

УДК 343.9

DOI <https://doi.org/10.24144/2788-6018.2026.01.2.67>

## ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В КРИМІНОЛОГІЧНІ ДОСЛІДЖЕННЯ

**Нестерова І.А.,**

*кандидат юридичних наук, доцент,  
доцент кафедри кримінально-правової політики  
Ужгородського національного університету  
ORCID: 0000-0003-0481-2965  
e-mail: iryna.nesterova@uzhnu.edu.ua*

### **Нестерова І.А. Впровадження цифрових технологій в кримінологічні дослідження.**

Вказується, у сучасних реаліях цифровізації неминуче поступово змінюються всі сфери нашого життя, не обминув цей процес й науково – практичну діяльність.

Визначається, що кримінологічна наука, досліджуючи тенденції та причини злочинності, особистість правопорушника та способи запобігання кримінальним правопорушенням, все частіше використовує цифрові інструменти для збору, аналізу та інтерпретації даних. Сучасні цифрові технології відкривають великі можливості як для дослідників та правоохоронців, так і для правопорушників. Проблема впровадження сучасних цифрових технологій у кримінологічні дослідження виступає об'єктивною необхідністю є дуже актуальною.

Доведено, що використання програм цифрового інтелекту сьогодні для класифікації даних, виявлення закономірностей і прогнозування правопорушень є реалією.

Визначається, що поява новітніх програм прогнозування в системі кримінологічних досліджень є важливим і вже невід'ємним компонентом у масштабній системі профілактики та протидії злочинності.

Автор погоджується з думкою дослідників проблеми, які відзначають, що використання аналітичних даних може підвищувати ефективність роботи поліції та оптимізувати розподіл ресурсів. У кримінологічних дослідженнях вони дозволяють знаходити закономірності, які недоступні традиційними методами аналізу (Big Data).

Автор звертає увагу на те, що аналіз кримінологічних досліджень та практичного досвіду використання цифрових програм в правоохоронній діяльності окремих країн дає нам підстави стверджувати, що цифровізація змінює саму методологію кримінологічного аналізу, розширюючи можливості збору, обробки та інтерпретації даних.

В той же час, активне та свідоме використання новітніх технологій самими правопорушниками створює додаткові виклики для науки кримінології та правоохоронної практики, що робить недостатніми традиційні кримінологічні підходи. Виникає потреба модернізації методології кримінологічних досліджень, розвитку кримінального аналізу, посилення міждисциплінарної взаємодії та міжнародного співробітництва у сфері боротьби зі злочинними проявами.

**Ключеві слова:** кримінологічні дослідження, цифровізація, цифровий інтелект, злочинні прояви, кримінологічний аналіз, прогнозування, запобігання, профілактика

### **Nesterova I.A. Implementation of digital technologies in criminological research.**

It is indicated that in the modern realities of digitalization, all spheres of our lives are inevitably gradually changing, and this process has not bypassed scientific and practical activities.

It is determined that criminological science, which studies trends and causes of crime, the personality of the offender, and methods of crime prevention, increasingly relies on digital tools for the collection, analysis, and interpretation of data. Modern digital technologies open up broad opportunities for both researchers and law enforcement agencies, as well as for offenders. Therefore, the issue of implementing digital technologies in criminological research is highly relevant and represents an objective necessity.

It has been proven that the use of artificial intelligence software for data classification, pattern detection, and crime prediction is already a reality. The emergence of modern predictive systems in criminological research is regarded as an important and inseparable component of the comprehensive framework for crime prevention and control.

The author supports the opinions of scholars who note that the use of analytical data can increase police effectiveness and optimise resource allocation. Within criminological research, Big Data technologies make it possible to identify regularities that cannot be revealed through traditional analytical approaches.

Attention is drawn to the fact that the analysis of criminological studies and practical experience of applying digital technologies in the law enforcement systems of various countries demonstrates that digitalisation is transforming the methodology of criminological analysis itself, expanding the possibilities for data collection, processing, and interpretation.

At the same time, the active and deliberate use of digital technologies by offenders creates additional challenges for criminology and law enforcement practice, rendering traditional criminological approaches insufficient. This gives rise to the need to modernise the methodology of criminological research, to develop criminal analysis, and to strengthen interdisciplinary cooperation and international collaboration in combating criminal activity.

**Key words:** criminological research, digitalisation, artificial intelligence, criminal activity, criminological analysis, forecasting, prevention, crime control.

**Постановка проблеми.** У сучасних реаліях цифровізації неминуче поступово змінюються всі сфери нашого життя, не обминув цей процес й науково – практичну діяльність. Наука кримінологія, яка швидко розвивається та в дослідженнях якої цифрові технології відіграють важливу та навіть визначальну роль (в окремих випадках), не є винятком. Кримінологічна наука, досліджуючи тенденції та причини злочинності, особистість правопорушника та способи запобігання кримінальним правопорушенням, все частіше використовує цифрові інструменти для збору, аналізу та інтерпретації даних. Сучасні цифрові технології відкривають великі можливості як для дослідників та правоохоронців, так і для правопорушників. Проблематика впровадження сучасних цифрових технологій у кримінологічні дослідження виступає об'єктивною необхідністю є дуже актуальною.

**Аналіз останніх досліджень і публікацій.** Проблематика впровадження інноваційних технологій у кримінологічні дослідження посідає важливе місце в сучасній науці.

Проблемі визначення та важливості кримінологічних досліджень присвячені праці відомих вітчизняних науковців, таких як: О.М. Бандурка, І.Г. Богатирьов, В.В. Голіна, Л.М. Давиденко, І.М. Даньшин, О.М. Джужа, А.П. Закалюк, А.Ф. Зелінський, О.Г. Колб, О.М. Костенко, О.М. Литвак, О.М. Литвинов та ін. Втім, сучасні реалії вимагають вивчення окремих дискусійних аспектів та потребують подальшого наукового аналізу.

З огляду на це **метою даної статті** є дослідження практичних аспектів та можливостей використання цифрових технологій у кримінологічних дослідженнях.

**Виклад матеріалу дослідження та його основні результати.** До завдань кримінології на сучасному етапі розвитку слід віднести: імплементацію міжнародних стандартів боротьби зі злочинністю, інноваційних методів її дослідження, нових кримінологічних знань [1, с. 61, 67–68].

Це стосується сучасних можливостей для детального збору, аналізу інформації щодо стану, коефіцієнту, динаміки та інших показників злочинності; кримінологічного аналізу особистості правопорушника; кримінологічного прогнозування та розробки превентивних заходів запобігання правопорушенням; створення за допомогою новітніх цифрових технологій програм щодо розслідування різних категорій кримінальних правопорушень, особливо кіберзлочинів.

Сучасні технології, такі як штучний інтелект та алгоритми машинного навчання, дають можливість автоматизувати процеси аналізу даних та знаходити складні взаємозв'язки, які раніше були непомітними або надто трудомісткими для обробки вручну [2, с. 141]. Додатково цифрові інструменти дозволяють швидко відслідковувати зміни у поведінкових моделях та соціальних тенденціях, що можуть сигналізувати про нові види злочинів або зміни у структурі кримінальної діяльності [3, с. 152]. Аналіз даних із соціальних мереж, відеоспостереження та інших цифрових джерел створює можливість досліджувати поведінку в режимі реального часу, що сприяє розробці превентивних заходів та своєчасному реагуванню на потенційні загрози. Іншим важливим аспектом є використання геоінформаційних систем, що дає змогу досліджувати просторові особливості злочинності, зокрема аналізувати гарячі точки злочинної активності та ефективність заходів щодо забезпечення безпеки [4, с. 119].

Системи прогнозування, які базуються на історичних даних і поточних тенденціях, можуть бути корисними для правоохоронних органів у плануванні ресурсів та профілактиці кримінальних правопорушень. Ці технології надають кримінологам можливість працювати з більш масштабними і різноманітними джерелами інформації, відкриваючи нові горизонти для наукових досліджень та практичної діяльності.

Яскравим прикладом цифрової трансформації кримінології є predictive policing як модель прогнозування злочинності на основі аналізу історичних даних. У США та деяких європейських країнах такі системи використовуються для визначення зон підвищеного ризику та планування патрулювання.

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 повинні

патрулювати або підтримувати свою присутність, щоб найкраще використовувати ресурси або мати найбільші шанси стримувати або запобігати майбутнім кримінальним проявам [5]. 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 [6, с. 144].

Поява новітніх програм прогнозування в системі кримінологічних досліджень є важливим і вже невід'ємним компонентом у масштабній системі профілактики та протидії злочинності. Так, наприклад, використання великих даних (Big Data) та аналітики значно підвищує ефективність прогнозування кримінальної активності, дозволяючи виявляти закономірності в злочинних даних та покращувати планування превентивних заходів [7].

У кримінологічних дослідженнях вони дозволяють знаходити закономірності, які недоступні традиційними методами аналізу. Великий обсяг – лише одна з особливостей феномену Big Data, у якому, з одного боку, знайшли втілення комп'ютерно-інформаційні тренди останніх десятиріч; з іншого – він сам здатен впливати й реально трансформує існуючі уявлення та напрацьовані впродовж тривалого часу практики й моделі поведінки як окремих індивідів, так і складних організаційних структур [8, с. 1]. В кримінологічних дослідженнях Big Data використовується, в першу чергу, для моделювання різних форм прогнозування; виявлення та аналізу злочинної активності та ризиків; виявлення проявів латентної злочинності та ін. За допомогою Big Data правоохоронні органи мають можливість робити перерозподіл своїх ресурсів більш ефективно, концентруючи увагу на ділянках з більш високим рівнем злочинності [9, с. 165].

Використання програм цифрового інтелекту сьогодні для класифікації даних, виявлення закономірностей і прогнозування правопорушень є реалією.

Основною складовою сучасних кримінологічних досліджень є цифрова криміналістика, оскільки значна частина кримінальних правопорушень має цифровий компонент. Цей напрям включає збір, збереження та аналіз цифрових слідів – інформації з комп'ютерів, смартфонів, серверів, хмарних сервісів. Міжнародні організації, зокрема UNODC, розробляють стандарти цифрової криміналістики для боротьби з кіберзлочинністю. UNODC у рамках освітнього модуля з кіберзлочинності зазначає, що одним із ключових напрямів є розробка та популяризація стандартів і передових практик у сфері цифрової криміналістики та обробки цифрових доказів для ефективного розслідування кіберзлочинів [10].

Важливою подією у сфері протидії кіберзлочинності стало відкриття для підписання першої у світі міжнародної Конвенції про запобігання, припинення та боротьбу з кіберзлочинністю [11], яка відбулась у жовтні 2025 року у В'єтнамі. На момент відкриття документ підписали 72 держави, що свідчить про високий рівень міжнародної підтримки інституціоналізації співробітництва у сфері протидії злочинності у кіберпросторі.

Конвенція має на меті формування єдиного міжнародно-правового підґрунтя для протидії кіберзлочинності, включаючи уніфікацію підходів до криміналізації відповідних діянь, удосконалення механізмів міжнародної правової допомоги та забезпечення ефективного обміну інформацією між компетентними органами держав. Запровадження таких універсальних стандартів є надзвичайно актуальним у контексті глобалізації цифрових технологій, зростання кількості та складності кіберзлочинів, а також транскордонного характеру їх вчинення. Водночас Конвенція набуде чинності лише після її ратифікації державами-учасниками відповідно до їх внутрішніх правових процедур. Це означає, що остаточне формування міжнародно-правового режиму протидії кіберзлочинності вимагатиме часу та узгоджених політико-правових рішень на національному рівні. Очікується, що реалізація положень Конвенції сприятиме підвищенню ефективності боротьби з кіберзлочинністю, посиленню захисту прав людини у цифровому середовищі та зміцненню міжнародної безпеки загалом.

Для кращого та більш детального аналізу поведінки правопорушника в умовах сучасної цифровізації набуває обертів дослідження цифрових слідів.

Цифрові сліди відіграють ключову роль у сучасних кримінологічних дослідженнях та судовій експертизі, оскільки саме вони часто стають суттєвими доказами у кримінальному провадженні. У наукових публікаціях цифрові сліди визначаються як інформаційні залишки, що виникають внаслідок взаємодії особи чи об'єкта з цифровими пристроями та системами та мають потенційну доказову цінність у встановленні обставин злочину. Такі сліди формуються під час використання комп'ютерних систем, мереж, мобільних пристроїв, хмарних сервісів або іншої цифрової інфраструктури і можуть містити відомості про дії суб'єкта, часові параметри активності, метадані тощо [12, с. 229]. У кримінологічних та криміналістичних дослідженнях така інформація може бути важливою доказовою інформацією в процесуальних діях (ухвалення конкретних тактичних дій) та моделювання поведінки особи правопорушника.

Окремо необхідно приділити увагу створення в правоохоронних органах відділів кримінального аналізу. Використання технологій відеоаналізу та розпізнавання облич стало важливим інструмен-

том у боротьбі зі злочинністю. Ці інновації дозволяють зменшити людський фактор у кримінальному аналізі, прискорити розкриття злочинів і підвищити точність ідентифікації підозрюваних. Постійно вдосконалюються способи ефективного застосування відеоспостереження для забезпечення публічної безпеки [13, с. 91]. За допомогою спеціальної програми аналізуються зображення відеоспостереження, що дає змогу швидко зіставляти кадри з відеоспостереження з базами даних облич осіб, які проходили у справах про кримінальні правопорушення. Це зменшує ймовірність помилкової ідентифікації та сприяє ефективній та оперативній роботі спеціальних підрозділів. Постійно вдосконалюються способи ефективного застосування відеоспостереження для забезпечення публічної безпеки, у тому числі за рахунок інтеграції відеоаналітичних модулів із іншими цифровими системами кримінального аналізу. Наприклад, поєднання розпізнавання облич зі відстеженням поведінкових патернів дозволяє не лише встановити особу, а й прогнозувати потенційні ризики правопорушень. Це особливо важливо в умовах розширення мережі відеоспостереження в містах, де традиційні методи перевірки інформації стають дедалі менш ефективними. Незважаючи на переваги, використання технологій відеоаналізу та розпізнавання облич супроводжується низкою правових і етичних викликів. Однією з найчастіше обговорюваних проблем є питання захисту персональних даних та прав людини під час масового збору відеоданих, оскільки без ретельно опрацьованих стандартів і процедур існує ризик порушення приватності громадян. Аналіз застосування цих технологій у міжнародній практиці показує, що навіть високо розвинені країни стикаються з проблемами забезпечення прозорості їх використання та запобігання упередженню алгоритмів щодо певних груп населення [14].

Звичайно, використання програм кримінального аналізу та розпізнавання облич залежить також від відповідної підготовки кваліфікованих кадрів та чіткого правового забезпечення.

Забезпечення належного рівня кваліфікації співробітників, адаптація процедур обробки цифрових доказів до вимог кримінального процесу та інтеграція цифрових технологій у повсякденну діяльність правоохоронних підрозділів — важливі складові успішної реалізації кримінального аналізу в умовах цифровізації суспільства [15, с. 145]

Паралельно з тим модернізуються і збільшується кількість цифрових засобів, які використовують самі правопорушники, це: анонімізаційні сервіси, криптовалюти, зашифрований трафік, deepfake-технології, технічні пристрої для перехоплення інформації, складні пакети шкідливого ПЗ, інструменти для проведення DDoS-атак, спеціалізовані сервіси у DarkNet для придбання експлоїтів, а також технології приховування цифрових слідів, які істотно ускладнюють їх ідентифікацію в ході кримінального провадження [16]. Тому традиційні, класичні кримінологічні способи вже є недостатніми; виникає гостра необхідність модернізації і самих кримінологічних досліджень.

За даними організації Інтерпол, цифровізація злочинності та кіберзагрози залишаються ключовими аспектами сучасної глобальної кримінальної діяльності, що потребує активного міжнародного співробітництва та обміну цифровими доказами у розслідуваннях [17]. Інтерпол активно працює в цієї сфері, вдосконалюючи методи протидії кіберзлочинності. Так, наприклад, Інтерпол відкрив у Сінгапурі центр інновацій з пошуку правопорушників в Інтернеті та захисту інформаційного простору, в якому працює понад 100 експертів з більш ніж 50 країн. З метою ефективною боротьби з кібератаками, проривом є залучення представників недержавних установ, які працюють в сфері інформаційних технологій.

**Висновки.** Таким чином, в сучасних умовах інформатизації та модернізації всіх сфер суспільного життя, впровадження сучасних цифрових технологій у кримінологічні дослідження виступає об'єктивною необхідністю. Застосування штучного інтелекту, аналітики великих даних, дослідження цифрових слідів, відеоаналізу та систем розпізнавання образів істотно розширює аналітичні можливості кримінологічних досліджень, підвищує ефективність прогнозування злочинності й розробки ефективних методів протидії злочинним проявам. Аналіз кримінологічних досліджень та практичного досвіду використання цифрових програм в правоохоронній діяльності окремих країн дає нам підстави стверджувати, що цифровізація змінює саму методологію кримінологічного аналізу, розширюючи можливості збору, обробки та інтерпретації даних.

В той же час, активне та свідоме використання новітніх технологій самими правопорушниками створює додаткові виклики для науки кримінології та правоохоронної практики, що робить недостатніми традиційні кримінологічні підходи. Виникає потреба модернізації методології кримінологічних досліджень, розвитку кримінального аналізу, посилення міждисциплінарної взаємодії та міжнародного співробітництва у сфері боротьби зі злочинними проявами.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Головкін Б.М. *Поняття, предмет, система кримінології та її завдання на сучасному етапі розвитку. Питання боротьби зі злочинністю.* 2014. Вип. 28. С. 59-68. URL: [https://dspace.nlu.edu.ua/bitstream/123456789/7715/1/Golovkin\\_59-68.pdf](https://dspace.nlu.edu.ua/bitstream/123456789/7715/1/Golovkin_59-68.pdf).

2. Давиденко В.Л. Цілі та завдання віктимологічного впливу на злочинність. *Актуальні проблеми вітчизняної юриспруденції*. 2017. № 1. Т. С. 141–143. URL: <https://dspace.univd.edu.ua/items/cae78617-62eb-43a0-89da-a8831849146e>.
3. Денисов С.Ф. Деякі аспекти сутності та предмета кримінології як науки. *Вісник Кримінологічної асоціації України*. 2021. № 1 (24). С. 151–159. URL: <https://dspace.univd.edu.ua/items/8d7669ce-66e2-4594-bb5c-3c1383a3ad55>.
4. 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. (м. Вінниця, 31 травня 2023). Вінниця: ХНУВС, 2023. С. 118–121. URL: <https://dspace.univd.edu.ua/handle/123456789/17463>.
5. 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>.
6. Федчак І.А. Історія, сутність та поняття моделі здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing). *Науковий Вісник Львівського державного університету внутрішніх справ*. № 3. 2023. С. 141–147. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/5944/1/18.pdf>.
7. Kounadi, O., Ristea, A., Araujo, A. et al. A systematic review on spatial crime forecasting. *Crime Sci* 9. 7, 2020. URL: <https://doi.org/10.1186/s40163-020-00116-7>.
8. Задорожна І.М. Великі дані як об'єкт управління. *Економіка та менеджмент*. 2016. № 1–2. С. 75–79. URL: [https://econommeneg.btsau.edu.ua/sites/default/files/visnyky/economika/zadorozhna\\_1-2\\_2016.pdf](https://econommeneg.btsau.edu.ua/sites/default/files/visnyky/economika/zadorozhna_1-2_2016.pdf).
9. Нестерова І.А. Сучасні технології в кримінологічних дослідженнях: the 16th International scientific and practical conference "Trends in the development of science through the creation of new technologies" (December 16-19, 2025) Seville, Spain. International Science Group. 2025. С. 164–167.
10. Standards and best practices for digital forensics – UNODC Cybercrime Module 4: Key Issues. URL: <https://www.unodc.org/cld/es/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.htm>.
11. The United Nations Convention against Cybercrime opens for signature in Hanoi. Office of Legal Affairs, United Nations. URL: <https://www.un.org/ola/en/news/united-nations-convention-against-cybercrime-opens-signature-hanoi>.
12. Караман К.В. Сучасна парадигма криміналістичного значення цифрових слідів у кримінальному провадженні. *Вісник Кримінологічної асоціації України*, 2025. № 2 (35). С. 224–232. URL: <https://vca.univd.edu.ua/index.php/vca/article/view/560/608>.
13. Мордвинцев М. В., Пашнев Д. В., Наконечний В. С. Особливості використання технологій відеоаналізу та програмного забезпечення з розпізнавання облич у кримінальному аналізі. *Право і безпека*. 2025. № 1 (96). С. 90–103. URL: <https://pb.univd.edu.ua/index.php/PB/article/view/853/691>.
14. Cuellar, M., et al. *Accuracy and Fairness of Facial Recognition Technology in Low-Quality Police Images*. URL: <https://arxiv.org/abs/2505.14320>. <https://doi.org/10.48550/arXiv.2505.14320>.
15. Моса В.В. Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами правоохоронних органів України. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. Випуск 73: частина 2, 2022. С.141–147. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/11/24-1.pdf>.
16. Interpol. *Spotlight Cybercrime Focus*. Outsmarting real-life criminals in the virtual world Interpol. URL: <https://www.interpol.int/es/Recursos/INTERPOL-Spotlight/Issue-2-Cybercrime/Spotlight-Cybercrime-Focus>.
17. INTERPOL, *Annual Report 2024*. URL: [https://www.interpol.int/content/download/23674/file/Annual\\_Report%202024\\_EN.pdf](https://www.interpol.int/content/download/23674/file/Annual_Report%202024_EN.pdf).

Дата першого надходження рукопису до видання: 23.12.2025  
Дата прийняття до друку рукопису після рецензування: 26.01.2026  
Дата публікації: 2.02.2026