

DOI: 10.33270/05267303.2
УДК 343.81

БОГАТИРЬОВ Іван*

доктор юридичних наук, професор, професор кафедри кримінально-виконавчого права та кримінального права Пенітенціарної академії України
14000, вул. Гонча, 34, м. Чернігів, Україна
ORCID: <https://orcid.org/0000-0003-4001-7256>

Іноземні практики розвитку цифрової кримінології: інноваційний напрям

Анотація. Статтю присвячено комплексному аналізу сучасних іноземних практик розвитку цифрової кримінології як інноваційного напрямку кримінологічної науки, що формується під впливом глобальної цифровізації суспільних відносин і стрімкого розвитку інформаційно-комунікаційних технологій. Актуальність дослідження зумовлена необхідністю переосмислення традиційних кримінологічних підходів до вивчення злочинності в умовах цифрового середовища, поширення кіберзлочинності, використання штучного інтелекту, технологій великих даних (Big Data), алгоритмів машинного навчання та цифрової кримінологічної аналітики. За результатами наукового пошуку встановлено, що в провідних зарубіжних країнах цифрова кримінологія розвивається як міждисциплінарний науковий напрям, орієнтований на інтеграцію кримінологічних знань із досягненнями цифрових технологій, науки про дані та штучного інтелекту. Проаналізовано особливості використання алгоритмів прогнозування злочинності, кримінологічної аналітики, цифрової кримінальної розвідки, геоінформаційних систем, інструментів аналізу відкритих джерел інформації та інших сучасних технологічних рішень у діяльності правоохоронних органів США, Великої Британії, країн Європейського Союзу, а також Сінгапуру та Китаю. Визначено основні переваги цифрової трансформації кримінологічної діяльності, а також окреслено правові, етичні й організаційні ризики, пов'язані із застосуванням алгоритмічних моделей прийняття рішень, опрацюванням персональних даних і забезпеченням цифрових прав людини. Сформульовано висновок, що впровадження міжнародних практик цифрової кримінології сприятиме підвищенню ефективності кримінологічного прогнозування, удосконаленню механізмів запобігання злочинності, розвитку доказово орієнтованої кримінологічної політики та модернізації діяльності правоохоронних органів в умовах цифрової трансформації держави.

Ключові слова: іноземні практики; цифрова кримінологія; кіберзлочинність; штучний інтелект; Big Data; прогнозування; кримінальне правопорушення; правоохоронна діяльність.

Історія статті:

Отримано: 02.07.2026
Прийнято: 31.08.2026
Опубліковано: 01.10.2026

Рекомендоване посилання:

Богатирьов І. Іноземні практики розвитку цифрової кримінології: інноваційний напрям. *Наука і правоохорона*. 2026. Вип. 3 (73). С. 17–24. DOI: 10.33270/05267303.2

*Відповідальний автор



© Богатирьов І., 2026. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

Вступ

Українські вчені одноставно визначають сучасне суспільство як цифрове. Особливо це виявилось в умовах російсько-української війни, де цифрові технології стали невід'ємною складовою функціонування держави, економіки та повсякденного життя громадян. Вони забезпечують безперервність державного управління, надання адміністративних послуг, організацію дистанційної освіти, підтримку бізнесу, а також ефективну комунікацію між органами влади та населенням.

Водночас цифровізація значно посилила роль інформаційної безпеки, захисту персональних даних і стійкості цифрової інфраструктури до кіберзагроз, що набуває особливого значення під час воєнного стану. Такі виклики зумовлюють необхідність розвитку нових наукових підходів до дослідження злочинності, серед яких важливе місце посідає цифрова кримінологія. Іноземні практики свідчать, що в сучасних умовах запобігання та протидії злочинності вона є одним із ключових напрямів трансформації сучасної кримінологічної науки.

Нині в умовах війни цифрова кримінологія формує нову парадигму – від описового аналізу злочинності до її прогнозування та превентивного управління. Проте її ефективність можлива лише за умови дотримання балансу між технологічними можливостями, правовими обмеженнями й етичними стандартами. Європейська модель демонструє важливість прав людини, американська – потужність аналітики, азійські – ефективність цифрового контролю, а міжнародні організації – необхідність глобальної координації.

Отже, цифрова кримінологія поступово формується як самостійний науковий напрям у системі юридичних наук, що відповідає сучасним викликам цифрової епохи та забезпечує наукове підґрунтя для розроблення нових моделей запобігання злочинності, заснованих на використанні цифрових технологій, аналітики даних і прогнозування криміногенних процесів.

Метою статті є дослідження іноземних практик розвитку цифрової кримінології, аналіз сучасних підходів до використання цифрових технологій у кримінологічних дослідженнях та обґрунтування перспектив їх застосування в Україні.

Матеріали та методи

Методологічною основою дослідження стали загальнонаукові та спеціально-юридичні методи пізнання, що забезпечили комплексний аналіз сучасних іноземних практик розвитку цифрової кримінології. Інформаційну базу дослідження становлять наукові публікації українських і зарубіжних учених, міжнародні нормативно-правові акти, офіційні документи правоохоронних органів і міжнародних організацій, а також

матеріали щодо впровадження цифрових технологій у сфері запобігання та протидії злочинності.

У процесі дослідження застосовано порівняльно-правовий метод, який дав змогу зіставити підходи до розвитку цифрової кримінології у США, Великій Британії, країнах Європейського Союзу, а також Сінгапурі та Китаї. Системно-структурний метод використано для визначення місця цифрової кримінології у структурі сучасної кримінологічної науки та встановлення взаємозв'язку між цифровими технологіями, кримінологічним аналізом і практикою правоохоронної діяльності.

Методи аналізу та синтезу дали можливість узагальнити сучасні тенденції застосування штучного інтелекту, технологій великих даних (Big Data), машинного навчання, цифрової кримінальної аналітики, геоінформаційних систем (GIS), прогнозової поліцейської діяльності (Predictive Policing), цифрової криміналістики та мережевого аналізу соціальних зв'язків у процесі дослідження злочинності. Формально-логічний метод застосовано для уточнення понятійно-категоріального апарату цифрової кримінології, а метод узагальнення – для формулювання висновків щодо можливостей адаптації позитивного зарубіжного досвіду до системи кримінологічної науки та правоохоронної діяльності України.

Комплексне використання зазначених методів забезпечило всебічне дослідження сучасних іноземних моделей розвитку цифрової кримінології та визначення перспектив їх практичного впровадження в умовах цифрової трансформації суспільства.

Результати й обговорення

Результати дослідження свідчать, що цифрова кримінологія в провідних зарубіжних державах сформувалася як міждисциплінарний напрям, який інтегрує кримінологію, інформаційні технології, аналіз даних, штучний інтелект і цифрову криміналістику. Аналіз іноземних практик підтверджує, що найбільшого розвитку цей напрям набув у США, Великій Британії, країнах Європейського Союзу, а також у Сінгапурі та Китаї, де цифрові технології активно застосовують як для аналізу криміногенної ситуації, так і для прогнозування злочинності та прийняття управлінських рішень.

Встановлено, що одним із ключових напрямів розвитку цифрової кримінології є використання технологій Big Data й алгоритмів машинного навчання для виявлення закономірностей злочинної поведінки. Значне поширення отримали системи прогнозової аналітики (Predictive Policing), які забезпечують моделювання кримінальних ризиків, аналіз просторово-часових закономірностей злочинності й оптимізацію розподілу ресурсів правоохоронних органів.

Водночас у науковій літературі увагу зосереджено на необхідності забезпечення

прозорості алгоритмів, недопущення дискримінації та дотримання фундаментальних прав людини під час використання автоматизованих систем прийняття рішень. Досліджуючи російсько-українську війну у XXI столітті, слід зауважити, що тепер ми живемо в іншому вимірі – іноді без світла, з прильотами ракет і снарядів, але є надія, що переможемо ворога і в наш рідний дім, у нашу оселю прийде мир (Bohatyrov, 2023, p. 7).

Водночас у сучасній кримінології воєнний стан є не лише фактором фізичних руйнувань, а й потужним криміногенним чинником, що трансформує структуру злочинності, призводить до нових кримінальних ризиків і посилює вразливість населення. Саме тому досвід держав, які пережили збройні конфлікти, свідчить про необхідність поєднання традиційних заходів правоохоронної діяльності з комплексними програмами соціальної стійкості, підтримки громад, відновлення довіри до державних інституцій та розвитку механізмів раннього запобігання злочинності.

Іноземні кримінологічні практики, апробовані в країнах, що пройшли через військові конфлікти або терористичні загрози, демонструють ефективність інтегрованого підходу до превенції, який охоплює міжвідомчу взаємодію, залучення місцевих громад, підтримку психічного здоров'я населення, роботу з ветеранами та внутрішньо переміщеними особами, а також використання ризик-орієнтованих моделей прогнозування злочинності.

Для України адаптація таких підходів має не лише практичне, а й стратегічне значення, оскільки запобігання злочинності в умовах війни та повоєнного відновлення стає невід'ємною складовою забезпечення національної безпеки, верховенства права та сталого розвитку держави. У цьому контексті аналіз міжнародного досвіду розвитку кримінології надає можливість виявити сучасні тенденції дослідження злочинності, оцінити ефективність різних моделей її запобігання та визначити можливості їх адаптації до українських реалій.

Зокрема, українська вчена Г. В. Дідківська зазначає, що щорічні темпи зростання або зменшення злочинності у високорозвинутих зарубіжних державах зазвичай не перевищують 2–4 %. Західні кримінологи оцінюють цей показник позитивно, адже незначні коливання рівня злочинності дають змогу планомірно реалізувати довгострокові й поточні профілактичні програми без застосування надзвичайних заходів (Didkivska, 2019, p. 319).

Оскільки міжнародна практика доводить, що цифрова кримінологія вже перестала бути суто теоретичним напрямом і активно впроваджується в роботу правоохоронних органів багатьох держав, її розвиток в Україні є необхідною умовою підвищення ефективності запобігання та

протидії злочинності в умовах цифрової трансформації.

Українські вчені серед універсальних міжнародно-правових документів вирізняють Конвенцію про кіберзлочинність (Будапештська конвенція), прийняту Радою Європи у 2001 році та ратифіковану Законом України від 7 вересня 2005 року № 2824-IV¹. У цій Конвенції закріплено класифікацію комп'ютерних злочинів і рекомендації органам влади держав щодо боротьби з цими злочинами.

З метою запобігання та протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів країн світу такі злочини класифікують за кодифікатором міжнародної кримінальної поліції Генерального секретаріату Інтерполу, який 1991 року інтегровано в автоматизовану систему пошуку. Нині він доступний підрозділам Національних центральних бюро Інтерполу більшості країн світу, зокрема й НЦБ Інтерполу МВС України (Saienko, Savela, & Topolianskyi, 2021, p. 388).

Отже, цифрова кримінологія трансформувалася у дієвий правовий та практичний інструмент забезпечення публічної безпеки, прогнозування злочинності та управління криміногенними ризиками. Її розвиток доцільно проаналізувати крізь призму трьох основних моделей.

1. США: модель алгоритмічного прогнозування злочинності. Сполучені Штати Америки є одним із піонерів використання цифрових технологій у криміно-логічному аналізі. Розвиток цифрової кримінології тут базується на концепції *data-driven policing* – управління правоохоронною діяльністю на основі даних. Ключовим інструментом стали системи прогнозного поліцейського аналізу (Predictive Policing), які використовують статистичні моделі й алгоритми машинного навчання для визначення ймовірності вчинення злочинів у конкретних географічних зонах.

У США активно застосовують: інтегровані кримінальні бази даних (FBI Crime Data Explorer), системи відеоаналітики та розпізнавання об'єктів, аналітику соціальних мереж, технології OSINT (Open Source Intelligence). Водночас американська модель виявила суттєву проблему – алгоритмічну упередженість (algorithmic bias). У США практична реалізація алгоритмічного прогнозування злочинності ґрунтується на збиранні й аналізі великого обсягу даних про попередні злочини (час, місце та специфіка правопорушень), а також інформації про виклики поліції. Наприклад, такі дані активно використовували поліцейські департаменти великих міст, зокрема Los Angeles Police Department і Chicago Police Department.

¹ Конвенція про кіберзлочинність (Будапештська конвенція) : міжнар. док. від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

За дослідженнями вчених, використання аналітичних даних може підвищувати ефективність роботи поліції та оптимізувати розподіл ресурсів. Модель здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing) використовує дані про час, місця та характер минулих інцидентів, щоб забезпечити розуміння поліцейським керівникам того, де і в який час патрулі поліції мають патрулювати або підтримувати свою присутність, щоб найкраще використовувати ресурси або мати найбільші шанси стримувати або запобігати майбутнім кримінальним виявам¹.

Модель правоохоронної діяльності на основі прогнозів (Predictive Policing) – це проактивна поліцейська діяльність, яка використовує алгоритми прогнозування, засновані на поєднанні різних типів даних, щоб передбачити, де і коли може статися злочин, і визначити закономірності серед минулих кримінальних інцидентів. Прогнозна поліція зазвичай зосереджується на геопросторовому прогнозуванні (Fedchak, 2023, p. 144).

Зокрема, уряд США схвалив проект компанії SpaceX зі створення глобальної супутникової мережі Starlink, яку часто називають «всесвітнім Wi-Fi» Ілона Маска. Федеральна комісія зі зв'язку США (FCC) дозволила реалізацію проекту, що передбачає запуск близько 12 тисяч супутників для забезпечення широкосмугового доступу до Інтернету практично з будь-якої точки планети. Згідно з планами, половину супутників мали вивести на орбіту до весни 2024 року².

2. Велика Британія: evidence-based підхід і кримінологічна аналітика. У Великій Британії цифрова кримінологія розвивається в межах концепції Evidence-Based Policing, яка передбачає прийняття управлінських рішень на основі емпіричних даних і науково перевірених моделей. Тут поліція активно використовує: геоінформаційні системи (GIS) для картографування злочинності, аналітичні платформи для оцінювання ризиків, моделі гарячих точок злочинності (*hot spots policing*), інтегровані системи кримінальної розвідки.

Отже, у Великій Британії підхід до боротьби зі злочинністю базується на принципі «evidence-based», тобто рішення приймають на основі даних і доказів, а не лише досвіду або інтуїції поліцейських. Для цього збирають багато інформації: де і коли стаються злочини, які це види правопорушень, які соціальні умови в районах. Ці дані аналізують кримінологи й аналітики. Наприклад, якщо в районі часто крадуть велосипеди, можуть виявити, що там погане освітлення або

мало камер. Тоді проблему вирішують не лише патрулями, а й змінами в інфраструктурі. Після всіх заходів обов'язково перевіряють результат: чи зменшилася кількість злочинів і чи працює обрана стратегія. Якщо ні – підхід змінюють. Тому система постійно вдосконалюється на основі реальних даних.

3. Європейський Союз: правова модель цифрової кримінології. У межах Європейського Союзу розвиток цифрової кримінології відбувається під сильним впливом прав людини та принципів захисту персональних даних. Ключову роль відіграють такі інституції, як: Europol; Eurojust і FRA. Варто зазначити, що європейська модель ґрунтується на балансі між технологічною ефективністю та правовими гарантіями.

Встановлено, що в країнах ЄС цифрова кримінологія розвивається через: транскордонні інформаційні системи безпеки (SIS, EUROPOL SIENA); спільні аналітичні платформи; розвиток кіберзлочинності як окремого напрямку кримінології та алгоритмічний аудит правоохоронних технологій. На практиці це означає, що в європейській моделі регулювання штучного інтелекту та цифрових технологій пріоритетом є захист прав і свобод людини. Будь-які системи штучного інтелекту мають відповідати чітким правовим вимогам щодо безпеки, прозорості, недискримінації та захисту персональних даних.

4. Сінгапур: модель тотальної цифрової інтеграції. Сінгапур демонструє одну з найбільш технологічно розвинених моделей цифрової кримінології, що базується на концепції *smart nation policing*. Її характерними рисами є: повна інтеграція систем відеоспостереження, використання штучного інтелекту для аналізу поведінкових патернів, автоматизовані системи виявлення підозрілої активності та цифровий моніторинг громадських просторів у реальному часі.

Перевагою Сінгапурської моделі є висока ефективність у запобіганні злочинності завдяки поєднанню суворого законодавства, сучасних технологій та невідворотності покарання. На практиці це виявляється в масштабному впровадженні систем відеоспостереження, цифрового моніторингу громадських місць, оперативному обміні інформацією між правоохоронними органами та швидкому реагуванні на правопорушення. Саме тому успішність Сінгапурської моделі здебільшого залежить від наявності чітких правових гарантій, прозорості використання технологій та ефективного контролю за діяльністю державних органів, особливо поліції³.

5. Китай: модель масової алгоритмічної безпеки. Китайська модель цифрової кримінології базується на масштабному використанні технологій: системи розпізнавання облич, централі-

¹ Lau Tim. Predictive Policing Explained. Attempts to forecast crime with algorithmic techniques could reinforce existing racial biases in the criminal justice system. URL: <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>

² Уряд США схвалив запуск «всесвітнього wi-fi» Ілона Маска. URL: <https://ua.112.ua/suspilstvo/uriadssha-skhaliv-yv-zapusk-vseshvitnoho-wi-fi-ilonamaska-439811.1ytl>

³ Singapore Police Force. Police Workplan Seminar 2026. URL: <https://www.police.gov.sg/Media-Hub/Police-Life/2026/05/From-Frontlines-to-Frontiers-Police-Workplan-Seminar-2026>

зованих баз біометричних даних, AI-аналітики поведінки громадян, прогнозування ризиків соціальної девіації. Ця модель є найінтенсивнішою з позиції цифрового контролю, але зумовлює значну міжнародну дискусію щодо її відповідності стандартам прав людини.

Водночас вона дає змогу правоохоронним органам здійснювати безперервний моніторинг громадського порядку, оперативно ідентифікувати осіб, які перебувають у розшуку, а також прогнозувати потенційні загрози ще до моменту вчинення правопорушення. Практичне застосування цієї моделі також передбачає використання систем прогнозувального поліцейського аналізу, які оцінюють імовірність виникнення криміногенних ситуацій на основі статистичних, соціальних і поведінкових показників.

Отримані результати використовують для оптимізації патрулювання, розподілу ресурсів правоохоронних органів і посилення контролю в районах із підвищеним рівнем ризику. Настільки масштабне використання цифрових технологій супроводжується критикою з боку міжнародної спільноти через ризики порушення права на приватність, недостатню прозорість алгоритмів і можливість надмірного державного контролю за громадянами (Ху, 2024).

Для України міжнародний досвід є особливо актуальним у контексті: цифрової трансформації державного управління, зростання кіберзлочинності, воєнних загроз та інформаційних операцій, необхідності модернізації кримінологічного забезпечення безпеки. Перспективними напрямками імплементації міжнародного досвіду є: створення національних систем кримінологічної аналітики, впровадження AI-моделей прогнозування злочинності, розвиток кримінологічних GIS-платформ, інтеграція з міжнародними базами даних.

Ці напрями мають особливе значення через цифровізацію державного управління, необхідність протидії кібератакам, гібридним загрозам та інформаційним операціям, а також потребу адаптації системи кримінологічного забезпечення до викликів воєнного часу. Їх реалізація сприятиме підвищенню ефективності правоохоронної діяльності, своєчасному виявленню криміногенних ризиків і зміцненню національної безпеки (Bohatyrov, I., & Bohatyrov, A., 2024, p. 15).

На необхідності модернізації кримінологічного забезпечення безпеки, розвитку цифрових технологій аналізу злочинності та впровадження інструментів прогнозування на основі великих даних і штучного інтелекту акцентують українські вчені. Зокрема, І. А. Нестерова (2026) зазначає, що кримінологія дедалі частіше використовує цифрові інструменти для збирання, аналізу й інтерпретації даних; цифровізація змінює методи наукового аналізу злочинності; зростає роль автоматизованої обробки великих масивів даних і прогнозування злочинності.

Проведений нею аналіз кримінологічних досліджень і практичного досвіду використання цифрових програм у правоохоронній діяльності окремих країн довів, що цифровізація змінює саму методологію кримінологічного аналізу, розширюючи можливості збирання, опрацювання та інтерпретації даних. Водночас виникає потреба модернізації методології кримінологічних досліджень, розвитку кримінального аналізу, посилення міждисциплінарної взаємодії та міжнародного співробітництва у сфері боротьби зі злочинними виявами (Nesterova, 2026, p. 425).

Зазначена позиція повністю відображає реальні тенденції розвитку кримінології в умовах цифровізації: сучасні дослідження дедалі більше спираються на цифрові інструменти для збирання, опрацювання й аналізу великих масивів даних, що істотно підвищує точність і швидкість кримінологічного аналізу, оновлюють теоретико-методологічну базу кримінології, поглиблюють міжнародне співробітництво й інтеграції знань із суміжних сфер, зокрема інформатики, статистики та науки про дані.

С. Ф. Денисов (2021) зауважує, що додатково цифрові інструменти надають можливість швидко відстежувати зміни в поведінкових моделях і соціальних тенденціях, що можуть сигналізувати про нові види злочинів або зміни в структурі кримінальної діяльності (Denysov, 2021, p. 152). На думку В. Л. Давиденка (2017), сучасні технології, такі як штучний інтелект та алгоритми машинного навчання, дають змогу автоматизувати процеси аналізу даних і виявляти складні взаємозв'язки, які раніше були непомітними або надто трудомісткими для обробки вручну (Davydenko, 2017, p. 141).

Також слушно зауважує Д. А. Зінченко (2023), що завдяки аналізу даних із соціальних мереж, відеоспостереження та інших цифрових джерел є можливість досліджувати поведінку в режимі реального часу, що сприяє розробленню превентивних заходів і своєчасному реагуванню на потенційні загрози. Іншим важливим аспектом є використання геоінформаційних систем, за допомогою яких досліджують просторові особливості злочинності, зокрема аналізують «гарячі точки» злочинної активності й ефективність заходів щодо забезпечення безпеки (Zinchenko, 2023, p. 119).

Українська вчена О. Бугера (2018), досліджуючи використання соціальних інтернет-мереж для запобігання злочинності, зазначає, що найактивніше спілкування, взаємне інформування й обговорення найгостріших проблем сучасності в різноманітних життєвих сферах відбувається в соціальних мережах. Вони є невід'ємним елементом спілкування більшості учасників онлайн-комунікації (Buhera, 2018, p. 238).

Одним із найперспективніших напрямів розвитку цифрової кримінології у зарубіжній практиці є застосування технологій штучного

інтелекту (Artificial Intelligence, AI) для аналізу злочинності, прогнозування кримінальних ризиків та удосконалення діяльності правоохоронних органів. У цьому контексті важливе значення має дослідження К. J. Hayward та М. М. Maas (2021) «Artificial intelligence and crime: A primer for criminologists», у якому автори визначають штучний інтелект як чинник, що одночасно змінює природу злочинності й трансформує механізми її запобігання.

Важливим напрямом розвитку цифрової кримінології в зарубіжній науці є інтеграція кримінологічних досліджень із кібербезпекою. На думку Б. Дюпона та Ч. Велана (2021), сучасні кіберзлочини дедалі частіше визначають не лише як кримінальні правопорушення, а і як загрози кібербезпеці, що зумовлює активніше залучення до їх запобігання та протидії не лише правоохоронних органів, а й інституцій національної безпеки. Автори пропонують тлумачити кримінальну злочинність і кібербезпеку як взаємопов'язані елементи єдиного континууму, де відбувається поступове стирання меж між традиційною кримінологією, інформаційною безпекою та діяльністю державних і приватних суб'єктів захисту цифрового простору.

Такий міждисциплінарний підхід сприяє формуванню цифрової кримінології як самостійного напрямку досліджень, що поєднує кримінологічні теорії, аналіз великих масивів цифрових даних, методи штучного інтелекту й практики кібербезпеки для виявлення, прогнозування та запобігання цифровим правопорушенням (Dupont, & Whelan, 2021).

Беззаперечним є той факт, що використання міжнародних цифрових масивів даних для проведення порівняльних кримінологічних досліджень є актуальною та малодослідженою проблемою. Тому поділяємо позицію А. Е. Nivette (2021), яка у своїй статті акцентує, що сучасна кримінологія дедалі більше ґрунтується на відкритих міжнародних базах даних, які забезпечують можливість комплексного аналізу злочинності, віктимізації, функціонування систем кримінальної юстиції та соціальних детермінант злочинності в різних країнах.

Водночас М. Bada, J. R. C. Nurse (2021) дійшли висновку, що, попри стрімке зростання кіберзлочинності, у міжнародній практиці досі бракує єдиного концептуального бачення профілювання кіберправопорушників, а більшість досліджень зосереджено на хакерах і базується на дедуктивному підході до побудови кримінологічного профілю. Водночас автори зосереджують увагу на необхідності інтеграції кримінологічних, психологічних, поведінкових і кібербезпекових підходів, а також активнішого залучення правоохоронних органів і фахівців із кібербезпеки до процесів аналізу цифрової злочинності.

Такий підхід, на думку вчених, демонструє, що сучасна цифрова кримінологія за кордоном

еволюціонує від традиційного опису злочинної поведінки до використання комплексної аналітики даних для прогнозування кримінальної активності, ідентифікації потенційних правопорушників і розроблення ефективних механізмів превенції кіберзлочинності (Bada, & Nurse, 2021).

Причому, як зазначає Т. М. Беркій, соціальними мережами користуються 82 % всіх інтернет-користувачів у світі, що становить близько 1,2 млрд осіб. Високий рівень їх поширення відображає один із головних трендів глобальної мережі: як тільки люди підключаються до Інтернету, вони негайно починають спілкуватися з іншими людьми. Нині відсоток користувачів соціальних мереж у світі коливається від 53 % (у Китаї) до 98% (у США)¹.

Завершуючи дослідження іноземних практик розвитку цифрової кримінології, доцільно зауважити, що він демонструє поступовий перехід від традиційних емпіричних моделей вивчення злочинності до комплексних аналітичних систем, заснованих на використанні цифрових даних, інтелектуальних технологій та міждисциплінарних підходів. Цифрова кримінологія формується не лише як сукупність новітніх інструментів дослідження кримінальних процесів, а і як самостійний напрям наукового пізнання, що інтегрує досягнення кримінології, інформаційних технологій, права, соціальних наук та аналітики даних.

Практика провідних країн світу підтверджує, що цифрова трансформація кримінологічної науки створює нові можливості для глибшого розуміння детермінант злочинності, виявлення закономірностей її розвитку та розроблення ефективніших стратегій запобігання кримінальним виявам. Для України врахування зарубіжних практик розвитку цифрової кримінології є важливим чинником модернізації кримінологічної науки та вдосконалення системи протидії злочинності в умовах цифрової трансформації суспільства.

Висновки

1. Результати дослідження свідчать, що цифрова кримінологія в провідних зарубіжних державах сформувалася як міждисциплінарний напрям, який інтегрує кримінологію, інформаційні технології, аналіз даних, штучний інтелект і цифрову криміналістику. Встановлено, що одним із ключових напрямів розвитку цифрової кримінології є використання технологій Big Data й алгоритмів машинного навчання для виявлення закономірностей злочинної поведінки. Значного поширення набули системи прогнозової аналітики (Predictive Policing), які забезпечують моделювання кримінальних ризиків, аналіз просторово-

¹ Беркій Т. М. Соціальні мережі: різні аспекти впливу на людину. URL: http://ukrainepravo.com/legal_publications/essay-on-it-law/it_1aw_berkiy_Socialnetworks_and_there_involves/

часових закономірностей злочинності й оптимізацію розподілу ресурсів правоохоронних органів.

2. Доведено, що перспективним напрямом для України є формування національної моделі цифрової кримінології, яка поєднуватиме міжнародні стандарти, національні наукові традиції та специфіку сучасних безпекових викликів. А також розвиток систем кримінального прогнозування на основі штучного інтелекту, упровадження сучасних методів аналізу великих даних, розширення міжнародної співпраці та підготовка фахівців нового покоління, здатних ефективно працювати

в умовах цифрової трансформації правоохоронної діяльності.

Подяки

Немає.

Фінансування

Дослідження не фінансувалося.

Конфлікт інтересів

Немає.

References

- [1] Bada, M., & Nurse, J.R.C. (2021). Profiling the Cybercriminal: A Systematic Review of Research. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (pp. 1-8). DOI: 10.1109/CyberSA52016.2021.9478246
- [2] Bohatyrov, I.H. (2023). *The Russian-Ukrainian War: A Criminologist's Perspective*. Kyiv: ADEF-Ukraine Publishing House.
- [3] Bohatyrov, I.H., & Bohatyrov, A.I. (2024). Organized Crime under Martial Law: Problems and Ways of Overcoming Them in Ukraine. *Law and Border*, 1(3), 5-26. DOI: 10.32453/law_border.v3i1.1637
- [4] Buhera, O. (2018). The Use of Social Internet Networks for Crime Prevention. *Entrepreneurship, Economy and Law*, 5, 238-241. Retrieved from <https://pgp-journal.kiev.ua/archive/2018/5/47.pdf>
- [5] Davydenko, V.L. (2017). Goals and Objectives of Victimological Impact on Crime. *Current Issues of Domestic Jurisprudence*, 1, 141-143. Retrieved from <http://dspace.univd.edu.ua/handle/123456789/10918>
- [6] Denysov, S.F. (2021). Some Aspects of the Essence and Subject Matter of Criminology as a Science. *Bulletin of the Criminological Association of Ukraine*, 1(24), 151-159. Retrieved from <http://dspace.univd.edu.ua/handle/123456789/10410>
- [7] Didkivska, H.V. (2019). *Criminological Characteristics of Ukraine's Participation in the System of International Crime Prevention*. Vinnytsia: Tvory.
- [8] Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, 54(1). DOI: 10.1177/00048658211003925
- [9] Fedchak, I.A. (2023). History, Essence and Concept of the Predictive Policing Model. *Scientific Bulletin of Lviv State University of Internal Affairs*, 3, 141-147. DOI: 10.32782/2311-8040/2023-3-18
- [10] Hayward, K.J., & Maas, M.M. (2021). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture*, 17(2), 209-233. DOI: 10.1177/1741659020917434
- [11] Nesterova, I.A. (2026). Implementation of Digital Technologies in Criminological Research. *Analytical and Comparative Jurisprudence*, 1(2), 421-425. DOI: 10.24144/2788-6018.2026.01.2.67
- [12] Nivette, A.E. (2021). Exploring the Availability and Potential of International Data for Criminological Study. *International Criminology*, 1, 70-77. DOI: 10.1007/s43576-021-00009-y
- [13] Saienko, M.I., Savela, Ye.A., & Topolianskyi, Yu.Yu. (2021). International Experience in Combating Cybercrime and Cyber Fraud. *Scientific Bulletin of Uzhhorod National University. Series "Law"*, 64, 386-391. DOI: 10.24144/2307-3322.2021.64.71
- [14] Xu, J. (2024). Opening the "Black Box" of Algorithms: Regulation of Algorithms in China. *Communication Research and Practice*, 10(3), 288-296. DOI: 10.1080/22041451.2024.2346415
- [15] Zinchenko, D.A. (2023). Analysis of Risks and Protection Strategies Against Cyberattacks in the Modern Digital World. *Counteracting Cybercrime and Human Trafficking: International Scientific and Practical Conference* (pp. 118-121). Vinnytsia: Kharkiv National University of Internal Affairs. Retrieved from <https://dspace.univd.edu.ua/handle/123456789/17463>

Список використаних джерел

- [1] Bada M., Nurse J. R. C. Profiling the Cybercriminal: A Systematic Review of Research. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (14–18 June 2021). P. 1–8. DOI: 10.1109/CyberSA52016.2021.9478246
- [2] Богатирьов І. Г. Російсько-українська війна: погляд кримінолога : монографія. Київ : АДЕФ-Україна, 2023. 244 с.
- [3] Богатирьов І. Г., Богатирьов А. І. Організована злочинність в умовах воєнного стану: проблеми та шляхи їх подолання в Україні. *Закон і кордон*. 2024. № 1. Т. 3. С. 5–26. DOI: 10.32453/law_border.v3i1.1637

- [4] Бугера О. Використання соціальних Інтернет-мереж для запобігання злочинності. *Підприємництво, господарство і право*. 2018. № 5. С. 238–241. URL: <https://pgp-journal.kiev.ua/archive/2018/5/47.pdf>
- [5] Давиденко В. Л. Цілі та завдання віктимологічного впливу на злочинність. *Актуальні проблеми вітчизняної юриспруденції*. 2017. № 1. С. 141–143. URL: <http://dspace.univd.edu.ua/handle/123456789/10918>
- [6] Денисов С. Ф. Деякі аспекти сутності та предмета кримінології як науки. *Вісник Кримінологічної асоціації України*. 2021. № 1 (24). С. 151–159. URL: <http://dspace.univd.edu.ua/handle/123456789/10410>
- [7] Дідківська Г. В. Кримінологічна характеристика участі України в системі запобігання міжнародної злочинності : монографія. Вінниця : Твори, 2019. 356 с.
- [8] Dupont B., Whelan C. Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*. 2021. Vol. 54. Issue 1. DOI: 10.1177/00048658211003925
- [9] Федчак І. А. Історія, сутність та поняття моделі здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing). *Науковий Вісник Львівського державного університету внутрішніх справ*. 2023. № 3. С. 141–147. DOI: 10.32782/2311-8040/2023-3-18
- [10] Hayward K. J., Maas M. M. Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture*. 2021. Vol. 17 (2). P. 209–233. DOI: 10.1177/1741659020917434
- [11] Нестерова І. А. Впровадження цифрових технологій в кримінологічні дослідження. *Аналітично-порівняльне правознавство*. 2026. Вип. 01. Ч. 2. С. 421–425. DOI: 10.24144/2788-6018.2026.01.2.67
- [12] Nivette A. E. Exploring the Availability and Potential of International Data for Criminological Study. *International Criminology*. 2021. Vol. 1. P. 70–77. DOI: 10.1007/s43576-021-00009-y
- [13] Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайства. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2021. Вип. 64. С. 386–391. DOI: 10.24144/2307-3322.2021.64.71
- [14] Xu J. Opening the 'black box' of algorithms: regulation of algorithms in China. *Communication Research and Practice*. 2024. No. 10 (3). P. 288–296. DOI: 10.1080/22041451.2024.2346415
- [15] Зінченко Д. А. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф. (Вінниця, 31 трав. 2023 р.). Вінниця : ХНУВС, 2023. С. 118–121. URL: <https://dspace.univd.edu.ua/handle/123456789/17463>

BOHATYROV Ivan

Doctor of Law, Professor, Professor of the Department of Criminal Enforcement and Criminal Law of the Penitentiary Academy of Ukraine

14000, 34 Honcha St., Chernihiv, Ukraine

ORCID: <https://orcid.org/0000-0003-4001-7256>

Foreign Practices in the Development of Digital Criminology: an Innovative Direction

Abstract. The article is devoted to a comprehensive study of contemporary foreign practices in the development of digital criminology as an innovative field of criminological science emerging under the influence of the global digitalization of social relations and the rapid advancement of information and communication technologies. The relevance of the study is обусловлено the need to reconsider traditional criminological approaches to the study of crime within the digital environment, taking into account the growing prevalence of cybercrime, the use of artificial intelligence, Big Data technologies, machine learning algorithms, and digital criminological analytics. The findings demonstrate that, in leading foreign countries, digital criminology is developing as an interdisciplinary field that integrates criminological knowledge with advances in digital technologies, data science, and artificial intelligence. The article analyzes the application of crime prediction algorithms, criminological analytics, digital criminal intelligence, geographic information systems (GIS), open-source intelligence (OSINT) tools, and other advanced technological solutions in the activities of law enforcement agencies in the United States, the United Kingdom, the Member States of the European Union, as well as Singapore and China. The principal advantages of the digital transformation of criminological practice are identified, while the legal, ethical, and organizational risks associated with the use of algorithmic decision-making models, the processing of personal data, and the protection of digital human rights are also examined. The article concludes that the implementation of international practices in digital criminology will contribute to enhancing the effectiveness of criminological forecasting, improving crime prevention mechanisms, advancing evidence-based criminological policy, and modernizing the activities of law enforcement agencies in the context of the state's digital transformation.

Keywords: foreign practices; digital criminology; cybercrime; artificial intelligence; Big Data; forecasting; foreign experience; law enforcement activities.