну й теорію компромісу. Негативна теорія полягає в розгляді ШІ виключно як об'єкта правових відносин. Позитивна теорія стверджує, що ШІ повинен мати статус суб'єкта права (фіктивна особистість, електронна особистість, ШІ – суб'єкт злочину¹ тощо). Теорія компромісу – штучний інтелект повинен мати кваліфікацію суб'єкта права, але з обмеженою правосуб'єктністю. Також дослідник пропонує власний погляд – теорію доцільності. Вона полягає в тому, що «залежно від ситуаційної доцільності застосування спеціалізованого робота із ШІ для заміни праці або діяльності традиційного суб'єкта він може бути об'єктом або суб'єктом правовідносин»².

Поділяючи позицію шановного колеги, вважаємо, що відповідь на стратегічне питання правового регулювання ШІ – об'єкт чи суб'єкт відносин – необхідно шукати в площині фактичного існування. Проблематика ШІ тісно пов'язана з гіпотетичними концепціями майбутніх технологій. Водночас правове регулювання забезпечує впорядкування суспільних відносин, пов'язаних із технологіями, що існують реально.

Однією з поширених класифікацій систем ШІ є їх поділ на «вузький (слабкий) ШІ» (ANI), «загальний (сильний) ШІ» (AGI) та «штучний суперінтелект» (ASI).

Слабкий штучний інтелект – *фактично* наявні технології, орієнтовані на автоматизацію певних видів діяльності людини або кількох завдань, які вона виконує. Наприклад, керування транспортним засобом, гра в шахи, розпізнавання обличчя, голосу, рукописного тексту тощо.

¹ Див., наприклад: Радутний О. Штучний інтелект як суб'єкт кримінального права. *Право України*. 2018. № 1. С. 123. DOI: <https://doi.org/10.33498/loiu-2018-01-123>.

² Баранов О. Штучний інтелект і система права : монографія / Ін-т інформації, безпеки і права Нац. акад. прав. наук України. Київ ; Одеса : Фенікс, 2025. С. 283–284.

Сильний штучний інтелект є *гіпотетичним* пристроєм, який має здатність мислити, усвідомлювати оточуючий світ і себе як особистість, виконувати всі завдання, як і людина, або навіть перевищувати її інтелектуальні здібності¹. Сильний ШІ (AGI) – *концепт, його реалізація можлива в майбутньому, але наразі системи загального інтелекту не існують*². У науці немає консенсусу щодо визначення таких систем, тому заради комерційних цілей технологічні компанії часто роблять повідомлення про те, що їх системи ШІ демонструють «спалахи AGI», окремі ознаки тощо. У ситуації термінологічної невизначеності й відсутності впевненого підтвердження існування таких технологій, можливості правового регулювання AGI видаються сумнівними³.

Штучний суперінтелект (ASI) перевершує людський інтелект, здатен краще за людину приймати високоякісні рішення, які враховують більше інформації та подальшу перспективу розвитку в часі⁴. ASI «*все ще є значною мірою теоретичним і залишається предметом дискусій та спекуляцій*»⁵.

Отже, для визначення стратегічного рівня правового регулювання ШІ ми пропонуємо орієнтуватися на аналіз технічних рішень, які існують реально. Зараз це системи ШІ, що виконують вузькі задачі під людським контролем і на основі даних, завантажених людьми. Саме системи ANI фактично представлені у сфері кримінальної юстиції. Відповідно, правове регулювання використання ШІ у сфері кримі-

¹ What is strong AI? IBM. URL: <https://www.ibm.com/think/topics/strong-ai> (дата звернення: 22.08.2025).

² The risks associated with Artificial General Intelligence: A systematic review / S. McLean, G. J. M. Read, J. Thompson et al. *Journal of Experimental & Theoretical Artificial Intelligence*. 2021. Vol. 35, Iss. 5. P. 649–663. DOI: <https://doi.org/10.1080/0952813X.2021.1964003>.

³ Leffer L. In the race to artificial general intelligence, where's the finish line? *Scientific American*. 2024, June 25. DOI: <https://doi.org/10.1038/scientificamerican032025-5u0fPrUaVI3TKyo4zEF29s>.

⁴ Russell S. Q & A: The future of artificial intelligence. *UC Berkeley. Electrical Engineering and Computer Sciences*. URL: <https://people.eecs.berkeley.edu/~russell/research/future/q-and-a.html> (дата звернення: 21.09.2025).

⁵ What is artificial general intelligence (AGI)? *Google Cloud*. URL: <https://cloud.google.com/discover/what-is-artificial-general-intelligence> (дата звернення: 22.08.2025).

нальної юстиції передбачає розгляд таких систем виключно як об'єктів права.

Тактичний рівень охоплює регулювання наявних і впроваджених ІІІ-систем, що використовуються в конкретних сферах, зокрема правоохоронній діяльності. Він передбачає реагування на наявні ризики. Регуляторні рішення на цьому рівні ґрунтуються на класифікації ризиків, вимогах до прозорості, змісті навчальних наборів даних, визначенні меж використання технологій ІІІ тощо.

Фахівці виокремлюють чотири основні групи ризиків застосування штучного інтелекту: приватність, маніпулятивний вплив, упереженість, непрозорість¹. Питання їх подолання формують основу сучасної наукової дискусії щодо правового регулювання ІІІ.

Нова якість втручання в приватне життя. Автоматизована обробка даних про особу створює принципово інший рівень загроз приватності. Аналіз уподобань у соціальних мережах², історії покупок³, інтернет-з'єднань⁴ із використанням технологій штучного інтелекту здатний суттєво порушити таємницю приватного життя конкретної людини.

Маніпулювання поведінкою. Технології штучного інтелекту сьогодні істотно впливають на поведінку споживачів шляхом таргетованої реклами, індивідуалізованих рекомендацій пошукових сервісів, персоналізованих стрічок новин тощо. Значною є небезпека маніпуляцій із використанням штучного інтелекту в політичній діяльності⁵.

¹ Dupont B., Stevens Y., Westermann H., Joyce M. Artificial intelligence in the context of crime and criminal justice : A report for the Korean Institute of Criminology. 2018, December. P. 24–28. URL: <https://www.researchgate.net/publication/337402608> (дата звернення: 21.09.2025).

² Kosinski M., Stillwell D., Graepel T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*. 2013, March 11. Vol. 110, No. 15. P. 5802–5805. DOI: <https://doi.org/10.1073/pnas.1218772110>.

³ Hill K. How target figured out a teen girl was pregnant before her father did. *Forbes*. 2012, February 16. URL: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> (дата звернення: 21.09.2025).

⁴ Zalnieriute M. Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law*. 2022. Vol. 116, Iss. 3. P. 585–592. DOI: <https://doi.org/10.1017/ajil.2022.35>.

⁵ Yuval Noah Harari argues that AI has hacked the operating system of human civilisation. *The Economist*. 2023, April 28. URL: <https://www.economist.com/by-invita->

Існує навіть спеціальний термін «астротурфінг»¹, яким позначають імітацію громадської підтримки ініціатив².

Дискримінація. Унаслідок особливостей машинного навчання, що є в основі штучного інтелекту, недостатня якість даних, використаних при створенні системи, здатна спричиняти системні помилки її роботи. Класичним прикладом такої проблеми є упередженість автоматизованих інструментів відбору кадрів. «Навчальні» масиви даних зазвичай формуються на основі відомостей про успішні рішення у сфері рекрутингу. Оскільки цей процес у багатьох випадках не є гендерно нейтральним, виникали ситуації запуску систем, що під час використання відтворювали й навіть посилювали гендерну нерівність³.

Непрозорість, проблема «чорної скриньки». Правові механізми захисту інтелектуальної власності й конкурентна боротьба на IT-ринку зумовлюють закритість алгоритмів систем штучного інтелекту, що внеможливорює перевірку коректності рішень і дієвий контроль за їх функціонуванням. У сферах, де хибна робота систем здатна спричинити значні збитки, це створює серйозні ризики.

Означені загрози стосуються не лише правоохоронної діяльності. Накопичений досвід і «критична» маса небезпек від неконтрольованого поширення систем штучного інтелекту є підґрунтям для законодавчих ініціатив, спрямованих на формування комплексної норматив-

tion/2023/04/28/yuval-noah-harari-argues-that-ai-has-hacked-the-operating-system-of-human-civilisation (дата звернення: 21.09.2025) ; Guggenberger N., Salib P. N. From fake news to fake views: New challenges posed by ChatGPT-like AI. *Lawfare*. 2023, January 20. URL: www.lawfaremedia.org/article/fake-news-fake-views-new-challenges-posed-chatgpt-ai (дата звернення: 21.09.2025).

¹ Badade A. B., Dhanaraj R. K. Astroturfing: understanding and addressing the influence of fake grassroots movements across diverse domains on social media platforms. *Proceedings of Fourth International Conference on Computing and Communication Networks. ICCCN 2024* / Eds.: A. Kumar, A. Swaroop, P. Shukla. Springer, Singapore, 2025. P. 527–538. (Lecture Notes in Networks and Systems ; Vol. 1317). DOI: https://doi.org/10.1007/978-981-96-3942-7_40.

² Dupont B., Stevens Y., Westermann H., Joyce M. Artificial intelligence in the context of crime and criminal justice. P. 45.

³ O'Connor S., Liu H. Gender bias perpetuation and mitigation in AI technologies: challenges and opportunities. *AI & Society*. 2024. Vol. 39. P. 2045–2057. DOI: <https://doi.org/10.1007/s00146-023-01675-4>.

но-правової основи для відповідального розвитку ШІ, захисту базових прав і підтримки інновацій. Серед найбільш значущих варто назвати європейський «Artificial Intelligence Act» (AIA)¹.

AIA визначає «систему ШІ» як машинну систему, що здатна працювати з різними рівнями автономності, виявляти адаптивність після впровадження та на основі отриманих даних робити висновки для досягнення явних або неявних цілей. Такі висновки можуть набувати форми прогнозів, створеного контенту, рекомендацій або рішень, що впливають на фізичне чи віртуальне середовище.

Це визначення забезпечує відмежування систем ШІ від традиційних програмних продуктів. На відміну від звичайних програм, які виконують заздалегідь визначені алгоритми, системам ШІ властиві здатність до висновків і моделювання на основі даних, а також автономність і самонавчання (адаптивність), які дають змогу системі змінюватися під час використання.

Акцент на «явних і неявних цілях» є відображенням згаданої раніше *alignment problem*. Він підкреслює, що система ШІ може діяти не лише відповідно до безпосередньо закладених розробником завдань, а й реалізовувати приховані або похідні цілі, які виникають у процесі навчання чи оптимізації. Урахування неявних цілей дає змогу поширити регуляцію на ризики, що виникають не лише через офіційно проголошені функції, а й від тих, які виявляються у фактичній поведінці системи. Наприклад у сфері медицини система підтримки діагностики має явну ціль – допомагати лікарю аналізувати симптоми та пропонувати можливі діагнози. Неявною ціллю тут може бути підвищення «точності» рекомендацій завдяки орієнтації лише на найбільш поширені захворювання, що призводить до ігнорування рідкісних патологій і ризику хибних висновків. Така зміна цілі не призведе до виведення за межі правового регулювання дій розробників і користувачів системи.

¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата звернення: 21.09.2025).

У АІА програми штучного інтелекту класифікуються на основі потенційних рівнів ризику. Категорія «неприйнятний ризик штучного інтелекту» забороняє розробку й використання певних програм штучного інтелекту, наприклад систем соціального скорингу. До «штучного інтелекту високого ризику» віднесено системи, які можуть поставити під загрозу безпеку людей або порушити їхні основні права.

Авторами АІА реалізовано ідею нормативної мінімізації вказаних раніше соціальних ризиків упровадження ШІ. Порушення приватності пропонується контролювати в спосіб класифікованих за рівнем ризику вимог щодо розробки, введення в експлуатацію та використання систем ШІ.

Небезпеки впливу на поведінку людини мінімізуються шляхом заборони окремих видів ШІ, які пропонується відносити до «Prohibited Artificial Intelligence Practices» (Article 5, АІА). Такі системи характеризуються «неприйнятним ризиком» і поділяються на чотири категорії: дві з них стосуються когнітивного поведінкового маніпулювання людьми або певними вразливими групами; інші дві заборонені категорії – це системи соціального скорингу й системи дистанційної біометричної ідентифікації в режимі реального часу. Однак для кожної категорії є винятки з основного правила¹.

Непрозорість пропонується долати шляхом обов'язкового документування створення, використання та вдосконалення високоризикованих систем ШІ, постійної актуалізації технічної документації таких систем, наявністю обов'язку виробника надавати контролюючим органам вичерпну інформацію щодо поточного стану системи ШІ, які віднесено до високоризикованих.

Нарешті, мінімізація упередженості забезпечується шляхом контролю за змістом і репрезентативністю навчальних, валідаційних і тестових наборів даних.

Значну увагу АІА приділяє системам ШІ, які використовують правоохоронні органи. Певні інструменти ШІ в правоохоронних ор-

¹ Kop M. EU Artificial Intelligence Act: The European approach to AI. *Transatlantic Antitrust and IPR Developments* / Transatlantic Technology Law Forum. 2021. № 2. P. 8–18. URL: <https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/> (дата звернення: 21.09.2025).

ганах віднесено до категорії «високого ризику» (AIA Annex III). Йдеться про поліграфи або аналогічні інструменти й системи, призначені для виконання таких завдань, як: оцінка ризику того, що фізична особа стане жертвою кримінальних злочинів; оцінка достовірності доказів під час розслідування злочинів; оцінка ризику вчинення фізичною особою правопорушення або рецидиву; оцінка рис особистості та характеристик чи минулої злочинної поведінки фізичних осіб або груп; профілювання фізичних осіб під час розслідування злочинів.

Оскільки такі системи віднесено до високоризикованих, їх користувачі, постачальники, розробники та продавці повинні дотримуватися передбачених AIA вимог. Зокрема кожна програма повинна пройти вичерпний процес оцінки та зменшення ризиків (оцінка відповідності). Висуваються вимоги до даних, які використовуються для навчання цих систем штучного інтелекту, їх набори мають бути достатніми, щоб попередити дискримінаційні результати й алгоритмічні упередження¹. Сертифікація, оцінка й моніторинг високоризикованих систем III має відбуватися спеціальним уповноваженим органом, такі системи мають бути зареєстрованими та включеними у відповідну базу даних, має бути забезпечений постійний процес запису та зберігання відомостей щодо всіх подій, які відбуваються в системі, необхідним є забезпечення надійності функціонування та кіберзахисту системи тощо.

Чимало уваги ми приділили деталям, оскільки вважаємо, що вони найкраще демонструють, як змінилася дискусія щодо правового регулювання соціалізації штучного інтелекту. Цілком природно, що починалася вона з питань стратегічного рівня, але фактичні інформаційні технології, їх використання та розширення сфери застосування достатньо чітко визначили напрями подальшого розвитку дискурсу. Фокус змістився на чіткі прикладні задачі, дискусія набула традиційного юридичного характеру та змісту.

Рівні правового регулювання штучного інтелекту у сфері кримінальної юстиції можна розглядати як взаємодоповнювальну систему.

¹ The EU AI act. *AP4AI*. URL: <https://ap4ai.eu/eu-ai-act> (дата звернення: 21.09.2025).

На метарівні ключовим завданням є узгодження технологічного розвитку з базовими цінностями й суспільними пріоритетами, адже саме тут формулюється бачення, що ІІІ в кримінальній юстиції має слугувати не стандартизації чи автоматизації, а індивідуалізації правового впливу для підвищення ефективності використання соціальних ресурсів. Стратегічний рівень передбачає вихід із гіпотетичних моделей на ґрунт реально наявних технологій, адже саме вони формують актуальні виклики для правової системи. Нарешті, тактичний рівень забезпечує реагування на безпосередні ризики впровадження штучного інтелекту в правоохоронну практику – від захисту приватності й попередження дискримінаційних результатів до забезпечення прозорості алгоритмів і створення механізмів відповідальності за їх використання.

7.3. Використання штучного інтелекту для вчинення кримінальних правопорушень

Стрімкий розвиток штучного інтелекту змінює не лише легальні сфери діяльності, а й злочинність. З'являються нові форми шахрайства, які передбачають формування персонального інформаційного середовища для потерпілої особи та профілювання значної кількості людей із метою подальшого автоматизованого фішигу або вішингу. Імовірними можуть стати масштабні кібератаки на основі автоматизованого виявлення вразливостей комп'ютерних систем і їх знову ж таки автоматизованого використання. Протиправне використання технологій штучного інтелекту можливе також шляхом створення високоякісних підробок відео- або аудіоконтенту, розробки надскладних схем легалізації доходів, здобутих злочинним шляхом тощо¹.

Відповідно до наших оцінок за кілька років національна судова практика реагуватиме на випадки несанкціонованого втручання в ро-

¹ Dupont B., Stevens Y., Westermann H., Joyce M. Artificial intelligence in the context of crime and criminal justice. P. 40–56.

боту комп'ютерних мереж із використанням згенерованих системами штучного інтелекту шкідливих програмних засобів, давати оцінку використанню індивідуалізованих дипфейків для вчинення шахрайства, що охоплюватиме десятки тисяч потерпілих.

Предметом обговорення Всесвітнього економічного форуму 2025 року є зростання на 704% випадків обходу онлайн-перевірки біометричних даних особи з використанням дипфейків¹. Також зазначалося, що мовні моделі на базі штучного інтелекту зробили фішингові шахрайства більш поширеними й переконливими, маніпулюючи людьми, змушуючи їх розкривати конфіденційну інформацію в безпрецедентних масштабах².

Звіт «AI and Serious Online Crime» (березень 2025), підготовлений дослідниками Центру з питань нових технологій та безпеки (CETaS) при «The Alan Turing Institute» (Велика Британія), містить висновок про суттєве пришвидшення процесів злочинного використання AI у сферах фінансового шахрайства, фішингу, DDoS-атак, створення та поширення CSAM («Child Sexual Abuse Material»), а також так званих «романтичних» шахрайств. Дослідження підкреслює, що поширення відкритих ШІ-моделей, зокрема китайського походження, створює нові можливості для організованих злочинних груп, тоді як зростання практик «jailbreaking», видалення «guardrails» і розробки «кримінальних LLM» (WormGPT, FraudGPT) формує небезпечні тенденції протиправної діяльності³.

Фінансове шахрайство – одна з найбільш уразливих сфер до впливу штучного інтелекту, яка за оцінками експертів уже зазнає якісної

¹ Див. приклад такого використання у відео (Fraud attempt against a federal agency using deepfake technology / ID.ME. *YouTube*. 2025, January 7. URL: https://youtu.be/iCQhW6BXx_I?si=j6eRDdShYecw7O_m (дата звернення: 21.09.2025)) – коли особа демонструє документ (00:36), можна помітити реальне, незмінене обличчя.

² Hall B. How AI-driven fraud challenges the global economy – and ways to combat it. *World Economic Forum*. 2025, January 16. URL: <https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/> (дата звернення: 21.09.2025).

³ Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime : CETaS Research Reports / The Alan Turing Institute. 2025, March. 32 p. URL: https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_report_-_ai_and_serious_online_crime_0.pdf (дата звернення: 21.09.2025).

трансформації. Наводиться випадок у Гонконзі (2024), коли працівника міжнародної компанії ввели в оману синтетичним відео й аудіо «фінансового директора», змусивши переказати приблизно 20 млн фунтів стерлінгів. ШІ-згенеровані голоси й відео часто супроводжуються класичними фішинговими листами чи електронними інструкціями, що створює багаторівневий ефект переконання. ШІ дає змогу автоматично створювати та проводити численні шахрайські кампанії одночасно від імені «керівників», «банківських менеджерів» чи «близьких родичів». За прогнозом, до 2027 року втрати від ШІ-шахрайства у США можуть зрости з 12,3 млрд (2023) до 40 млрд доларів¹. У 2023 році 51% організацій повідомили про втрати від 5 до 25 млн доларів через ШІ-злочини². Водночас шахрайство з використанням ШІ вважається «легким і малоризиковим», що стимулює його поширення³.

ШІ істотно посилив проблему CSAM. Штучний інтелект застосовується для генерації реалістичних зображень і відео, які кваліфікуються за чинним законодавством як матеріали сексуального насильства над дітьми. Спільноти злочинців активно обмінюються знаннями й інструментами, продають готові моделі та програми для генерації, що створює «ефект навчання» всередині підпільних мереж⁴.

«Jailbreaking» у контексті штучного інтелекту означає маніпуляцію підказками (prompts) або втручання в систему з метою обійти вбудовані обмеження (guardrails), які запобігають генерації забороненого чи шкідливого контенту. За допомогою спеціальних інструкцій користувачі змушують AI-модель видавати інформацію, яку вона за правилами мала би блокувати (наприклад, детальні рекомендації для створення шкідливого ПЗ чи поради для злочинних дій). Дослідження показали, що для деяких великих мовних моделей (LLMs) рівень

¹ Lumley L. Deepfake fraud directed at banks on the rise. *The Banker*. 2024, June 12. URL: <https://www.thebanker.com/Deepfake-fraud-directed-at-banks-on-the-rise-1718178559> (дата звернення: 21.09.2025).

² 2024 AI, fraud, and financial crime survey : AI's role in perpetrating and fighting financial crime. *Biocatch*. URL: <https://www.biocatch.com/ai-fraud-financial-crime-survey> (дата звернення: 21.09.2025).

³ Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime. P. 16–17.

⁴ Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime. P. 17–18.

відмови у видачі шкідливих відповідей через jailbreaking знизився з 98 до лише 2%. Популярні LLM використовувалися для отримання порад про те, як «ефективно спокусити дитину» чи як організувати злочинні операції. Поряд із jailbreaking з'являються модифіковані спеціально для злочинців моделі III (WormGPT, FraudGPT), у яких guardrails узагалі немає. Крім безпосереднього використання, jailbreaking підвищує ризик появи чорного ринку «розблокованих» моделей, доступних через даркнет або Telegram-канали¹.

«Романтичне» шахрайство (romance fraud, romance scams) відбувається, коли злочинці встановлюють удавані емоційні чи романтичні стосунки з жертвою з метою подальшого фінансового чи іншого використання. Великі мовні моделі (LLMs) здатні автоматично генерувати персоналізовані повідомлення, що імітують стиль листування та створюють ілюзію реальної людини. Замість обмеженої кількості жертв шахрай може одночасно вести сотні «розмов», автоматизуючи процес знайомства й підтримання контакту. Злочинці використовують синтетичні фото, відео й голоси для підтримання довіри – від «селфі» до онлайн-дзвінків. Дослідження підкреслює, що III особливо ефективний на етапі «побудови довіри», коли важливо підтримати жертву тривалим емоційним контактом, перед тим як перейти до вимагання грошей. Поява більш реалістичних агентів (agentic AI) може дати змогу шахраям створювати майже повністю автономних «віртуальних партнерів», що знижує потребу в людському втручанні. Це створює ситуацію, коли відрізнити справжню особу від синтетичної буде дуже складно².

Технологія дипфейків зумовила появу нового виду посягань на приватне життя – створення порнографічних матеріалів із зображенням реальної особи за допомогою III без її згоди. Злочинці використовують фото потерпілої особи (наприклад, із соцмереж) і створюють порнокліп «з її участю» за допомогою нейромережі. Таким чином, виробляються фальшиві інтимні відео, які завдають істотної моральної, репутаційної, психологічної шкоди. У багатьох країнах спостерігається справжній бум таких випадків. За даними британської

¹ Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime. P. 13–15.

² Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime. P. 19–20.

«Revenge Porn Helpline», з 2017 по 2022 рік кількість звернень щодо зловживання дипфейками інтимного характеру зросла на 400 %¹. Оскільки зображення згенеровані, подібні дії не підпадають під ознаки традиційної заборони розповсюдження реальних інтимних фото без згоди потерпілої особи.

Реакцією на проблему таких дипфейків у США є «TAKE IT DOWN Act» (2025) – законопроект, внесений до Палати представників США 22 січня 2025 року, спрямований на протидію не-санкціонованій публікації інтимних зображень, зокрема створених із використанням технологій дипфейків. Закон забороняє розміщення в інтернеті без згоди особи і автентичних, і згенерованих зображень. Окремо передбачено кримінальну відповідальність за публікацію або погрозу публікації інтимних матеріалів щодо неповнолітніх. Порушники підлягають покаранню у вигляді штрафу або позбавлення волі. Законопроект також установлює обов'язок онлайн-платформ видаляти інтимні зображення, розміщені без згоди, протягом 48 годин після повідомлення. Отже, «TAKE IT DOWN Act» формує правові механізми захисту цифрової недоторканності приватного життя в умовах зростання загроз, пов'язаних із використанням технологій штучного інтелекту².

Після ухвалення «TAKE IT DOWN Act» у Конгресі США розглядається ще низка законопроектів. Ці ініціативи демонструють намір федеральних законодавців охопити різні сфери ризиків – від захисту приватності до забезпечення прозорості у виборчому процесі. «DEFIANCE Act» («Disrupt Explicit Forged Images and Nonconsensual Edits») спрямований на надання жертвам поширення дипфейків змоги подавати цивільні позови й вимагати компенсацію. «Protect Elections from Deceptive AI Act» забороняє поширення оманливих

¹ Demony C. Britain to make sexually explicit 'deepfakes' a crime. *Reuters*. 2025, January 7. URL: <https://www.reuters.com/world/uk/britain-make-sexually-explicit-deep-fakes-crime-2025-01-07/> (дата звернення: 21.09.2025).

² Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (Take It Down) Act. *Congress.gov*. 22.01.2025. URL: <https://www.congress.gov/congressional-record/congressional-record-index/118th-congress/2nd-session/tools-to-address-known-exploitation-by-immobilizing-technological-deepfakes-on-websites-and-networks-take-it-down-act/1918605> (дата звернення: 21.09.2025).

ШІ-зображень і відео щодо федеральних кандидатів, якщо вони створені для впливу на вибори чи збори коштів. «NO FAKES Act» передбачає заборону на створення або розповсюдження ШІ-реплік голосу чи образу людини без її згоди, за винятком випадків сатири, новин і коментарів. «DEEPFAKES Accountability Act» вимагає маркування дипфейк-контенту для забезпечення його технічної ідентифікації. «Protecting Consumers from Deceptive AI Act» доручає Національному інституту стандартів і технологій (NIST) розробити стандарти для маркування ШІ-контенту й зобов'язує онлайн-платформи додавати машинозчитувані позначки до згенерованого медіа¹.

Окрім федеральних законодавчих ініціатив, майже всі штати США мають власні законодавчі проекти щодо ШІ й дипфейків. Видається можливим сформулювати такі напрями законодавчого реагування на проблему дипфейків у США: захист політичного процесу (обов'язкові дисклеймери), криміналізація дипфейків (шахрайство, сексуальна експлуатація), захист прав споживачів (право знати про взаємодію із ШІ), відповідальність платформ (видалення контенту, прозорі процедури модерації).

Відповідно до звіту Департаменту внутрішньої безпеки США «Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure» (2024) до ключових загроз у сфері використання штучного інтелекту в критичній інфраструктурі належать *атаки проти самих систем ШІ*. По-перше, «отруєння» даних, коли до процесу навчання чи налаштування моделі цілеспрямовано вносяться фальсифіковані дані, що призводить до систематично хибних результатів. По-друге, маніпуляції з архітектурою чи налаштуваннями моделі, які здатні змінювати алгоритмічні висновки або спричиняти відмову в роботі. По-третє, «змагальні»² атаки, тобто спеціально сконструйовані

¹ Regan G. The State of Deepfake Regulations in 2025: What Businesses Need to Know. *Reality Defender*. 2025, June 18. URL: <https://www.realitydefender.com/insights/the-state-of-deepfake-regulations-in-2025-what-businesses-need-to-know> (дата звернення: 21.09.2025).

² «Змагальними» атаками називають втручання у роботу систем ШІ з використанням спеціально підготовлених даних, які експлуатують уразливості алгоритмів і призводять до генерації помилкових класифікацій або прогнозів. Зазвичай такі дані створюються іншими системами ШІ, які виступають у ролі

вані вхідні дані, що примушують модель давати неправильні класифікації чи прогнози. По-четверте, атаки на середовище розгортання, включно з експлуатацією інтерфейсів доступу, хмарних сервісів чи API, що підтримують функціонування моделей. Нарешті, по-п'яте, атаки на конфіденційність даних користувачів, які дають змогу отримати чутливу інформацію з навчальних або експлуатаційних процесів. Сукупно ці загрози здатні не лише підірвати коректність і безпечність роботи окремої системи, а й мати каскадний ефект для цілих секторів критичної інфраструктури¹.

Дослідження свідчать, що подібні порушення можливі не тільки відносно критичної інфраструктури. Наприклад, «отруєння» даних є особливо небезпечним у контексті дезінформації, де фальшиві наративи, наприклад про воєнні злочини, можуть цілеспрямовано поширюватися через відкриті вебресурси, які автоматично збираються та використовуються для тренування моделей². Наприклад, метод фальсифікації міток (mislabeling), «backdoor poisoning» або «boiling frog» можуть змусити модель видавати певні хибні відповіді лише у відповідь на специфічні запити, залишаючись коректною в більшості випадків^{3,4}. Відповідні дослідження показали, що атаки даних можуть істотно знижувати точність класифікаційних моделей III

«супротивника». Наприклад, система-супротивник може проаналізувати роботу системи комп'ютерного зору, що використовується у сфері дорожньої безпеки, та запропонувати мінімальні зміни пікселів у зображенні дорожнього знаку. Ці зміни залишаються непомітними для людського ока, проте змушують систему комп'ютерного зору помилково класифікувати знак «STOP» як знак «швидкісна траса».

¹ Impact of artificial intelligence on criminal and illicit activities / Department of Homeland Security. Public-Private Analytic Exchange Program, 2024. 59 p. URL: https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf (дата звернення: 21.09.2025).

² Falk R., Brown A.-L. Poison the well : AI, data integrity and emerging cyber threats / Cyber Security Cooperative Research Centre. 2023. 16 p. URL: <https://cybersecuritycrc.org.au/remote-assets/sites/default/files/2023-11/Poison%20the%20well%20-%20AI%2C%20data%20integrity%20and%20emerging%20cyber%20threats.pdf> (дата звернення: 23.08.2025).

³ What is AI data poisoning? *Cloudflare*. URL: <https://www.cloudflare.com/learning/ai/data-poisoning/> (дата звернення: 23.08.2025).

⁴ What is a data poisoning? [Examples & Prevention]. *Palo Alto Networks*. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-data-poisoning> (дата звернення: 23.08.2025).

до 27% у задачах розпізнавання зображень і до 22% у процесі виявлення шахрайства¹.

Правоохоронні органи наразі не мають достатніх можливостей для ефективної протидії злочинному використанню ШІ. Важливим є швидке масштабування використання АІ в правоохоронних структурах і розвиток міжнародної кооперації. Загальний висновок полягає в тому, що протидія злочинному використанню штучного інтелекту можлива лише за умови застосування принципу «АІ проти АІ», коли правоохоронні органи самі активно використовують інноваційні алгоритми для виявлення та запобігання новим формам кіберзлочинності².

Водночас попри масштабність описаних загроз, на нашу думку, немає потреби в спеціальних змінах до КК. Чинні кримінально-правові норми дають змогу належно кваліфікувати діяння, що вчиняються з використанням технологій штучного інтелекту, адже небезпека посягань охоплюється наявними складами злочинів. Наприклад, шахрайство, зумовлене застосуванням дипфейків чи генеративних моделей, охоплюється ст. 190 КК; розробка або поширення шкідливих програмних засобів – ст. 361–363-1 КК; виготовлення і розповсюдження CSAM – ст. 301, 301-1; а використання штучного інтелекту в процесі легалізації доходів злочинного походження – ст. 209 КК.

Подальший розвиток судової практики забезпечить необхідну деталізацію та роз'яснення для правильної кваліфікації нових форм злочинності. У цьому сенсі ключовим завданням є не так перегляд кримінально-правових норм, як вироблення єдиних підходів до їх тлумачення судами, а також належна підготовка експертів і слідчих, які мають здатність виявляти й аналізувати злочини, учинені з використанням штучного інтелекту. Такий підхід відповідає принципам стабільності й технологічної нейтральності кримінального законодавства, дає змогу уникнути надмірної фрагментації правових приписів.

¹ Kure H. I., Sarkar P., Ndanusa A. B., Nwajana A. O. Detecting and preventing data poisoning attacks on AI models. *arXiv*. 2025, March 25. 9 p. DOI: <https://doi.org/10.48550/arXiv.2503.09302>.

² Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime.

7.4. Динамічні санкції: один із можливих напрямів використання штучного інтелекту в кримінально-правовому регулюванні

Як було зазначено, одна з найбільших небезпек використання штучного інтелекту в кримінальній юстиції полягає в алгоритмічному «усередненні». Якщо технологія орієнтується на абстрактний профіль «середньої людини», правосуддя втрачає сенс індивідуалізації та перетворюється на механічне відтворення шаблонів. Саме ця проблема актуалізує пошук рішень, здатних поєднати єдність судової практики й індивідуалізований підхід. Одним із таких рішень може стати концепція динамічних санкцій, яку ми пропонуємо.

Призначення покарання сьогодні відбувається в межах статичних санкцій, визначених у КК (наприклад, «від трьох до восьми років позбавлення волі»). Ця система забезпечує законність, але породжує істотну варіативність вироків навіть за схожих обставин. Нерівність у покараннях підриває довіру до правосуддя. Водночас спроби законодавчо звужити дискрецію суддів шляхом жорсткішого визначення меж покарання мають свій зворотний бік: закон починає гірше відображати різноманіття життєвих ситуацій та індивідуальних обставин справи, що в кінцевому підсумку також знижує справедливість судових рішень.

Усе означене робить сферу законодавчого визначення санкцій та призначення покарань однією з найочевидніших для застосування технологій ШІ.

Ідея полягає у впровадженні рекомендованих діапазонів покарання, які формуються на підставі аналізу всіх актуальних вироків у подібних справах. Алгоритми ШІ виявляють закономірності та пропонують суддям статистично обґрунтований інтервал, що відображає реальну практику. Водночас: 1) законодавчо встановлені мінімум і максимум є обов'язковими; 2) рекомендації подаються у формі діапазону, що відображає найбільш поширену практику призначення

покарання судами в подібних справах; такий інтервал охоплює основну масу реальних вироків; 3) суддя зберігає право мотивовано відступити від рекомендованого діапазону.

Ефективність, допустимість і коректність роботи системи динамічних санкцій можуть бути забезпечені низкою технічних і правових заходів.

Як база для формування рекомендованих діапазонів мають застосовуватися лише ті вирoki, які набрали чинності. Оскільки судова практика постійно розвивається, алгоритм повинен періодично оновлювати вхідні дані, мати постійний доступ до потоку вироків. Це дасть змогу враховувати зміни в правозастосуванні, тенденції у визначенні видів і розмірів покарання.

Суддя отримуватиме не лише діапазон покарання, а й пояснення того, які обставини справи й характеристики особи підсудного вплинули на результат. Ідеться про такі зрозумілі для правників показники, як наявність рецидиву, обтяжуючі чи пом'якшуючі обставини, характер заподіяної шкоди. Така прозорість сприятиме довірі до системи, оскільки даватиме змогу судді критично оцінювати рекомендацію.

Окрім загального пояснення, система може показувати умовні сценарії, так звані «counterfactual explanations», як змінюватиметься рекомендація за умови змін фактичних даних. Наприклад: якщо б підсудний не мав попередніх судимостей, рекомендований діапазон був би настільки нижчим; або, за наявності добровільного відшкодування шкоди потерпілому, система рекомендувала б м'якше покарання. Такі пояснення знову ж таки дають змогу судді бачити логіку алгоритму в зрозумілій формі та критично оцінювати рекомендації.

До найбільш очевидних ризиків використання таких систем слід відносити упередженість даних і згадану раніше «input problem». Алгоритми, навчені на історичних даних щодо застосування закону про кримінальну відповідальність, можуть бути упередженими, закріплювати соціальні дискримінаційні практики¹. Окрім того, не всі релевантні характеристики винної особи чи обставини кримінального правопорушення можливо закодувати в алгоритмі («input problem»),

¹ Dressel J., Farid H. The accuracy, fairness, and limits of predicting recidivism. *Science Advances*. 2018. Vol. 4, No. 1. eaao5580. DOI: <https://doi.org/10.1126/sciadv.aao5580>.

що створює ризик спрощення контексту та, як наслідок, генерування занадто широких нерелевантних рекомендацій¹.

До небезпечних когнітивних ризиків, що виникають у суддів при застосуванні систем штучного інтелекту у сфері кримінальної юстиції, належить також ефект анкерингу (якорування або фокусування). Його суть полягає в тому, що початково запропонована оцінка, навіть якщо вона є випадковою чи штучно згенерованою, значною мірою впливає на подальші рішення людини. У контексті призначення покарання це означає, що суддя, отримавши певний «рекомендований діапазон», схильний орієнтуватися на нього, навіть якщо фактичні обставини справи дають змогу ухвалити інше рішення.

Дослідження Гарвардського університету, проведене М. Ваккаро та Д. Уолдо, показало, що використання алгоритму COMPAS як інструмента оцінки ризику рецидиву призводить саме до такого ефекту. У серії експериментів встановлено: якщо учасникам демонстрували «низькі» бали ризику кримінальної поведінки, їх власні оцінки ризику були статистично значно нижчими; якщо ж «високі» – вони суттєво підвищували власні прогнози. Середнє відхилення становило понад 40%, що повністю відповідає класичним показникам ефекту фокусування, відомого з психологічних досліджень Е. Тверські та Д. Канемана². Отже, навіть коли судді або інші вповноважені особи формально залишаються «кінцевими арбітрами», алгоритмічні оцінки фактично задають якір, від якого вони несвідомо відштовхуються. Важливим висновком дослідження є те, що в такій ситуації контроль судді над остаточним рішенням сам собою не усуває упереженості. Алгоритмічний «якір» усе одно впливатиме на процес, а помилки чи викривлення у вихідних даних системи можуть масово відтворюватися в судових вирокх³.

¹ Ryberg J. Artificial intelligence and criminal justice: How to use algorithmic sentencing support in real life (and ethically non-ideal) penal systems? *AI Ethics*. 2025. Vol. 5. P. 3255–3263. DOI: <https://doi.org/10.1007/s43681-024-00655-8>.

² Tversky A., Kahneman D. Judgment under uncertainty: heuristics and biases. *Science*. 1974. Vol. 185, No. 4157. P. 1124–1131. DOI: <https://doi.org/10.1126/science.185.4157.1124>.

³ Vaccaro M., Waldo J. The effects of mixing machine learning and human judgment. *ACM Queue*. 2019. Vol. 17, Iss. 4. 22 p. DOI: <https://doi.org/10.1145/3358955.3363293>.

Можливість означених ризиків актуалізує питання мінімізації негативних наслідків пропонованої системи динамічних санкцій. Визначення інституційних і технічних запобіжників шкоди від роботи системи є важливою складовою її розробки.

Як підкреслюють С. Вахтер, Б. Міттельштадт і К. Рассел, прозорість алгоритмів у правовій сфері є ключовою умовою легітимності їх застосування. Вони розглядають «counterfactual explanations» (як зміниться рекомендація залежно від змін фактичних даних) як засіб мінімізації ризику «чорної скриньки». Як ефективний засіб виявлення упередженості й технічних помилок дослідники також розглядають незалежний аудит – перевірку навчальних даних, моделей і результатів сторонніми експертами з метою виявлення упередженості чи технічних помилок¹.

Представлені й результати наукових досліджень щодо виявлення упередженості в навчальних даних для систем ШІ. Як неодноразово зазначалося, моделі «навчені» на реальних судових рішеннях, можуть відтворювати системну дискримінацію, наприклад за ознаками статі, раси чи соціально-економічного статусу. В. Лум і Д. Джондроу запропонували підхід «fair representation learning» і методи очищення даних (pre-processing), які дають змогу зменшувати вплив історичних упереджень. Ідея полягає в тому, щоб вилучати з навчальних даних захищені характеристики (race, gender, ethnicity), а також застосовувати математичні методи, які усувають приховані кореляції². Такий підхід знижує ризик того, що рекомендації системи будуть дискримінаційними.

Навіть за умови високої точності алгоритмів остаточне рішення має бути за суддею. Європейська хартія етики застосування ШІ в правосудді (CEPEJ, 2018) закріпила принцип «під контролем користувача» (under user control), відповідно до якого системи штучного інтелекту повинні бути лише допоміжним інструментом, а не автономним

¹ Wachter S., Mittelstadt B., Russell C. Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*. 2018. Vol. 31, Iss. 2. P. 841–887. DOI: <https://doi.org/10.48550/arXiv.1711.00399>.

² Lum K., Johndrow J. E. A statistical framework for fair predictive algorithms. *arXiv*. 2016. DOI: <https://doi.org/10.48550/arXiv.1610.08077>.

суб'єктом ухвалення рішень¹. Аналогічні положення закріплені й у згаданому раніше «EU Artificial Intelligence Act».

Нарешті мінімізація ефекту анкерінгу, когнітивного упередження людей, які використовують рекомендаційні системи, забезпечується спеціальними методиками критичної оцінки результатів роботи ШІ. Зокрема, крім «counterfactual explanations» і прозорості алгоритмів, доволі часто згадується порядок ознайомлення з рекомендаціями ШІ. Пропонується спершу надавати судді можливість сформулювати власну оцінку, а потім ознайомлюватися з рекомендаціями системи².

Запровадження системи динамічних санкцій на основі штучного інтелекту здатне поєднати два важливі напрями кримінально-правового регулювання – єдність судової практики й індивідуалізацію покарання. Використання алгоритмів для формування рекомендованих діапазонів, що відображають актуальні тенденції в правозастосуванні на момент постановлення вироку, дасть змогу підвищити рівень довіри до судової системи та створити умови для більш справедливого й обґрунтованого призначення покарання.

Із технічного погляду, така система є реальною вже на теперішньому рівні розвитку технологій: існують напрацьовані методики прозорих алгоритмів, інструменти незалежного аудиту й механізми очищення даних від упередженості. Однак для ефективного функціонування динамічних санкцій необхідне подальше розширення та якісне вдосконалення наборів даних, які накопичуються та аналізуються в процесі протидії злочинності. Йдеться про інтеграцію різних джерел – від судових рішень і статистики покарань до інформації про соціальні, економічні та кримінологічні чинники, що впливають на призначення санкцій³.

Пропонуємо наступне визначення: динамічна санкція – це відносно визначена санкція, доповнена рекомендованим діапазоном

¹ European Ethical Charter on the use of artificial intelligence in judicial systems and their environment : Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018) / European Commission for the Efficiency of Justice (CEPEJ). Strasbourg : Council of Europe, 2018. 77 p. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (дата звернення: 21.09.2025).

² Vaccaro M., Waldo J. The effects of mixing machine learning and human judgment.

³ Більш докладно це аргументували в попередньому розділі.

покарання, який постійно оновлюється на основі аналізу судової практики із застосуванням технологій штучного інтелекту. У якості пропозиції для обговорення пропонуємо такий зміст можливої статті КК:

«Стаття... Динамічні санкції

Разом із законодавчо визначеними мінімальними й максимальними межами покарання за вчинення окремих кримінальних правопорушень установлюються рекомендовані діапазони покарання, що формуються з використанням технологій штучного інтелекту на основі аналізу судової практики.

Рекомендований діапазон покарання визначає інтервал (у межах мінімуму й максимуму санкції), що відображає найбільш поширену практику призначення покарання судами за аналогічні правопорушення з урахуванням типових обставин справи, характеристик особи винного, пом'якшуючих та обтяжуючих обставин.

Суд під час призначення покарання зобов'язаний ознайомитися з рекомендованим діапазоном і врахувати його. Суд має право мотивовано відступити від рекомендованого діапазону, якщо обставини справи істотно відрізняються від типових, на основі яких було сформовано відповідну рекомендацію.

Система формування рекомендованих діапазонів покарання функціонує під контролем державного органу, уповноваженого на здійснення моніторингу судової практики, який забезпечує: періодичне оновлення даних на основі вироків, що набрали законної сили; публічність і прозорість алгоритмів, використаних для формування діапазонів; незалежний аудит моделей і навчальних даних; можливість отримання пояснення рекомендації, включно з варіантами зміни результату за інших обставин справи.»

Використання технологій штучного інтелекту дає змогу проаналізувати всі актуальні судові рішення й визначити статистично обґрунтований рекомендований інтервал, у межах якого найчастіше призначається покарання за конкретну категорію справ. У такий

спосіб мінімізуються ризики надмірної варіативності рішень і нерівність у призначенні покарань, властиві «статичним» санкціям.

Запропонований механізм не позбавляє суд дискреції, але забезпечує її обґрунтованість і технологічну прозорість, зменшує різницю у вироках за схожих обставин, а також створює основу для динамічного оновлення кримінально-правової політики відповідно до актуальних соціальних і правозастосовних тенденцій.

Разом із тим очевидно, що реалізація такого підходу вимагатиме масштабних змін у процесах збирання, верифікації та аналізу даних про судові рішення, а також розбудови інфраструктури кібербезпеки й захисту даних. Необхідним є створення нормативних, технічних і організаційних передумов для надійної роботи таких систем – від уніфікації форматів судових рішень до розробки державних стандартів етичного й безпечного використання алгоритмів у сфері кримінальної юстиції.

Доповнення Кримінального кодексу нормою про динамічні санкції саме собою не створить повноцінну експертну систему рекомендацій. Вона має стати елементом комплексної цифрової трансформації правосуддя, яка включатиме як модернізацію судових інформаційних систем, так і підготовку фахівців, здатних критично працювати з алгоритмічними рекомендаціями.

Висновки

Системи штучного інтелекту довели свою спроможність допомагати правоохоронним органам і судам у сферах прогнозування злочинності, оцінки ризиків рецидиву, забезпечення єдності судової практики та вдосконалення кримінального законодавства. Вони дають змогу працювати з великими масивами даних, виявляти приховані закономірності та пропонувати рішення, що підвищують обґрунтованість і швидкість реагування.

Поряд із потенційними перевагами є небезпека, що алгоритмічні системи закріплюватимуть наявні упередження та сприятимуть форму-

ванню «усереднених» рішень. Це може призвести до втрати індивідуалізації кримінально-правового впливу, перетворивши правосуддя на механічне відтворення шаблонів. Ризики посилюються ефектом зворотної петлі в прогнозуванні злочинності та проблемою «input problem», коли важливі деталі справи залишаються поза увагою алгоритму.

Алгоритмічна упередженість і «чорна скринька» ШІ зумовлюють критичну потребу у впровадженні пояснюваних моделей (explainable AI), що дають змогу відстежити логіку ухвалення рішень. Прозорість, незалежний аудит і контроль є ключовими умовами, які забезпечують законність і легітимність використання ШІ в кримінальній юстиції.

Оптимальна модель регулювання ШІ передбачає три взаємодоповнювальні рівні: метарівень – узгодження технологій із базовими суспільними цінностями та принципами справедливості; стратегічний рівень – визначення орієнтирів для правового осмислення технологій, що реально існують, з урахуванням ризиків гіпотетичного розвитку; тактичний рівень – конкретні механізми реагування на наявні загрози: захист приватності, попередження дискримінації, забезпечення прозорості й відповідальності.

Штучний інтелект стає інструментом нових форм кримінальних правопорушень (фішинг, дипфейки, CSAM, фінансові шахрайства, jailbreaking). Водночас діяння такого типу переважно охоплюються чинними нормами КК. Тому першочерговим завданням є не зміна кримінально-правових заборон, а вироблення судової практики, розвиток експертизи й міжнародної кооперації для ефективного реагування.

Майбутнє ШІ в кримінальній юстиції визначатиметься тим, чи стане він інструментом для посилення справедливості, індивідуалізації впливу й раціонального використання ресурсів, чи перетвориться на механізм стандартизації та посилення соціальної нерівності. Зважаючи на це, нами запропоновано концепцію системи динамічних санкцій. Її запровадження на основі алгоритмів штучного інтелекту може бути важливим кроком у напрямі поєднання єдності судової практики й індивідуалізації покарання. Такі системи не відмінюють роль судді, а створюють рекомендаційний інструмент, що максимально враховує реальний стан актуальної судової практики. У підсумку динамічні санкції здатні зменшити несправедливість у призначенні покарань і зміцнити довіру суспільства до правосуддя.

Висновки

Кримінальне право й інформатизація перебувають у взаємодії. Інформатизація формує нові виклики для безпеки суспільства, породжуючи раніше невідомі загрози. Водночас вона надає унікальні можливості для посилення ефективності кримінального права. Саме ця взаємна залежність визначає необхідність синхронізації розвитку права й цифрових технологій.

Інформаційна безпека розглядається як об'єкт кримінально-правової охорони. Є три основні групи посягань: кримінальні правопорушення у сфері використання інформаційних технологій; кримінальні правопорушення у сфері обмеженого доступу до інформації; кримінальні правопорушення у сфері формування інформаційного простору. Кожна з цих груп потребує специфічних механізмів кримінально-правового регулювання.

Важливим питанням є визначення поняття «комп'ютерний злочин». Коректність такого визначення безпосередньо впливає на можливість здійснювати обґрунтовані висновки щодо поширеності цього виду кримінальної діяльності й розмірів заподіяної шкоди. Надмірно широке визначення ускладнює напрацювання ефективних стратегій протидії, спотворює статистичну картину та створює ризик помилкових рішень на рівні кримінально-правової політики.

В Україні створено якісну організаційну й законодавчу інфраструктуру для протидії злочинам у сфері використання інформаційних технологій. Національне законодавство гармонізоване з міжнародними стандартами, зокрема положеннями Будапештської конвенції, та передбачає спеціалізовані підрозділи правоохоронних органів. Водночас спостерігається помітна тенденція до примітивізації фактичної протидії: ресурси й зусилля здебільшого зосереджується на простих формах злочинної діяльності, тоді як складні й небезпечніші прояви кіберзлочинності залишаються на периферії уваги. Подолання цієї диспропорції є необхідною умовою для підвищення ефективності кримінально-правової охорони інформаційної безпеки.

Окрім появи нових видів кримінальних правопорушень (розділ XVI Особливої частини КК), значно масштабніший вплив інформатизації проявився в оновленні форм традиційних посягань. Насамперед це стосується злочинів проти власності. У протидії таким злочинам простежується неоднозначність судової практики. Правоохоронна система зіштовхується з постійним оновленням технологічної бази злочинців, зокрема з поширенням віртуальних активів як нового предмета злочинного впливу. Важливо зазначити, що прогноз змін найпоширенішого за рівнем обліку кримінального правопорушення – шахрайства – безпосередньо пов'язаний із використанням інформаційних технологій. Водночас очікуване розширення протиправного використання віртуальних активів в Україні сьогодні супроводжується лише фрагментарним регулюванням, що ускладнює діяльність правоохоронців. Міжнародні стандарти в цій сфері, насамперед Рекомендації FATF, прямо вимагають поширення процедур фінансового моніторингу та принципів KYC/AML на постачальників послуг, пов'язаних з обігом віртуальних активів. Європейський Союз у Регламенті MiCA (Markets in Crypto-Assets Regulation) запровадив цілісну модель регулювання обігу криптоактивів, яка має не лише захистити інвесторів, а й створити передумови для ефективного запобігання їх злочинному використанню. Українська правова система тільки наближається до цих стандартів, що зумовлює розрив між темпами цифровізації фінансового сектору й готовністю кримінальної юстиції адекватно реагувати на нові форми злочинності.

Інформаційні технології не тільки трансформують злочинність. Вони дають змогу проводити комплексний моніторинг злочинності, застосовувати методи прогнозування та моделювання. Створена автором аналітична платформа «CrimeDataLab» є практичною реалізацією підходів обчислювальної соціальної науки у сфері протидії злочинності. Вона поєднує можливості роботи з великими масивами відкритих даних й інструменти сучасної візуалізації для оцінки ефективності кримінально-правового регулювання та діяльності правоохоронних органів. Використання платформи дало змогу встановити низку тенденцій, що раніше залишалися поза увагою через фрагментарність і складність доступу до офіційної статистики. Зокрема, було

виявлено прояви примітивізації протидії незаконному обігу наркотиків, корупції та глорифікації дій ворога; визначено особливості протидії злочинності в умовах війни.

Штучний інтелект формує нову якість взаємодії права й технологій. З одного боку, він є інструментом підвищення ефективності кримінальної юстиції: оптимізація роботи слідчих, персоналізація призначення покарання, моделювання наслідків криміналізації чи декриміналізації. З іншого, – новий засіб злочинної діяльності: створення deepfake-контенту, автоматизація шахрайства, несанкціонованого втручання, відмивання коштів тощо.

Сучасні виклики вимагають оновлених методологічних підходів. Традиційні правові інструменти дедалі частіше виявляються недостатніми для ефективної протидії злочинам у цифровій сфері. Необхідне впровадження гнучких механізмів кримінально-правового регулювання, здатних оперативно реагувати на технологічні зміни. Водночас ключовою залишається проблема балансу – між безпекою та правами людини, між автоматизацією правосуддя та збереженням індивідуалізованого підходу до особи.

Національний контекст визначає особливу актуальність досліджуваної проблематики. В умовах збройної агресії проти України інформаційна сфера стала одним із головних полів бою. Тому кримінальне право виконує тут не лише охоронну, а й стратегічну функцію – забезпечення стійкості суспільства й держави. Використання сучасних інформаційних технологій у правоохоронній діяльності стає не лише інструментом внутрішньої безпеки, а й фактором міжнародної інтеграції України.

Синхронізація кримінального права й інформатизації є ключем до ефективності юстиції в цифрову добу. Майбутнє кримінального права пов'язане не з ізоляцією від технологій, а з їх інтеграцією. Такий підхід дасть змогу трансформувати ризики інформатизації в ресурси розвитку кримінальної юстиції та забезпечить адекватну відповідь на виклики цифрової епохи.

Подяки

У серпні 1985 року я вперше побачив персональний комп'ютер. Мій батько, Віталій Піусович Карчевський, доклав чимало зусиль, аби його інститут отримав клас електронно-обчислювальних машин «АГАТ». Відтоді ми з батьком багато говорили про програми й технічні рішення, він навчив мене першим крокам у програмуванні й найважливішому – умінню правильно формулювати завдання для машини.

Дисертація моєї мами, Наталії Василівни Карчевської, була присвячена педагогічним аспектам використання мікро-ЕОМ у навчальному процесі (1991 рік). Її наполегливість і глибока віра в те, що технології мають органічно доповнювати освіту, сформували мій підхід до викладання: головне не техніка сама собою, а її здатність допомагати людині розкривати свої здібності.

Моя дружина, Олена Василівна Карчевська, політолог. Саме завдяки їй професійній, але обережній, критиці в цій книзі відображено теми громадянського суспільства, демократичної участі й відкритих даних.

Мої діти, Таїсія та Тимофій, поки що не доктори філософії, проте їхня щирість і здатність дивитися на речі без упереджень завжди надихають мене й підтримують у роботі.

Науковий керівник моєї кандидатської дисертації (2003) професор Людмила Миколаївна Кривоченко й науковий консультант докторської дисертації (2013) професор Борис Григорович Розовський прищепили розуміння, що наукова робота має справжню цінність лише тоді, коли її результати мають практичне значення та здатні змінювати реальність.

Дякую шановним рецензентам цієї роботи: доктору юридичних наук, професору Олексію Володимировичу Копану, доктору юридичних наук, професору Євгену Олександровичу Письменському, доктору юридичних наук, професору Роману Олександровичу Мовчану.

Із глибокою вдячністю також згадую колективи Луганського державного університету внутрішніх справ імені Е. О. Дідоренка, Львівського державного університету внутрішніх справ і Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України. Багаторічна спільна робота залишила після себе теплі спогади.

Вдячний колективам Університету Короля Данила, Українського католицького університету й Інституту інформації, безпеки і права Національної академії правових наук України. Можливість працювати разом із колегами, розвивати наукові дослідження та освітні ініціативи, формувати нові підходи до вивчення кримінального права в умовах цифрової трансформації має велике значення для мене.

Дуже важливим етапом написання цієї книги стала участь у наукових та освітніх проєктах. Аналітична платформа «CrimeDataLab» була створена в межах дослідження «Рационалізація протидії злочинності в Україні», яке підтримували Національний фонд досліджень України й Кембриджський університет. Особливо цінною була підтримка Метью Бленда (Matthew Bland).

Вдячний Владиславі Станіславівні Батиргарєєвій і команді проєкту «Кримінально-правові та кримінологічні засади протидії глорифікації збройної агресії РФ в Україні» за спільну роботу, яка продемонструвала нові перспективи використання відкритих даних у наукових дослідженнях.

Зі Світланою Володимирівною Хилюк, Христиною Орестівною Мигаль і Благодійною фундацією «Здорові рішення» працювали над звітом «Кримінально-правове регулювання в сфері обігу наркотичних речовин: ефективність, оптимальні межі, виклики воєнного стану» для Благодійної фундації «Здорові рішення». Це була ще одна нагода перевірити «CrimeDataLab» у дії, переконатися, як відкриті дані можуть раціоналізувати дискурс громадянського суспільства та влади. Вдячний колежанкам за важливу роботу разом.

Важливою справою були й численні семінари під егідою Організації з безпеки та співробітництва в Європі для правоохоронців, присвячені протидії злочинам у сфері інформаційних технологій, а також злочинному використанню віртуальних активів. Спілкування та спільна робота з такою аудиторією завжди приносили безцінні емпіричні матеріали. Щиро вдячний Віталію Олександровичу Гацелюку, Сергію Вікторовичу Гриненку й Ірині Ігорівні Потаповій за плідну співпрацю.

Щиро дякую Олені Дмитрівні Арлановій, Антону Сергійовичу Кудінову й Вячеславу Анатолійовичу Штаньку за участь в Open Data Hackathon, де ми вдосконалили «CrimeDataLab».

Також вдячний команді 1991 Accelerator за акселераційну програму. Рух від наукової ідеї до життєздатного рішення, від академічного результату до інноваційного продукту – це надзвичайно цінний досвід.

Окрему вдячність хочу висловити студентам факультету права Українського католицького університету та студентам Університету Короля Данила. Викладаючи з 2023 року курс «Кримінальне право та інформатизація», відчував справжнє задоволення від спілкування з аудиторією допитливих і наполегливих студентів та студенток, які вміють ставити гострі запитання та шукати нестандартні відповіді.

Дякую захисникам і захисницям України – тим, хто зі зброєю в руках боронить нашу державу. Дякую тим, хто на своїх робочих місцях щодня робить усе можливе для відновлення справедливості, миру й гідного життя. Їхня мужність, стійкість і відданість своїй справі зміцнюють віру в те, що наука, право та суспільство мають спільну мету – утвердження людської гідності та свободи.

Список використаних джерел

Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації. *Право України*. 2000. № 12. С. 69–73.

Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження). Київ : Атіка, 2007. 304 с.

Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1 : Сфери застосування, ризики і бар'єри, проблеми правового регулювання : монографія / НДПП НАПрН України. Київ : АртЕк, 2018. 344 с.

Баранов О. Штучний інтелект і система права : монографія / Ін-т інформації, безпеки і права Нац. акад. прав. наук України. Київ ; Одеса : Фенікс, 2025. 296 с.

Батиргареева В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. 2020. № 1 (32). С. 110–119. DOI: [https://doi.org/10.37750/2616-6798.2020.1\(32\).200388](https://doi.org/10.37750/2616-6798.2020.1(32).200388).

Бова А. А. Методичні аспекти крос-національних соціологічних опитувань щодо віктимізації та безпеки. *Наука і правоохорона*. 2017. № 1. С. 143–148.

Бова А. А. Соціологічні опитування потерпілих від злочинів в Україні. *Український соціум*. 2006. № 1 (12). С. 33–41.

В'юник М. В., Карчевський М. В., Арланова О. Д. Кримінально-правове регулювання в Україні: реалії та перспективи (аналітичні матеріали) / упоряд. Ю. В. Баулін ; Коміс. з питань прав. реформи, Робоча група з розвитку кримін. права. Харків : Право, 2020. 212 с. URL: <https://dspace.nlu.edu.ua/handle/123456789/18398> (дата звернення: 21.09.2025).

Віктимологія : навч. посіб. / В. В. Голіна, Б. М. Головкін, М. Ю. Валуїська та ін. ; за ред. В. В. Голіни, Б. М. Головкіна. Харків : Право, 2017. 308 с.

Гебура О. Члени наркобанд майже не потрапляють за ґрати. Аналіз судових рішень. *Texty.org.ua*. 17.07.2025. URL: <https://texty.org.ua/projects/115496/imitaciya-narkoborotby-chomu-pravoohoronna-systema-karaye-spozhyvachiv-a-ne-prodavciv/> (дата звернення: 21.09.2025).

Голубев В. О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту*. 1997. № 2. С. 35–40.

Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури : постанова Каб. Міністрів України від 24.03.2023 № 257. URL: <https://zakon.rada.gov.ua/laws/show/257-2023-п> (дата звернення: 21.09.2025).

ДСТУ 2226:1993. Автоматизовані системи. Терміни та визначення. Чинний від 01.07.1994. Вид. офіц. Київ, 1994. 92 с.

ДСТУ ISO/IEC 2382:2017. Інформаційні технології. Словник термінів (ISO/IEC 2382:2015, IDT). Чинний від 01.01.2019. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=75076 (дата звернення: 21.09.2025).

Дудаш Т. Особливості аргументування рішень Європейського суду з прав людини (до характеристики методологічних підходів). *Право України*. 2017. № 4. С. 86–95.

Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія : монографія / І. Р. Шинкаренко, В. О. Голубєв, М. В. Карчевський, І. Ф. Хараберюш ; МВС України, Донец. юрид. ін-т Луган. держ. ун-ту внутр. справ. Донецьк : РВВ ЛДУВС, 2007. 266 с.

Карчевський М. В. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 27. С. 267–272.

Карчевський М. В., Карчевська О. В. Структурний вимір правового регулювання ІІІ. *Український політико-правовий дискурс*. 2025. № 12. DOI: <https://doi.org/10.5281/zenodo.15782211>.

Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.

Карчевський М. В. Обчислювальне кримінологічне аргументування: поняття, можливості та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2022. № 4 (100). С. 112–126. DOI: <https://doi.org/10.33766/2524-0323.100.112-126>.

Карчевський М. В. Особливості кваліфікації шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2014. Вип. 1. С. 272–281. URL: http://nbuv.gov.ua/UJRN/Nvlduvs_2014_1_30 (дата звернення: 21.09.2025).

Карчевський М. В. Практика протидії кримінальним правопорушенням у сфері використання інформаційних технологій. *Питання боротьби зі злочинністю*. 2024. Вип. 48. С. 116–124. DOI: <https://doi.org/10.31359/2079-6242-2024-48-116>.

Карчевський М. В. Протидія злочинності в Україні: інфографіка (2013–2024) : інтерактивний довідник, 2024. URL: <https://karchevskiy.com/i-dovidnyk/> (дата звернення: 30.08.2025).

Карчевський М. В. Протидія злочинності в умовах війни: аналіз статистичних даних (2013–2023). *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 2. С. 80–90. DOI: <https://doi.org/10.32782/2311-8040/2024-2-12>.

Карчевський М. В., Савченко А. В. Особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 30. С. 254–259.

Карчевський М. В., Федюк В. В. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кримінально-правова охорона інформаційної безпеки в Україні* : монографія / за заг. ред. В. І. Борисова, О. О. Пашенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. Розд. III. С. 165–187. DOI: <https://doi.org/10.31359/9786178518899>.

Карчевський М. В., Шульженко Н. В., Куковинець Д. О. Міжнародні стандарти, рекомендації ЄС, прогресивний зарубіжний досвід щодо кримінально-правової охорони інформаційної безпеки. *Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки* : монографія : електрон. наук. вид. / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2023. Розд. 1. С. 4–86. URL: https://ivpz.kh.ua/wp-content/uploads/2024/03/Моно_Інфобезпека_2023_НДІ-ВПЗ_авт_compressed.pdf (дата звернення: 21.09.2025).

Кістяник В. І. Правова аргументація: сучасні підходи до її розуміння в зарубіжних дослідженнях. *Наукові записки НаУКМА. Серія «Юридичні науки»*. 2012. Т. 129. С. 20–22.

Козюбра М. І. Моделі (типи) юридичної аргументації. *Наукові записки НаУКМА. Серія «Юридичні науки»*. 2013. Т. 144–145. С. 3–8.

Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, В. В. Бут, В. Д. Гавловський та ін. Київ : Атіка, 2002. 240 с.

Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. ... канд. політ. наук : 21.01.01. Київ, 2005. 20 с.

Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 21.09.2025).

Конверський А. Є. Логіка : підручник. 2-ге вид., випр. Київ : Київ. ун-т, 2017. 391 с.

Кормич Б. А. Інформаційна безпека: організаційно правові основи : навч. посіб. Київ : Кондор, 2004. 384 с.

Кушнір І. П., Адамчук С. В. Протидія дезінформації: організаційно-правовий аспект. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 470–475. DOI: <https://doi.org/10.24144/2788-6018.2025.01.78>.

Ліпкан В. А. Адміністративно-правові основи забезпечення національної безпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.07. Київ, 2008. 34 с.

Лісовий В. «Комп'ютерні» злочини: питання кваліфікації. *Право України*. 2002. № 2. С. 86–88.

Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. для студентів ВНЗ. Київ : КНТ, 2007. 531 с.

Навроцький В. О. Наскрізні кримінально-правові поняття : навч. посіб. Київ : Юрінком Інтер, 2023. 376 с.

Пилипчук В. Г. Теоретико-правові проблеми розвитку законодавства у сфері національної та інформаційної безпеки України. *Інформація і право*. 2025. № 2 (53). С. 9–22. DOI: [https://doi.org/10.37750/2616-6798.2025.2\(53\).334015](https://doi.org/10.37750/2616-6798.2025.2(53).334015).

Поклад В., Кури Х. Виктимологические исследования в криминологии. *Виктимологічні аспекти злочинності. Криминологічні дослідження*. 2006. Вип. 1. Луганськ : РВВ ЛДУВС. С. 6–12.

Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III. URL: <https://zakon.rada.gov.ua/laws/show/2121-14> (дата звернення: 21.09.2025).

Проект Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції) реєстр. № 5102

від 18.02.2021. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5102&conv=9> (дата звернення: 21.09.2025).

Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку : постанова Нац. банку України від 19.05.2021 № 43. URL: <https://zakon.rada.gov.ua/laws/show/v0043500-21> (дата звернення: 21.09.2025).

Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах : постанова Нац. банку України від 02.07.2019 № 88. URL: <https://zakon.rada.gov.ua/laws/show/v0088500-19> (дата звернення: 21.09.2025).

Про затвердження річних форм звітів щодо здійснення правосуддя місцевими та апеляційними судами : наказ Держ. суд. адміністрації України від 23.06.2018 № 325. URL: <https://zakon.rada.gov.ua/rada/show/v0325750-18> (дата звернення: 21.09.2025) ; Про затвердження форм єдиної звітності про стан кримінальної протиправності : наказ Офісу Ген. прокурора України від 30.06.2020 № 299. URL: <https://zakon.rada.gov.ua/laws/show/v0299905-20> (дата звернення: 21.09.2025).

Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. *Відомості Верховної Ради України*. 2023. № 51. Ст. 127.

Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20> (дата звернення: 21.09.2025).

Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. URL: <https://zakon.rada.gov.ua/laws/show/2824-15> (дата звернення: 21.09.2025).

Про Стратегію інформаційної безпеки : рішення Ради нац. безпеки і оборони України від 15.10.2021, введ. в дію Указом Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21> (дата звернення: 21.09.2025).

Рабінович П. М., Дудаш Т. І. Правова аргументація: терміно-поняттєвий інструментарій дослідження. *Вісник Національної академії правових наук України*. 2016. № 2. С. 8–20. URL: http://nbuv.gov.ua/UJRN/varpu_2016_2_3 (дата звернення: 21.09.2025).

Радутний О. Штучний інтелект як суб'єкт кримінального права. *Право України*. 2018. № 1. С. 123–136. DOI: <https://doi.org/10.33498/lopu-2018-01-123>.

Розовський Б. Г. Карному кодексу слід надати нагадування-епіграф: «Багато розстріляних було посмертно реабілітовано!». *Актуальні проблеми права: теорія і практика*. 2020. № 2 (40). С. 20–50.

Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія. Київ : ДКС, 2012. 340 с.

Сашук Г. М. Безпекові імперативи телевізійного простору України : автореф. дис. ... канд. політ. наук : 23.00.03. Київ, 2005. 16 с.

Синхронізація. *Словник української мови. Академічний тлумачний словник (1970–1980)*. URL: <https://sum.in.ua/s/synkhronizacija> (дата звернення: 21.09.2025).

Скляренко О. А. Сучасні проблеми інформаційної безпеки України в умовах внутрішніх трансформацій. *Актуальні проблеми міжнародних відносин*. 2006. Вип. 64, ч. I. С. 125–131.

Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави : автореф. дис. ... канд. юрид. наук : 12.00.01. Київ, 2011. 19 с.

Туляков В. О. Вчення про жертву злочину: соціальні та правові основи : автореф. дис. ... д-ра. юрид. наук : 12.00.08. Одеса, 2001. 36 с.

Усманов Р. А. Кримінальна відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням комп'ютерної техніки : дис. ... д-ра філософії : 081. Кропивницький, 2024. 252 с.

Усманов Р. А. Шахрайство з використанням електронно-обчислювальної техніки: аналіз судової практики. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 1. С. 153–163. DOI: <https://doi.org/10.32782/2311-8040/2024-1-19>.

Філософський енциклопедичний словник / НАН України, Ін-т філософії ім. Г. С. Сковороди ; редкол.: В. І. Шинкарук (голова) та ін. ; наук. ред. Л. В. Озадовська, Н. П. Поліщук. Київ : Абрис, 2002. 742 с.

Шехавцов Р. М., Хавронюк М. І. Звіт щодо кримінальної статистики в Україні / Центр політико-прав. реформ. Київ, 2019. 80 с. URL: <https://pravo.org.ua/books/zvit-shhodo-kryminalnoyi-statystyky-v-ukrayini/> (дата звернення: 21.09.2025).

Щербина О. Ю. До питання про розуміння аргументації у логіко-юридичних дослідженнях. *Гуманітарні студії*. 2014. Вип. 21. С. 45–53.

Akinoyemi B., Adewusi O., Oyeboade A. An improved classification model for fake news detection in social media. *International Journal of Information*

Technology and Computer Science. 2020. Vol. 12, No. 1. P. 34–43. DOI: <https://doi.org/10.5815/ijitcs.2020.01.05>.

Badade A. B., Dhanaraj R. K. Astroturfing: understanding and addressing the influence of fake grassroots movements across diverse domains on social media platforms. *Proceedings of Fourth International Conference on Computing and Communication Networks. ICCCN 2024* / Eds.: A. Kumar, A. Swaroop, P. Shukla. Springer, Singapore, 2025. P. 527–538. (Lecture Notes in Networks and Systems ; Vol. 1317). DOI: https://doi.org/10.1007/978-981-96-3942-7_40.

Benefit-cost analysis of a randomized evaluation of Communities That Care: Monetizing intervention effects on the initiation of delinquency and substance use through grade 12 / M. R. Kuklinski, A. A. Fagan, J. D. Hawkins et al. *Journal of Experimental Criminology*. 2015. Vol. 11, Iss. 2. P. 165–192. DOI: <https://doi.org/10.1007/s11292-014-9226-3>. PMID: 26213527; PMCID: PMC4512954.

Berk R. A. Artificial intelligence, predictive policing, risk assessment for law enforcement. *Annual Review of Criminology*. 2021. Vol. 4. P. 209–237. DOI: <https://doi.org/10.1146/annurev-criminol-051520-012342>.

Berk R. Demystifying AI in criminal justice. *arXiv*. 2025, July 28. 25 p. DOI: <https://doi.org/10.48550/arXiv.2507.19305>.

Bossler A. M., Berenblum T. Introduction: new directions in cybercrime research. *Journal of Crime and Justice*. 2019. Vol. 42, Iss. 5. P. 495–499. DOI: <https://doi.org/10.1080/0735648X.2019.1692426>.

Bostrom N. Deep Utopia: Life and meaning in a solved world. Ideapress Publishing, 2024. 525 p.

Brave New Coin : вебсайт. URL: <https://bravenewcoin.com> (дата звернення: 21.09.2025).

Brenner S. W. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara : Praeger, 2010. 284 p. (Crime, Media, and Popular Culture / Series eds.: F. Y. Bailey, S. Chermak). DOI: <https://doi.org/10.5040/9798400636554>.

Burton J., Janjeva A., Moseley S., Alice. AI and Serious Online Crime : CETaS Research Reports / The Alan Turing Institute. 2025, March. 32 p. URL: https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_report_-_ai_and_serious_online_crime_0.pdf (дата звернення: 21.09.2025).

Chisholm J. Benefit-cost analysis and crime prevention. Canberra : Australian Institute of Criminology, 2000. 6 p. (Trends & issues in crime and

criminal justice ; no. 147). URL: <https://www.aic.gov.au/publications/tandi/tandi147> (дата звернення: 21.09.2025).

Christian B. The alignment problem : How can machines learn human values? Atlantic Books, 2021. 496 p.

Cioffi-Revilla C. Computational social science. *Wiley Interdisciplinary Reviews Computational Statistics*. 2010. Vol. 2, Iss. 3. P. 259–271. DOI: <https://doi.org/10.1002/wics.95>.

Combating virtual assets-based money laundering and crypto-enabled crime: 2021 Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies / Basel Institute on Governance ; Interpol ; Europol. *Basel Institute on Governance*. URL: <https://baselgovernance.org/publications/combating-virtual-assets-based-money-laundering-and-crypto-enabled-crime> (дата звернення: 21.09.2025).

Constitutional dimensions of predictive algorithms in criminal justice / M. Brenner, J. Suk Gersen, M. Haley et al. *Harvard Civil Rights-Civil Liberties Law Review*. 2020. Vol. 55. P. 267–310. URL: <https://journals.law.harvard.edu/crcl/wp-content/uploads/sites/80/2020/09/Brenner-et-al.pdf> (дата звернення: 21.09.2025).

Cybercrime Classification and Measurement : Consensus Study Report / Eds.: H. S. Stern, D. L. Cork ; National Academies of Sciences, Engineering, and Medicine. Washington, DC : The National Academies Press, 2025. XX, 140 p. DOI: <https://doi.org/10.17226/29048>.

Daniels G. The «Average Man»? : technical report, accession number AD0010203 / Air Force Aerospace Medical Research Lab. 1977, April 25. URL: <https://apps.dtic.mil/sti/citations/tr/AD0010203> (дата звернення: 21.09.2025).

Demony C. Britain to make sexually explicit ‘deepfakes’ a crime. *Reuters*. 2025, January 7. URL: <https://www.reuters.com/world/uk/britain-make-sexually-explicit-deepfakes-crime-2025-01-07/> (дата звернення: 21.09.2025).

DOJ report on AI in criminal justice: key takeaways. *Council on Criminal Justice*. 2025, April. URL: <https://counciloncj.org/doj-report-on-ai-in-criminal-justice-key-takeaways/> (дата звернення: 21.09.2025).

Dooley S., Yamada H. ‘Suitcase Killer’ Melanie McGuire defends innocence from inside prison. *ABC News*. 2020, September 24. URL: <https://>

abcnews.go.com/US/suitcase-killer-melanie-mcguire-defends-innocence-inside-prison/story?id=73099717 (дата звернення: 21.09.2025).

Dragulescu A., Arendt C. *xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files*. R package version 0.6.5. 2020. URL: <https://CRAN.R-project.org/package=xlsx> (дата звернення: 21.09.2025).

Dressel J., Farid H. The accuracy, fairness, and limits of predicting recidivism. *Science Advances*. 2018. Vol. 4, No. 1. eaao5580. DOI: <https://doi.org/10.1126/sciadv.aao5580>.

Dupont B., Stevens Y., Westermann H., Joyce M. Artificial intelligence in the context of crime and criminal justice : A report for the Korean Institute of Criminology. 2018, December. P. 24–28. URL: <https://www.researchgate.net/publication/337402608> (дата звернення: 21.09.2025).

El Capitan: NNSA's first exascale machine. *Advanced Simulation and Computing*. URL: <https://asc.llnl.gov/exascale/el-capitan> (дата звернення: 21.09.2025).

El Capitan retains top spot in 65th TOP500 list as Exascale Era expands. *TOP500*. URL: <https://top500.org/news/el-capitan-retains-top-spot-65th-top500-list-exascale-era-expands/> (дата звернення: 21.09.2025).

ENIAC. *Engineering and Technology History Wiki*. URL: <https://ethw.org/ENIAC> (дата звернення: 21.09.2025) ; The ENIAC by J. Presper Eckert and John W. Mauchly / Computer History Museum. *YouTube*. 2022, June 10. URL: <https://www.youtube.com/watch?v=7GuXDcMfGfA> (дата звернення: 21.09.2025).

European Ethical Charter on the use of artificial intelligence in judicial systems and their environment : Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018) / European Commission for the Efficiency of Justice (CEPEJ). Strasbourg : Council of Europe, 2018. 77 p. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (дата звернення: 21.09.2025).

Falk R., Brown A.-L. Poison the well : AI, data integrity and emerging cyber threats / Cyber Security Cooperative Research Centre. 2023. 16 p. URL: <https://cybersecuritycrc.org.au/remote-assets/sites/default/files/2023-11/Poison%20the%20well%20-%20AI%2C%20data%20integrity%20and%20emerging%20cyber%20threats.pdf> (дата звернення: 23.08.2025).

Faulkner A. From case law to code: Evaluating AI's role in the justice system. *Montreal AI Ethics Institute*. 2025, May 26. URL: <https://>

montrealethics.ai/from-case-law-to-code-evaluating-ais-role-in-the-justice-system/ (дата звернення: 19.08.2025).

Ferguson A. G. The rise of big data policing : Surveillance, race, and the future of Law enforcement. New York : New York University Press, 2017. DOI: <https://doi.org/10.2307/j.ctt1pwtb27>.

Feteris E. T. Fundamentals of legal argumentation : A survey of theories on justification of judicial decisions. 2nd ed. Dordrecht : Springer, 2017. 225 p. (Argumentation Library ; Vol. 1).

Forrester D., Frenz S., O'Connell M., Pease K. The Kirkholt burglary prevention project: Phase II : Crime prevention unit paper 23. London : Home Office, 1990. VI, 50 p. (Crime Prevention Unit Papers). URL: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0503146df6dffa3c65ffd4247e84ffa0783b2ba0> (дата звернення: 21.09.2025).

Fotoohi S., Saeidi S. Discovering the maximum clique in social networks using artificial bee colony optimization method. *International Journal of Information Technology and Computer Science*. 2019. Vol. 11, No. 10. P. 1–11. DOI: <https://doi.org/10.5815/ijitcs.2019.10.01>.

Fraud attempt against a federal agency using deepfake technology / ID.ME. *YouTube*. 2025, January 7. URL: https://youtu.be/iCQhW6BXx_I?si=j6eRDdShYecw7O_m (дата звернення: 21.09.2025).

Freiberger P. A., Swaine M. R. ENIAC. *Encyclopedia Britannica*. Last updated: 2025, August 24. URL: <https://www.britannica.com/technology/ENIAC> (дата звернення: 21.09.2025).

Giddens A., Griffiths S. Sociology. Cambridge : Polity Press, 2006. 5th ed., fully rev. and upd. XXV, 1093 p.

Guggenberger N., Salib P. N. From fake news to fake views: New challenges posed by ChatGPT-like AI. *Lawfare*. 2023, January 20. URL: www.lawfaremedia.org/article/fake-news-fake-views-new-challenges-posed-chatgpt-ai (дата звернення: 21.09.2025).

Hägele S. Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review. *Electron Markets*. 2024. Vol. 34. Art. 33. 22 p. DOI: <https://doi.org/10.1007/s12525-024-00714-2> ; Zhou Z., Shen B. Toward understanding the use of centralized exchanges for decentralized cryptocurrency. *arXiv*. 2022. DOI: <https://doi.org/10.48550/arXiv.2204.08664>.

Hall B. How AI-driven fraud challenges the global economy – and ways to combat it. *World Economic Forum*. 2025, January 16. URL: <https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/> (дата звернення: 21.09.2025).

Hallucination-free? Assessing the reliability of leading AI legal research tools / V. Magesh, F. Surani, M. Dahl et al. *Journal of Empirical Legal Studies*. 2025. Vol. 22, Iss. 2. P. 216–242. DOI: <https://doi.org/10.1111/jels.12413>.

Hao K. AI is sending people to jail – and getting it wrong. *MIT Technology Review*. 2019, January 21. URL: <https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/> (дата звернення: 21.09.2025).

Hazra T., Kumar C. R. S., Nene M. J. Strategies for searching targets using mobile sensors in defense scenarios. *International Journal of Information Technology and Computer Science*. 2017. Vol. 9, No. 5. P. 61–70. DOI: <https://doi.org/10.5815/ijitcs.2017.05.08>.

Hill K. How target figured out a teen girl was pregnant before her father did. *Forbes*. 2012, February 16. URL: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> (дата звернення: 21.09.2025).

Hox J. J. Computational social science methodology, anyone? *Methodology*. 2017. Vol. 13, Iss. suppl. 1. P. 3–12. DOI: <https://doi.org/10.1027/1614-2241/a000127>.

Hua R. AI and racial Bias in legal decision-making: A student fellow project. *Harvard Law School*. 2025, March 19. URL: <https://clp.law.harvard.edu/knowledge-hub/insights/ai-and-racial-bias-in-legal-decision-making-a-student-fellow-project/> (дата звернення: 21.09.2025).

Hung T. W., Yen C. P. Predictive policing and algorithmic fairness. *Synthese*. 2023. Vol. 201, Iss. 3. P. 1–25. DOI: <https://doi.org/10.1007/s11229-023-04189-0>.

Ibarra N. Santa Cruz becomes first U. S. city to approve ban on predictive policing. *Santa Cruz Sentinel*. 2020, June 25. URL: <https://www.santacruzsentinel.com/2020/06/23/santa-cruz-becomes-first-u-s-city-to-approve-ban-on-predictive-policing/> (дата звернення: 21.09.2025).

ICT specialists in employment. *Eurostat*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment (дата звернення: 21.09.2025).

Impact of artificial intelligence on criminal and illicit activities / Department of Homeland Security. Public-Private Analytic Exchange Program, 2024. 59 p. URL: https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf (дата звернення: 21.09.2025).

Iskandarli G. Y. Applying clustering and topic modeling to automatic analysis of citizens' comments in e-government. *International Journal of Information Technology and Computer Science*. 2020. Vol. 12, No. 6. P. 1–10. DOI: <https://doi.org/10.5815/ijitcs.2020.06.01>.

Joh E. E. The new surveillance discretion: Automated suspicion, big data, and policing. *Harvard Law & Policy Review*. 2016. Vol. 10. P. 15–42.

Joint declaration [of the United Nations Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression] on freedom of expression and elections in the digital age. 2020, 30 April. URL: https://www.ohchr.org/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf (дата звернення: 21.09.2025).

Jorgensen R. Algorithms and the individual in criminal law. *Canadian Journal of Philosophy*. 2022. Vol. 52, Iss. 1. P. 61–77. DOI: <https://doi.org/10.1017/can.2021.28>.

Kop M. EU Artificial Intelligence Act: The European approach to AI. *Transatlantic Antitrust and IPR Developments* / Transatlantic Technology Law Forum. 2021. № 2. P. 8–18. URL: <https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/> (дата звернення: 21.09.2025).

Kosinski M., Stillwell D., Graepel T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*. 2013, March 11. Vol. 110, No. 15. P. 5802–5805. DOI: <https://doi.org/10.1073/pnas.1218772110>.

Kure H. I., Sarkar P., Ndanusa A. B., Nwajana A. O. Detecting and preventing data poisoning attacks on AI models. *arXiv*. 2025, March 25. 9 p. DOI: <https://doi.org/10.48550/arXiv.2503.09302>.

Leffer L. In the race to artificial general intelligence, where's the finish line? *Scientific American*. 2024, June 25. DOI: <https://doi.org/10.1038/scientificamerican032025-5u0fPrUaVI3TKyo4zEF29s>.

Leukfeldt E. R., Yar M. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behavior*. 2016. Vol. 37, Iss. 3. P. 263–280. DOI: <https://doi.org/10.1080/01639625.2015.1012409>.

Lim G., Bradshaw S. Chilling legislation: Tracking the impact of «fake news» laws on press freedom internationally. *Center for International Media Assistance*. 2023, July 23. URL: <https://www.cima.ned.org/publication/chilling-legislation> (дата звернення: 21.09.2025).

Lum K., Isaac W. To predict and serve? *Significance*. 2016. Vol. 13, Iss. 5. P. 14–19. DOI: <https://doi.org/10.1111/j.1740-9713.2016.00960.x>.

Lum K., Johndrow J. E. A statistical framework for fair predictive algorithms. *arXiv*. 2016. DOI: <https://doi.org/10.48550/arXiv.1610.08077>.

Lumley L. Deepfake fraud directed at banks on the rise. *The Banker*. 2024, June 12. URL: <https://www.thebanker.com/Deepfake-fraud-directed-at-banks-on-the-rise-1718178559> (дата звернення: 21.09.2025).

Lusthaus J. Reconsidering crime and technology: what is this thing we call cybercrime? *Annual Review of Law and Social Science*. 2024. Vol. 20. P. 369–385. DOI: <https://doi.org/10.1146/annurev-lawsocsci-041822-044042>.

Manifesto of computational social science / R. Conte, N. Gilbert, G. Bonelli et al. *European Physical Journal Special Topics*. 2012. 22 p. URL: <http://www.everyaware.eu/resources/publications/Conte-2012.pdf> (дата звернення: 19.09.2025).

Mann A. Core concept: Computational social science. *Proceedings of the National Academy of Sciences*. 2016, January 19. Vol. 113, No. 3. P. 468–470. DOI: <https://doi.org/10.1073/pnas.1524881113>.

Manning M. Cost-Benefit Analysis. *Encyclopedia of Criminology and Criminal Justice* / Eds.: G. Bruinsma, D. Weisburd. New York : Springer, 2014. P. 641–651. DOI: https://doi.org/10.1007/978-1-4614-5690-2_176.

Marciniak D. Algorithmic policing: an exploratory study of the algorithmically mediated construction of individual risk in a UK police force. *Policing and Society*. 2023. Vol. 33, Iss. 4. P. 449–463. DOI: <https://doi.org/10.1080/10439463.2022.2144305>.

Masnick M. Twenty years ago today: Barbra Streisand sued a photographer, and the Streisand effect was born. *Techdirt*. 2023, May 20. URL: <https://www.techdirt.com/2023/05/20/twenty-years-ago-today-barbra-streisand-sued-a-photographer-and-the-streisand-effect-was-born> (дата звернення: 25.08.2025).

McGuire M., Dowling S. Cyber crime: A review of the evidence / Home Office. October 2013. (Research Report 75). URL: <https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence> (дата звернення: 21.09.2025).

Noordt C. van, Misuraca G. Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union. *Government Information Quarterly*. 2022. Vol. 39, Iss. 3. Art. 101714. DOI: <https://doi.org/10.1016/j.giq.2022.101714>.

O'Connor S., Liu H. Gender bias perpetuation and mitigation in AI technologies: challenges and opportunities. *AI & Society*. 2024. Vol. 39. P. 2045–2057. DOI: <https://doi.org/10.1007/s00146-023-01675-4>.

Palmirani M., Vitali F., Van Puymbroeck W., Durango F. N. Drafting legislation in the era of AI and digitisation. Brussels : European Commission, Directorate-General for Informatics, 2022. 96 p. URL: <https://interoperable-europe.ec.europa.eu/sites/default/files/document/2022-06/Drafting%20legislation%20in%20the%20era%20of%20AI%20and%20digitisation%20-%20study.pdf> (дата звернення: 21.09.2025).

Patrock R. 'Reading tea leaves': An assessment of the reliability of police recorded crime statistics. *The Police Journal*. 2011. Vol. 84, Iss. 1. P. 47–67. DOI: <https://doi.org/10.1350/POJO.2011.84.1.512>.

Peng R. D. Reproducible research in computational science. *Science*. 2011. Vol. 334, Iss. 6060. P. 1226–1227. DOI: <https://doi.org/10.1126/science.1213847>.

Piscione D. P. It's Time for Your Company to Invest in AI. Here's How. *Harvard Business Review*. 2025, July 2. URL: <https://hbr.org/2025/07/its-time-for-your-company-to-invest-in-ai-heres-how> (дата звернення: 21.09.2025).

Positron : The data science code editor / Posit Software, PBC formerly RStudio, PBC. URL: <https://posit.co/> (дата звернення: 21.09.2025).

Prakken H., Sartor G. Law and logic: A review from an argumentation perspective. *Artificial Intelligence*. 2015. Vol. 227. P. 214–245. DOI: <https://doi.org/10.1016/j.artint.2015.06.005>.

Provost F., Fawcett T. Data science and its relationship to big data and data-driven decision making. *Big Data*. 2013. Vol. 1, No. 1. P. 51–59. DOI: <https://doi.org/10.1089/big.2013.1508>.

Ranaweera N. Beyond numbers: Embracing the depth of qualitative research in criminology affiliations. *International Journal of Qualitative*

Research. 2024. Vol. 3, Iss. 3. P. 315–325. DOI: <https://doi.org/10.47540/ijqr.v3i3.1346>.

Regan G. The State of Deepfake Regulations in 2025: What Businesses Need to Know. *Reality Defender*. 2025, June 18. URL: <https://www.realitydefender.com/insights/the-state-of-deepfake-regulations-in-2025-what-businesses-need-to-know> (дата звернення: 21.09.2025).

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj> (дата звернення: 21.09.2025).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата звернення: 21.09.2025).

Rodger H., Lensen A., Betkier M. Explainable artificial intelligence for assault sentence prediction in New Zealand. *Journal of the Royal Society of New Zealand*. 2022. Vol. 53, Iss. 1. P. 133–147. DOI: <https://doi.org/10.1080/03036758.2022.2114506>. PMID: 39439993; PMCID: PMC11459755.

Runaway feedback loops in predictive policing / D. Ensign, S. A. Friedler, S. Neville et al. *Proceedings of Machine Learning Research*. 2018. Vol. 81 : Proceedings of the 1st Conference on Fairness, Accountability and Transparency. P. 160–171. URL: <https://proceedings.mlr.press/v81/ensign18a.html> (дата звернення: 21.09.2025).

Russell S. Artificial intelligence and the problem of control. *Perspectives on digital humanism* / Eds.: H. Werthner, E. Prem, E. A. Lee, C. Ghezzi. Springer, 2022. P. 19–24. DOI: https://doi.org/10.1007/978-3-030-86144-5_3.

Russell S. Q & A: The future of artificial intelligence. *UC Berkeley. Electrical Engineering and Computer Sciences*. URL: <https://people.eecs.berkeley.edu/~russell/research/future/q-and-a.html> (дата звернення: 21.09.2025).

Ryberg J. Artificial intelligence and criminal justice: How to use algorithmic sentencing support in real life (and ethically non-ideal) penal

systems? *AI Ethics*. 2025. Vol. 5. P. 3255–3263. DOI: <https://doi.org/10.1007/s43681-024-00655-8>.

Ryberg J. Criminal sentencing and artificial intelligence: What is the input problem? *Criminal Law and Philosophy*. 2025. Vol. 19. P. 203–220. DOI: <https://doi.org/10.1007/s11572-024-09739-2>.

Sanger R. Artificial intelligence and criminal law. *The Colleges of Law*. 2024, January 12. URL: <https://www.collegesoflaw.edu/blog/2024/01/12/artificial-intelligence-and-criminal-law/> (дата звернення: 08.08.2025).

Schulte T., Bohnet-Joschko S. How can big data analytics support people-centred and integrated health services: A scoping review. *International Journal of Integrated Care*. Jun 16, 2022. Vol. 22. Art. 23. DOI: <https://doi.org/10.5334/ijic.5543>. PMID: 35756337; PMCID: PMC9205381.

Sedgwick K. Bitcoin is Great for Criminals. It's Even Better for Law Enforcement. *Bitcoin.com*. 2018, July 16. URL: <https://news.bitcoin.com/bitcoin-is-great-for-criminals-its-even-better-for-law-enforcement/> (дата звернення: 21.09.2025).

Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering: 2022 Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies / Basel Institute on Governance ; Europol. *Basel Institute on Governance*. URL: <https://baselgovernance.org/publications/seizing-opportunity-5-recommendations-crypto-assets-related-crime-and-money-laundering> (дата звернення: 21.09.2025).

shiny: Web Application Framework for R / W. Chang, J. Cheng, J. J. Allaire et al. R package version 1.11.1. 2025. URL: <https://CRAN.R-project.org/package=shiny> (дата звернення: 21.09.2025).

Stelmach J., Brożek B. Methods of legal reasoning. Springer, 2006. 236 p. (Law and Philosophy Library ; Vol. 78).

Textreadr. *GitHub*. URL: <https://github.com/trinker/textreadr> (дата звернення: 21.09.2025).

The EU AI act. *AP4AI*. URL: <https://ap4ai.eu/eu-ai-act> (дата звернення: 21.09.2025).

The R Project for Statistical Computing : вебсайт / R Core Team ; R. Foundation for Statistical Computing, Vienna, Austria. URL: <https://www.r-project.org/> (дата звернення: 21.09.2025).

The risks associated with Artificial General Intelligence: A systematic review / S. McLean, G. J. M. Read, J. Thompson et al. *Journal of Experimental & Theoretical Artificial Intelligence*. 2021. Vol. 35, Iss. 5. P. 649–663. DOI: <https://doi.org/10.1080/0952813X.2021.1964003>.

The 2025 Crypto Crime Report. *Chainalysis*. 2025, February. URL: <https://www.chainalysis.com/crypto-crime-2025-report> (дата звернення: 25.08.2025).

Thomas L. The youngest science : Notes of a medicine-watcher. Penguin Books, 1995. 272 p.

Titah R. How AI skews our sense of responsibility. *MIT Sloan Management Review*. 2024, May 13. URL: <https://sloanreview.mit.edu/article/how-ai-skews-our-sense-of-responsibility/> (дата звернення: 21.09.2025).

Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (Take It Down) Act. *Congress.gov*. 22.01.2025. URL: <https://www.congress.gov/congressional-record/congressional-record-index/118th-congress/2nd-session/tools-to-address-known-exploitation-by-immobilizing-technological-deepfakes-on-websites-and-networks-take-it-down-act/1918605> (дата звернення: 21.09.2025).

Trejo O. What is Bias in machine learning? Real-world examples that show the impact of AI Bias. *Scalable Path*. Originally published on May 4, 2020, last updated on August 28, 2024. URL: <https://www.scalablepath.com/machine-learning/bias-machine-learning> (дата звернення: 21.09.2025).

Tversky A., Kahneman D. Judgment under uncertainty: heuristics and biases. *Science*. 1974. Vol. 185, No. 4157. P. 1124–1131. DOI: <https://doi.org/10.1126/science.185.4157.1124>.

United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes : Resolution 79/243 adopted by the United Nations General Assembly on 24 December 2024 : A/RES/79/243. URL: <https://undocs.org/en/A/RES/79/243> (дата звернення: 21.09.2025).

Vaccaro M., Waldo J. The effects of mixing machine learning and human judgment. *ACM Queue*. 2019. Vol. 17, Iss. 4. 22 p. DOI: <https://doi.org/10.1145/3358955.3363293>.

Vidal-Tomás D. Centralised exchanges & proof-of-solvency: The guardians of trust. *SSRN*. 2024, February 15. 49 p. DOI: <https://doi.org/10.2139/ssrn.4761565>.

Wachter S., Mittelstadt B., Russell C. Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*. 2018. Vol. 31, Iss. 2. P. 841–887. DOI: <https://doi.org/10.48550/arXiv.1711.00399>.

Weiss K. R. Barbra Streisand sues to keep Malibu home photos off web site. *Los Angeles Times*. 2003, May 30. URL: <https://www.latimes.com/archives/la-xpm-2003-may-30-me-barbra30-story.html> (дата звернення: 25.08.2025).

Welcome to the tidyverse / Wickham H., Averick M., Bryan J. et al. *Journal of Open Source Software*. 2019. Vol. 4, Iss. 43. Art. 1686. 6 p. DOI: <https://doi.org/10.21105/joss.01686>.

What is a data poisoning? [Examples & Prevention]. *Palo Alto Networks*. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-data-poisoning> (дата звернення: 23.08.2025).

What is AI data poisoning? *Cloudflare*. URL: <https://www.cloudflare.com/learning/ai/data-poisoning/> (дата звернення: 23.08.2025).

What is artificial general intelligence (AGI)? *Google Cloud*. URL: <https://cloud.google.com/discover/what-is-artificial-general-intelligence> (дата звернення: 22.08.2025).

What is strong AI? *IBM*. URL: <https://www.ibm.com/think/topics/strong-ai> (дата звернення: 22.08.2025).

Wickham H. stringr: Simple, Consistent Wrappers for Common String Operations. R package version 1.5.2. 2025. URL: <https://CRAN.R-project.org/package=stringr> (дата звернення: 21.09.2025).

Wickham H., Bryan J. readxl: Read Excel Files. R package version 1.4.5. 2025. URL: <https://CRAN.R-project.org/package=readxl> (дата звернення: 21.09.2025).

Wickham H., Hester J., Bryan J. readr: Read Rectangular Text Data. R package version 2.1.5. 2024. URL: <https://CRAN.R-project.org/package=readr> (дата звернення: 21.09.2025).

Xie Y., Cheng J., Tan X., Aden-Buie G. DT: A Wrapper of the JavaScript Library ‘DataTables’. R package version 0.34.0. 2025. URL: <https://CRAN.R-project.org/package=DT> (дата звернення: 21.09.2025).

Yuval Noah Harari argues that AI has hacked the operating system of human civilisation. *The Economist*. 2023, April 28. URL: <https://www.economist.com/by-invitation/2023/04/28/yuval-noah-harari-argues-that-ai-has-hacked-the-operating-system-of-human-civilisation> (дата звернення: 21.09.2025).

Zalnieriute M. Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law*. 2022. Vol. 116, Iss. 3. P. 585–592. DOI: <https://doi.org/10.1017/ajil.2022.35>.

2024 AI, fraud, and financial crime survey : AI's role in perpetrating and fighting financial crime. *Biocatch*. URL: <https://www.biocatch.com/ai-fraud-financial-crime-survey> (дата звернення: 21.09.2025).

7th Global Conference on Criminal Finances and Cryptocurrencies. *Basel Institute on Governance*. URL: <https://baselgovernance.org/node/2446> (дата звернення: 21.09.2025).

Зміст

Передмова	4
Вступ	5
Розділ 1. Інформаційна безпека	8
Розділ 2. «Комп'ютерний» злочин	12
Розділ 3. Науково-практичний коментар до розділу XVI Особливої частини Кримінального кодексу України та критична оцінка поточної судової практики	16
3.1. Несанкціоноване втручання (ст. 361 Кримінального кодексу України)	20
3.2. Шкідливі програмні або технічні засоби (ст. 361-1 Кримінального кодексу України)	26
3.3. Розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 Кримінального кодексу України)	28
3.4. Незаконні дії осіб, які мають право доступу до комп'ютерної інформації (ст. 362 Кримінального кодексу України)	30
3.5. Порухнення правил експлуатації комп'ютерної техніки, порядку чи правил захисту інформації (ст. 363 Кримінального кодексу України)	32
3.6. Масове розповсюдження повідомлень електров'язку (ст. 363-1 Кримінального кодексу України)	35
3.7. Що «не так» із протидією кримінальним правопорушенням у сфері використання інформаційних технологій	37
Висновки	42
Розділ 4. Кримінальні правопорушення проти власності, що вчиняються з використанням комп'ютерів	45
4.1. «Комп'ютерне» шахрайство	49
4.2. Кримінальні правопорушення щодо віртуальних активів	54
Висновки	65
Розділ 5. «Некомп'ютерні» посягання на інформаційну безпеку	67
5.1. Порухнення обмеженого доступу до інформації	67
5.2. Кримінально-правова охорона формування інформаційного простору	70
Висновки	74

Розділ 6. Інформаційні технології та аналіз злочинності	75
6.1. Обчислювальне кримінологічне аргументування	76
6.2. «CrimeDataLab»: сучасний аналіз відкритих даних щодо протидії злочинності в Україні	81
6.3. Обмеженість обчислювального кримінологічного аргументування та шляхи її подолання	99
Висновки	109
 Розділ 7. Штучний інтелект і кримінальне право	 111
7.1. Можливості й ризики, які створює штучний інтелект у сфері кримінальної юстиції	112
7.2. Правове регулювання використання штучного інтелекту	121
7.3. Використання штучного інтелекту для вчинення кримінальних правопорушень	133
7.4. Динамічні санкції: один із можливих напрямів використання штучного інтелекту в кримінально-правовому регулюванні	141
Висновки	147
 Висновки	 149
Подяки	152
Список використаних джерел	155

Наукове видання

Карчевський Микола Віталійович

**КРИМІНАЛЬНЕ ПРАВО В УМОВАХ
ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.
Від несанкціонованого доступу
до «jailbreak» штучного інтелекту**

Монографія

Коректорка *М. А. Ковальчук*

Редактор виносок і списку використаних джерел *П. О. Білоус*

Підписано до друку 11.11.2025. Формат 60×84/16.
Ум. друк. арк. 10,2. Обл.-вид. арк. 8. Тираж 100 пр. Зам. № 462

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20, (063) 254-50-84
Вебсайт: <https://pravo-izdat.com.ua>
E-mail для замовників послуг: verstka@pravo-izdat.com.ua
E-mail для покупців: sales@pravo-izdat.com.ua
Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт»,
вул. Весніна, 12, Харків, 61023, Україна
Тел. (057) 717-25-44
Свідоцтво суб'єкта видавничої справи ДК № 5748 від 06.11.2017