Кримінальний процес та криміналістика

УДК 343.9:004.056

DOI https://doi.org/10.5281/zenodo.20408309

Вплив інноваційних технологій на ефективність правоохоронних органів у боротьбі із кіберзлочинністю

Дрижакова Діна Юріївна,
аспірантка, кафедра кримінально-правової політики та кримінального права, Інститут права, КНУ імені Тараса Шевченка, м. Київ, Україна, https://orcid.org/0009-0004-7585-5860

Товпига Ліна Миколаївна,
доктор філософії в галузі права, доцент кафедри цивільного права та процесу, Національний авіаційний університет, м. Київ, Україна, https://orcid.org/0000-0003-0625-1188

Квітатіані Карина Вячеславівна,
асистент, кафедра права, Вінницький національний аграрний університет, м. Вінниця, Україна, https://orcid.org/0009-0005-0291-5065

Прийнято: 15.05.2026 | Опубліковано: 27.05.2026

Анотація. Поглиблення цифровізації соціально-економічних процесів супроводжується ускладненням форм кіберзлочинності та інших правопорушень у віртуальному середовищі, що зумовлює необхідність удосконалення інструментів гарантування інформаційної безпеки держави. Інноваційні технології, зокрема штучний інтелект, аналітика великих даних та

автоматизовані інформаційно-аналітичні системи, трансформують процеси збирання, оброблення та аналізу оперативно-службової інформації, підтримують ухвалення тактичних і стратегічних рішень у діяльності правоохоронних органів. Метою дослідження є визначення впливу інноваційних технологій на результативність діяльності правоохоронних органів у сфері протидії правопорушенням у цифровому середовищі та обґрунтування умов їхнього ефективного застосування. Для розв'язання завдань дослідження використано такі методи: аналіз і синтез – для узагальнення наукових напрацювань, порівняльний метод – для зіставлення практик використання технологій, системно-структурний підхід – для виявлення взаємозв'язків між інструментами й управлінськими процесами та елементи статистичного оцінювання результативності діяльності правоохоронних органів. З'ясовано, що застосування інтелектуальних алгоритмів, технологій аналізу великих даних і автоматизованих систем моніторингу кіберпростору у діяльності правоохоронних органів забезпечує підвищення швидкості опрацювання оперативної інформації, точності виявлення кіберзагроз і правопорушень та ефективності ухвалення процесуальних і оперативно-службових рішень. Виявлено стримувальні чинники упровадження інноваційних технологій у правоохоронній діяльності, зокрема недостатній рівень інтеграції державних інформаційних ресурсів і баз даних, обмежений рівень цифрових та аналітичних компетентностей працівників правоохоронних органів, фрагментарність нормативно-правового регулювання у сфері кібербезпеки. Доведено, що результативність протидії кіберзлочинності значною мірою залежить від ефективності міжвідомчої взаємодії правоохоронних органів та узгодженості обміну інформацією між ними. Узагальнено, що застосування інноваційних технологій у діяльність правоохоронних органів сприяє підвищенню ефективності розкриття, розслідування та запобігання кіберзлочинам, однак потребує комплексного поєднання організаційних, правових і кадрових складників системи

формування кібербезпеки держави. Перспективи подальших досліджень пов’язані з удосконаленням інтеграції інформаційних систем правоохоронних органів та інших державних інституцій, розвитком їхніх аналітичних можливостей щодо оброблення великих масивів даних у сфері протидії кіберзлочинності.

Ключові слова: цифровізація, публічне управління, інформаційна безпека, великі дані, машинне навчання, аналітичні системи, цифрова криміналістика, інформаційний моніторинг.

Impact of innovative technologies on the efficiency of law enforcement agencies in combating cybercrime

Dina Dryzhakova,
Postgraduate Student, Department of Criminal Legal Policy and Criminal Law, Institute of Law, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, https://orcid.org/0009-0004-7585-5860

Lina Tovpyha,
PhD in Law, Docent of the Department of Department of Civil Law and Procedure, National Aviation University, Kyiv, Ukraine, https://orcid.org/0000-0003-0625-1188

Karyna Kvitatiani,
Assistant, Department of Law, Vinnytsia National Agrarian University, Vinnytsia, Ukraine, https://orcid.org/0009-0005-0291-5065

Abstract. The deepening digitalization of socio-economic processes is accompanied by the complication of cybercrime and other offenses in the virtual environment, necessitating improvements in tools to ensure the state's information security. Innovative technologies, in particular artificial intelligence, big data

analytics and automated information and analytical systems, transform the processes of collecting, processing and analyzing operational and service information and also support the adoption of tactical and strategic decisions in law enforcement agency activities. The purpose of the study is to determine the impact of innovative technologies on the effectiveness of law enforcement agencies in combating offenses in the digital environment, and to substantiate the conditions for their effective application. To solve the research tasks, the following methods were used: analysis and synthesis - to generalize scientific developments, a comparative method - to compare the practices of using technologies, a system-structural approach - to establish relationships between tools and management processes, as well as elements of statistical assessment of the effectiveness of law enforcement agencies. It has been established that the use of intelligent algorithms, big data analysis technologies and automated cyberspace monitoring systems in the activities of law enforcement agencies increases the speed of processing operational information, the accuracy of detecting cyber threats and offenses and the efficiency of making procedural and operational service decisions. Restraining factors for the implementation of innovative technologies in law enforcement activities have been identified, including insufficient integration of state information resources and databases, limited digital and analytical competencies among law enforcement officers, and fragmentation of cybersecurity regulatory and legal frameworks. It has been proven that the effectiveness of countering cybercrime largely depends on interagency cooperation and the consistency of information exchange between law enforcement agencies. In summary, the introduction of innovative technologies into law enforcement agencies' activities increases the efficiency of detecting, investigating and preventing cybercrime, but requires a comprehensive integration of the organizational, legal and personnel components of the state cybersecurity system. Prospects for further research include improving the integration of information systems across law enforcement agencies and other state institutions, as well as

ISSN: 3041-2110

developing their analytical capabilities for processing large data sets in combating cybercrime.

Keywords: digitalization, public administration, information security, big data, machine learning, analytical systems, digital forensics, information monitoring.

Постановка проблеми. Інтенсивний розвиток цифрового середовища супроводжується не лише розширенням можливостей для обміну інформацією, але й трансформацією форм протиправної діяльності, які набувають складнішого, латентного та технологічно опосередкованого характеру. Зростання кількості правопорушень у віртуальному просторі, їхня транскордонність та високий рівень адаптивності суб'єктів протиправної діяльності створюють суттєві виклики для функціонування правоохоронних органів. За таких умов традиційні механізми реагування виявляються недостатньо ефективними, що визначає необхідність переосмислення інструментального забезпечення їхньої діяльності.

Проблема полягає у невідповідності між динамікою розвитку цифрових технологій, які активно використовуються у протиправній діяльності, та рівнем упровадження інноваційних рішень у практику правоохоронних органів. Попри наявність окремих технологічних напрацювань, фрагментарність їхнього застосування, обмежена інтеграція інформаційних ресурсів і недостатній рівень координації між суб'єктами гарантування безпеки зумовлює зниження можливостей своєчасного виявлення загроз, ускладнення процесів аналізу інформації та негативно впливає на обґрунтованість ухвалення процесуальних і оперативно-службових рішень правоохоронними органами.

Відповідно, зв'язок сформульованої проблематики із науковими та практичними завданнями полягає у необхідності формування цілісного уявлення про роль технологічних рішень у підвищенні результативності

 ISSN: 3041-2110

діяльності правоохоронних органів та визначенні умов їхнього ефективного застосування. У науковому вимірі це передбачає поглиблення досліджень щодо інтеграції інформаційних систем, розвитку аналітичних інструментів та удосконалення методів оброблення даних. У практичному аспекті розв'язання цих питань сприятиме підвищенню якості управління, ухваленню обґрунтованих процесуальних і оперативно-службових рішень у сфері виявлення, розслідування та попередження кіберзлочинів, посиленню міжвідомчої взаємодії та зниженню рівня латентності правопорушень у цифровому середовищі.

Аналіз останніх досліджень і публікацій. Питання застосування інноваційних технологій у діяльності правоохоронних органів в умовах цифровізації активно розглядаються у вітчизняній та закордонній науковій літературі. Зокрема, теоретичні засади державної політики інформаційної безпеки в умовах гібридних загроз розкриває Ю. Бідзіля, акцентуючи на необхідності комплексного підходу до захисту інформаційного простору [1]. Роль поліції у забезпеченні кібербезпеки критичної інфраструктури у контексті цифровізації суспільства досліджує В. Василенко, підкреслюючи значення інституційної спроможності правоохоронних органів [2]. Водночас соціальні аспекти кібербезпеки в умовах воєнного стану висвітлюють С. Лучик та В. Лучик, звертаючи увагу на зростання вразливості цифрового середовища [3].

Основні проблеми протидії кіберзлочинності та організаційної ролі Національної поліції України розглядають Б. Макаліш, О. Мойко та В. Лучик, наголошуючи на необхідності удосконалення оперативно-аналітичних механізмів реагування [4]. Додатково, цифровізацію правоохоронних органів у контексті трансформації судової системи аналізує О. Ковальчук (O. Kovalchuk), виокремлюючи інституційні зміни у сфері правозастосування [5]. На цьому тлі механізми розвитку кіберзлочинної діяльності у воєнний

 ISSN: 3041-2110

період досліджує М. Пелих, визначаючи чинники ескалації цифрових загроз [6].

Окремі аспекти правозастосовної та теоретико-правової проблематики кібербезпеки висвітлюють С. Банах зі співавторами та М. Сніголя, В. Шевчук і Ю. Балтрунене, досліджуючи вплив штучного інтелекту на діяльність органів правопорядку та судової експертизи [7; 8]. А використання спеціальних засобів у діяльності поліції аналізують А. Жбанчик та О. Бойко, акцентуючи на необхідності оновлення концептуальних підходів до формування державної безпеки [9].

У цьому контексті закордонні дослідження розширюють уявлення про трансформацію кіберзлочинності та інструменти її протидії. Зокрема, виклики та рішення у сфері правозастосування у цифрову епоху аналізує М. Ф. Ф. Расийд (M. F. F. Rasyid) [10], а роль кібербезпеки у процесах виявлення та розслідування злочинів досліджують Т. Махмуд із колегами (T. Mahmood et al.) [11]. Одночасно застосування онтологічних моделей для цифрової криміналістики та аналізу кіберзагроз обґрунтовують Ї. Ч. Ток зі співавторами (Y. C. Tok et al.) [12], тоді як концепцію співпраці правоохоронних органів у межах кіберстійкості розглядає Ф. Шіліро (F. Schiliro) [13].

Крім того, відповідно до практико орієнтованих засад питання ефективності регуляторних змін у сфері кіберзлочинності вивчають А. Бухтіарова та Д. Тимошик [14], натомість особливості аналізу ризиків і стратегій кіберзахисту розглядають Д. Зінченко й О. Макарова [15].

Виділення невирішених раніше частин загальної проблеми. Усупереч значній кількості наукових напрацювань, присвячених застосуванню інноваційних технологій у діяльності правоохоронних органів, низка основних аспектів залишається недостатньо дослідженою. Передусім відсутнє цілісне оцінювання впливу технологічних рішень на результативність діяльності правоохоронних органів у сфері протидії кіберзлочинності з

 ISSN: 3041-2110

урахуванням взаємозв'язку між технічними, організаційними та правовими компонентами. Наявні дослідження здебільшого зосереджено на окремих інструментах (аналітика даних, автоматизовані системи, цифрова криміналістика), не враховуючи їхнього інтегрованого впливу на процеси управління діяльністю правоохоронних органів.

Водночас потребує розв'язання проблема інтеграції державних та відомчих інформаційних ресурсів і баз даних між різними суб'єктами сектору безпеки. Попри розвиток цифрових платформ, питання узгодженості форматів даних, швидкості обміну інформацією та забезпечення її вірогідності залишаються відкритими. Зокрема, малодослідженою є залежність результативності діяльності правоохоронних органів у сфері протидії кіберзлочинності від рівня професійної підготовки персоналу правоохоронних органів та їхньої здатності до використання складних аналітичних інструментів у практичній діяльності.

Причини збереження цих прогалин пов'язані із міждисциплінарним характером проблеми, що поєднує правові, технологічні та управлінські аспекти, й динамічністю цифрового середовища, яке ускладнює формування універсальних підходів до оцінювання результативності діяльності правоохоронних органів. Крім того, обмежений доступ до емпіричних даних і специфіка службової інформації стримують проведення комплексних досліджень.

Отже, ці питання є принципово важливими, оскільки без їхнього опрацювання неможливо сформувати обґрунтовані механізми підвищення результативності діяльності правоохоронних органів. А відсутність системного бачення впливу інноваційних технологій призводить до фрагментарності управлінських рішень і знижує ефективність використання наявних ресурсів.

Формулювання цілей статті (визначення завдання). Метою статті є комплексне дослідження впливу інноваційних технологій на результативність

ISSN: 3041-2110

діяльності правоохоронних органів у сфері протидії правопорушенням у цифровому середовищі.

Відповідно до мети дослідження сформульовано такі завдання:

– проаналізувати особливості трансформації протиправної діяльності у цифровому середовищі та її вплив на функціонування правоохоронних органів;

– визначити роль інноваційних технологій у процесах виявлення, аналізу та запобігання правопорушенням;

– дослідити взаємозв'язок між рівнем упровадження технологічних рішень та показниками діяльності правоохоронних органів у сфері протидії правопорушенням у цифровому середовищі;

– виявити основні обмеження, що стримують ефективне використання технологій, зокрема у сфері інтеграції інформаційних ресурсів, нормативного забезпечення та професійної підготовки персоналу;

– обґрунтувати напрями удосконалення використання технологічних інструментів з урахуванням потреб практичної діяльності.

Таким чином, обґрунтовані мета й завдання визначають логіку дослідження, орієнтовану на отримання науково обґрунтованих результатів, які мають значення як для розвитку теоретичних положень, так і для розв'язання прикладних завдань у сфері гарантування безпеки в умовах цифровізації.

Виклад основного матеріалу дослідження. Цифрове середовище характеризується зростанням складності протиправної активності, яка реалізується через використання розподілених мережевих інфраструктур, прихованих каналів комунікації та технологій анонімізації. Такі умови знижують результативність традиційних механізмів реагування і формують потребу в оновленні інструментів протидії кіберзагрозам [1]. У зв'язку із цим посилюється роль аналітичного оброблення даних та цифрових засобів виявлення правопорушень.

ISSN: 3041-2110

У практичній діяльності це виявляється у скороченні часу опрацювання інформації, підвищенні точності виявлення кіберзагроз та покращенні координації між підрозділами, залученими до протидії правопорушенням у цифровому середовищі. Важливу роль відіграють автоматизовані системи моніторингу, які постійно відстежують активність у мережі та дають змогу оперативно фіксувати підозрілі події ще на ранніх етапах їхнього розвитку.

У цьому процесі інноваційні технології змінюють характер роботи правоохоронних органів, оскільки забезпечують можливість охоплення великих обсягів інформації та виявлення прихованих зв'язків між подіями. Використання аналізу великих даних у поєднанні з алгоритмами машинного навчання сприяє структуруванню різнорідної інформації, визначенню взаємозв'язків між цифровими подіями та формуванню прогностичних моделей ризиків.

Такі технології є визначальними у виявленні, аналітичному опрацюванні та запобіганні правопорушенням у цифровому середовищі, оскільки забезпечують безперервний моніторинг інформаційного простору та глибоке оброблення великих обсягів даних. Зокрема, ефективність використання технологічних інструментів залежить від узгодженої роботи інформаційних систем, інтеграції джерел даних і рівня цифрової підготовки персоналу правоохоронних органів [2, с. 398]. Якщо ці компоненти функціонують розрізнено, знижується швидкість реагування та ускладнюється аналітична робота. Водночас залишаються проблеми, пов'язані із нерівномірним технічним забезпеченням, недостатнім рівнем підготовки фахівців і фрагментарністю нормативного регулювання у сфері кібербезпеки.

Особливо значущими такі засоби є під час роботи із цифровими злочинами. Так, у процесі виявлення кіберінцидентів цифрові інструменти фіксують аномальні дії у мережевих системах, відстежують нетипові поведінкові моделі користувачів і дають змогу оперативно ідентифікувати

ISSN: 3041-2110

потенційні загрози ще до їхньої реалізації. Це скорочує часовий інтервал між виникненням ризику та його реєстрацією.

У цьому контексті аналітичний компонент системи ґрунтується на структуризації різнорідної інформації, з'ясуванні прихованих зв'язків між подіями та формуванні цілісної картини цифрового середовища. Одночасно алгоритмічні методи опрацювання даних забезпечують виявлення закономірностей, що відображають схеми злочинної діяльності та їхню еволюцію.

У сфері запобігання порушенням технологічні рішення підтримують прогнозування розвитку ризиків і моделювання можливих сценаріїв їхньої реалізації. На основі накопичених масивів інформації формуються аналітичні висновки щодо ймовірних об'єктів впливу, способів атаки та рівня загрози, що дає змогу здійснювати випереджальне реагування.

Ще одним викликом застосування інноваційних технологій є запровадження воєнного стану в Україні, який посилив їхнє значення, оскільки зростає інтенсивність кібератак, збільшується навантаження на державні інформаційні системи та виникає потреба в оперативному обміні даними між структурами сектору безпеки [3]. За таких умов здатність правоохоронних органів швидко адаптуватися до технологічних змін безпосередньо впливає на ефективність реагування на загрози.

У підсумку формується тенденція до переходу від реактивного реагування до випереджального аналізу загроз, коли основна увага зосереджується на ранньому виявленні підозрілих цифрових активностей і прогнозуванні можливих сценаріїв розвитку кіберінцидентів.

Згідно із цим рівень упровадження технологічних рішень у діяльність правоохоронних органів безпосередньо впливає на результативність протидії правопорушенням у цифровому середовищі, що відбувається через зміну швидкості реагування, якості аналітичного опрацювання інформації та ефективності розкриття кіберінцидентів.

ISSN: 3041-2110

З огляду на це саме нормативно-правова база протидії правопорушенням у цифровому середовищі в Україні формує організаційні та функціональні умови для використання технологічних інструментів. Вона охоплює положення Закону України «Про основні засади забезпечення кібербезпеки України», який визначає засади функціонування національної системи кіберзахисту [16], Закону України «Про захист інформації в інформаційно-комунікаційних системах», що регламентує порядок оброблення та захисту даних [17], та Закону України «Про Національну поліцію», який регулює повноваження правоохоронних органів у сфері протидії правопорушенням [18]. Додатково застосовуються норми Кримінального кодексу України щодо злочинних правопорушень у сфері інформаційних технологій [19] та Кримінального процесуального кодексу України щодо збирання й використання електронних доказів [20]. Сукупність зазначених положень окреслює правові межі упровадження цифрових рішень, однак потребує подальшої гармонізації із міжнародними стандартами

Однак наразі саме ці регуляторні документи спрямовані на ефективну боротьбу із трансформацією протиправної діяльності у цифровому середовищі, яка характеризується переходом до мережевих, розподілених і технологічно складних форм її реалізації. Зокрема, використання шифрування, анонімних каналів комунікації та прихованих інфраструктур ускладнює ідентифікацію джерел загроз і підвищує вимоги до технічного забезпечення правоохоронної діяльності.

Така зміна характеру кіберзлочинності зумовлює переорієнтацію правоохоронних органів на використання цифрових засобів збирання, оброблення та аналізу інформації, систем моніторингу мережевої активності та аналітичних платформ [4, с. 315]. За таких умов рівень застосування технологічних рішень визначає здатність оперативно виявляти інциденти, аналізувати їхню структуру та формувати доказову базу.

ISSN: 3041-2110

Вплив технологічної інтеграції на результативність діяльності виявляється через кілька взаємопов'язаних параметрів. На базовому рівні використання окремих цифрових інструментів забезпечує лише часткове прискорення опрацювання інформації. На інтегрованому рівні поєднання інформаційних систем підвищує точність аналітичних висновків і покращує координацію між підрозділами. На комплексному рівні, коли застосовуються автоматизовані аналітичні платформи та засоби оброблення великих масивів даних, досягається найвищий рівень оперативності реагування та прогнозування ризиків.

Окремим чинником ефективності є професійна підготовка персоналу, оскільки недостатній рівень цифрових компетентностей знижує результативність навіть за умови наявності сучасних технологічних рішень [5, p. 46]. Додатковий вплив має фрагментарність нормативного регулювання та нерівномірність технічного забезпечення, що обмежує повноцінну інтеграцію цифрових інструментів у практичну діяльність.

У табл. 1 систематизовано основні цифрові інструменти, які застосовуються у діяльності правоохоронних органів, зокрема у сферах міжвідомчої взаємодії, професійної підготовки персоналу, оперативно-аналітичного опрацювання інформації та підтримки процесів розслідування правопорушень у цифровому середовищі.

Таблиця 1

Цифрові інструменти забезпечення діяльності правоохоронних органів у сфері протидії правопорушенням у цифровому середовищі

Напрям застосування	Цифровий інструмент	Функціональне призначення	Значення у практичній діяльності
Міжвідомча та міжнародна взаємодія	SIENA (Europol Secure Information Exchange Network Application)	Захищений обмін оперативною інформацією між правоохоронними органами	Забезпечує координацію розслідувань транснаціональних правопорушень
	INTERPOL I-24/7	Доступ до міжнародних баз даних Інтерполу	Сприяє ідентифікації осіб, об'єктів і

ISSN: 3041-2110

Напрям застосування	Цифровий інструмент	Функціональне призначення	Значення у практичній діяльності
			транспортних засобів
Моніторинг та виявлення кіберзагроз	SIEM-системи (Security Information and Event Management)	Збирання, кореляція та аналіз подій інформаційної безпеки	Забезпечує раннє виявлення кіберінцидентів і координацію реагування
	OSINT-платформи (Maltego, SpiderFoot)	Аналіз відкритих джерел інформації	Визначає зв'язки між цифровими об'єктами та подіями
Оперативно-аналітична діяльність	Аналітичні платформи (Palantir Gotham)	Інтеграція та візуалізація великих масивів даних	Підтримує комплексний аналіз інформації під час розслідувань
	Інструменти Big Data та ML	Оброблення великих масивів даних і прогнозування ризиків	Підвищує точність виявлення кіберзагроз
Підтримка розслідувань	Цифрові криміналістичні інструменти	Аналіз цифрових слідів та електронних доказів	Забезпечує фіксацію та відтворення кіберінцидентів
	Форензік-платформи	Дослідження цифрових доказів	Підтримує доказову базу у кримінальному провадженні
Професійна підготовка персоналу	LMS (Moodle, Blackboard)	Навчання та контроль знань	Розвиток цифрових компетентностей персоналу
	Кіберполігони (Cyber Range)	Моделювання кіберінцидентів	Формування практичних навичок реагування
	Симуляційні системи розслідувань	Відтворення слідчих ситуацій	Підвищення якості прийняття рішень

Джерело: власна розробка авторів

Отже, аналіз цифрових рішень засвідчує їхню функціональну диференціацію відповідно до завдань правоохоронної діяльності та ступеня інтеграції у практичні процеси. Інструменти інформаційного обміну забезпечують узгодженість дій між підрозділами та оперативність

передавання даних у межах розслідувань. Системи моніторингу кіберпростору сприяють своєчасному виявленню загроз, їхній ідентифікації та первинному оцінюванню ризиків.

Наступний рівень оброблення інформації забезпечують аналітичні платформи та технології опрацювання великих масивів даних, що дають змогу виявляти приховані зв'язки між подіями, формувати інформаційні моделі та підтримувати ухвалення управлінських рішень під час оперативно-службової діяльності. А навчально-симуляційні системи розширюють можливості підготовки персоналу, забезпечуючи відпрацювання алгоритмів реагування на кіберінциденти та підвищення рівня професійної готовності до роботи в умовах цифрових загроз.

Аналіз цих даних дає підстави стверджувати, що цифрові інструменти утворюють багаторівневу систему підтримки правоохоронної діяльності, у межах якої поєднуються інформаційний обмін, аналітичне опрацювання даних і розвиток професійних компетентностей. Ефективність функціонування такої системи значною мірою зумовлено динамікою зовнішніх безпекових умов, серед яких особливої значущості набуває збільшення кількості кіберзагроз у воєнний період.

Зростання інтенсивності та складності атак змінює організацію протидії правопорушенням у цифровому середовищі та потребує розширення можливостей правоохоронних органів через упровадження аналітичних, моніторингових та інтеграційних рішень. За цих умов цифрові інструменти набувають системоутворювального значення, забезпечуючи безперервне збирання й опрацювання даних, оперативність реагування та координацію взаємодії між суб'єктами кібербезпеки [6, с. 236].

Вплив інтеграції технологічних інструментів на результативність діяльності правоохоронних органів може бути продемонстровано через зміни у показниках ефективності (рис. 1).

 ISSN: 3041-2110

Наведена на рис. 1 модель відображає характер впливу технологічних рішень на результативність діяльності правоохоронних органів, де взаємодія елементів формує єдиний аналітико-оперативний контур. Вирішальне значення має поєднання швидкості опрацювання інформації та якості аналітичних результатів, оскільки саме ці параметри зумовлюють оперативність реагування та рівень обґрунтованості рішень у практичній діяльності.

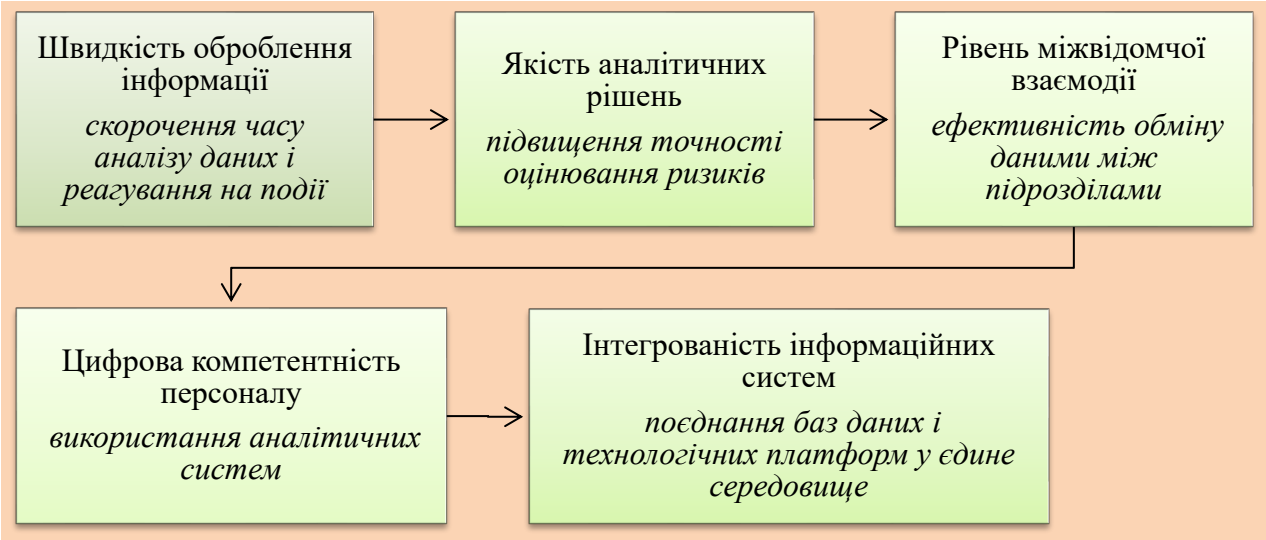

Рис. 1. Вплив технологічних рішень на показники результативності діяльності правоохоронних органів

Джерело: власна розробка авторів

Подальший ефект реалізується через організаційні умови функціонування системи, особливо за узгодженості міжвідомчої взаємодії, яка визначає ефективність обміну даними та координації дій. Її недостатній рівень знижує можливості використання цифрових інструментів і уповільнює процес реагування на правопорушення.

Крім того, важливим системоутворювальним елементом є інтегрованість інформаційних систем, що формує єдине інформаційне середовище для накопичення, зіставлення та аналізу даних. Фрагментація інформаційних ресурсів ускладнює комплексне аналітичне оцінювання ситуацій і знижує точність управлінських рішень. У цьому контексті визначальною є цифрова компетентність персоналу, яка забезпечує практичне

використання технологічних можливостей; її недостатній рівень обмежує ефективність навіть інтегрованих систем.

Одночасно аналіз практики упровадження цифрових рішень дає змогу виокремити системні обмеження їхньої реалізації. Одним із них є недостатня узгодженість інформаційних потоків між відомствами, що призводить до дублювання та втрати оперативності оброблення даних і знижує якість аналітичного забезпечення [7, с. 235].

Додатковим стримувальним чинником є невідповідність нормативного регулювання темпам технологічного розвитку [8, с. 26]. Відсутність єдиних стандартів використання цифрових інструментів та опрацювання електронних доказів ускладнює міжвідомчу взаємодію і зменшує рівень уніфікації процесів.

Окремо постає кадровий аспект, оскільки ефективність технологічного забезпечення залежить від рівня підготовки персоналу [9, с. 214]. Нерівномірність цифрових навичок та обмежений доступ до спеціалізованого навчання формують дисбаланс у використанні аналітичних інструментів між різними підрозділами.

Отже, із метою підвищення ефективності використання технологічних рішень доцільним є упровадження низки організаційно-інноваційних заходів. Насамперед перспективним напрямом є створення єдиної національної аналітичної платформи із модульною архітектурою, що забезпечуватиме не лише обмін даними, а і їхню автоматизовану інтерпретацію із застосуванням алгоритмів прогнозування ризиків у режимі реального часу.

Додатково доцільно розвивати систему цифрового наставництва у межах правоохоронних органів, яка передбачатиме закріплення за досвідченими аналітиками молодших співробітників для формування практичних навичок роботи зі складними інформаційними масивами. Такий підхід дасть змогу скоротити адаптаційний період та підвищити рівень готовності персоналу до роботи в умовах високої динаміки кіберзагроз.

ISSN: 3041-2110

Крім того, перспективним є застосування елементів гейміфікованого професійного тренінгу, основаного на моделюванні кризових цифрових ситуацій із багатоваріантними сценаріями розвитку подій. Це сприятиме формуванню здатності до швидкого затвердження рішень в умовах невизначеності та підвищенню адаптивності оперативного реагування. Окрему увагу варто приділити розвитку партнерських програм із приватним сектором у сфері кібербезпеки для оперативного обміну технологічними рішеннями та аналітичними інструментами.

Висновки. Під час дослідження узагальнено особливості впливу інноваційних технологій на діяльність правоохоронних органів у сфері протидії правопорушенням у цифровому середовищі. Визначено, що основні зміни виявляються у прискоренні аналітичного оброблення інформації, підвищенні точності ідентифікації кіберзагроз та розширенні можливостей оперативного реагування.

Результати аналізу засвідчують, що ефективність протидії кіберзлочинності зростає за умови поєднання технологічних рішень із належним рівнем організаційної взаємодії та цифрової підготовки персоналу. Найбільший ефект спостерігається у випадках інтеграції аналітичних систем, інструментів моніторингу та засобів опрацювання великих масивів даних у єдине інформаційне середовище.

З’ясовано, що трансформація кіберзлочинної діяльності ускладнює процес її виявлення, що зумовлює необхідність переходу до превентивних моделей реагування, орієнтованих на ранню ідентифікацію загроз та прогнозування ризиків. Підтверджено, що результативність діяльності правоохоронних органів залежить від ступеня інтеграції цифрових технологій, рівня міжвідомчої координації та якості кадрового забезпечення, які у сукупності формують здатність системи до своєчасного реагування на кіберінциденти.

ISSN: 3041-2110

Перспективним напрямом подальших досліджень є розроблення комплексних моделей оцінювання ефективності цифрової трансформації правоохоронної діяльності із застосуванням міждисциплінарних підходів, що поєднують правові, управлінські та інформаційно-аналітичні методології. Зокрема, необхідним є поглиблення аналізу етичних і правових аспектів використання автоматизованих систем у сфері гарантування безпеки.

Список використаних джерел

1. Бідзіля Ю. М. Державна політика інформаційної безпеки в умовах гібридних загроз. *Український політико-правовий дискурс*. 2025. № 17. DOI: https://doi.org/10.5281/zenodo.17757320.

2. Василенко В. М. Національна кібербезпека в контексті цифровізації суспільства: роль поліції у захисті критичної інфраструктури. *Бюлетень Харківського національного університету внутрішніх справ*. 2025. Т. 109, № 2. С. 392–405. DOI: https://doi.org/10.32631/v.2025.2.33.

3. Лучик С., Лучик В. Кібербезпека в умовах війни: соціальні аспекти. *Наука і техніка сьогодні. Серія «Техніка».* 2024. № 7(35). С. 857–870. DOI: https://doi.org/10.52058/2786-6025-2024-7(35)-857-870.

4. Макаліш Б. Д., Мойко О. О., Лучик В. Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3(31). С. 309–322. DOI: https://doi.org/10.28925/2663-4023.2025.31.983.

5. Kovalchuk O. Digitalization of law enforcement agencies in the digital transformation of the judiciary. *Entrepreneurship, Economy and Law*. 2023. № 5. С. 42–52. DOI: https://doi.org/10.32849/2663-5313/2023.5.07.

6. Пелих М. Механізми розвитку кіберзлочинної діяльності у воєнний період. *Development Service Industry Management*. 2024. № 3. С. 219–222. DOI: https://doi.org/10.31891/dsim-2024-7(32).

7. Банах С., Юзвін Х., Колісник В., Дукач В., Бойко Ю. Актуальні проблеми правознавства. *Актуальні проблеми правознавства*. 2025. № 1(41). С. 233–239. DOI: https://doi.org/10.35774/app2025.01.233.

8. Сніголя М., Шевчук В., Балтрунене Ю. Штучний інтелект у діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. 2022. № 4(29). С. 12–49. DOI: https://doi.org/10.32353/khrife.4.2022.02.

9. Жбанчик А. В., Бойко О. І. Спеціальні засоби в діяльності поліції: нова концепція. *Аналітично-порівняльне правознавство*. 2022. № 5. С. 212–216. DOI: https://doi.org/10.24144/2788-6018.2022.05.39.

10. Rasyid M. F. F. Cybercrime: challenges and solutions in law enforcement in the digital era. *Proceeding of the International Conference on Law and Human Rights*. 2024. Vol. 1, № 1. P. 76-85. DOI: https://doi.org/10.62383/iclehr.v1i1.28.

11. Mahmood T., Rasool F. G., Samee H. Technological innovations in criminal justice: the role of cybersecurity in crime detection, investigation and prevention. *Journal of Asian Development Studies*. 2025. Vol. 14, № 1. P. 1579–1593. DOI: https://doi.org/10.62345/jads.2025.14.1.125.

12. Tok Y. C., Zheng D. Y., Chattopadhyay S. A smart city infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International: Digital Investigation.* 2025. Vol. 52. DOI: https://doi.org/10.48550/arXiv.2408.02023.

13. Schiliro F. Building a resilient cybersecurity posture: a framework for leveraging prevent, detect and respond functions and law enforcement collaboration. *arXiv*. 2023. DOI: https://doi.org/10.48550/arXiv.2303.10874.

14. Зінченко Д. А., Макарова О. П. 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 р.). Вінниця: ХНУВС, 2023. С. 118–121. URL:

https://dspace.univd.edu.ua/handle/123456789/17463 (дата звернення: 28.04.2026).

15. Бухтіарова А. Г., Тимошик Д. Д. Оцінка ефективності регуляторних змін у боротьбі з кіберзлочинністю: географічна і часова складові. *Цифрові трансформації та інноваційні технології в економіці: виклики, реалії, стратегії*: матеріали Міжнар. наук.-практ. конф. (м. Суми, 27–29 трав. 2024 р.). Суми: Сумський державний університет, 2024. С. 28–31. URL: https://essuir.sumdu.edu.ua/handle/123456789/98207 (дата звернення: 28.04.2026).

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.04.2026).

17. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 28.04.2026).

18. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 28.04.2026).

19. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 28.04.2026).

20. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 28.04.2026).

 ISSN: 3041-2110