2. Chapelle C. A. Generative AI as Game Changer: Implications for Language Education. *System*. 2025. Vol. 132. Art. 103672. DOI: https://doi.org/10.1016/j.system.2025.103672.

3. Law L. Application of Generative Artificial Intelligence (GenAI) in Language Teaching and Learning: A Scoping Literature Review. *Computers and Education Open*. 2024. Vol. 6. Art. 100174. DOI: https://doi.org/10.1016/j.caeo.2024.100174.

4. Li B., Lowell V. L., Wang C., Li X. A Systematic Review of the First Year of Publications on ChatGPT and Language Education: Examining Research on ChatGPT's Use in Language Learning and Teaching. *Computers and Education: Artificial Intelligence*. 2024. Vol. 7. Art. 100266. DOI: https://doi.org/10.1016/j.caeai.2024.100266.

5. NATO Standard ATrainP-5, Edition A, Version 2, Language Proficiency Levels. Brussels : NATO Standardization Office, 2016. 32 p.

6. Weng Z., Fu Y. Generative AI in Language Education: Bridging Divide and Fostering Inclusivity. *International Journal of Technology in Education*. 2025. Vol. 8, no. 2. P. 395–420. DOI: https://doi.org/10.46328/ijte.1056.

МАЦЮК МИКОЛА МИКОЛАЙОВИЧ
курсант 214 н. гр. факультету забезпечення державної безпеки Київський інститут Національної гвардії України

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Останніми роками впровадження інформаційних технологій у діяльність правоохоронних органів стало одним із найбільш актуальних напрямів наукового та практичного осмислення. Це зумовлено тим, що сучасна система забезпечення правопорядку вже не може ефективно функціонувати без швидкого доступу до інформації, її обробки, аналізу, захисту та оперативного обміну між підрозділами. В умовах зростання кількості безпекових викликів, кіберризиків і загального навантаження на сектор безпеки цифрові рішення фактично стали важливим інструментом підтримання правопорядку та захисту громадян.

Разом із тим цифровізація правоохоронної сфери не обмежується лише технічним оновленням або впровадженням нових програмних продуктів.

Рівень цифровізації правоохоронних органів безпосередньо впливає на їхню здатність реагувати на сучасні виклики – від традиційної злочинності до кіберзагроз, інформаційних атак і проявів гібридної агресії [1; 2]. У цьому сенсі інформаційні технології вже давно перестали бути другорядним елементом службової діяльності й поступово перетворилися на один із системоутворюючих компонентів функціонування правоохоронної системи. Йдеться про значно ширший процес, який пов'язаний зі зміною підходів до збору, зберігання, передачі та використання інформації, а також ставить питання про дотримання прав людини, захист персональних даних і правові межі використання цифрових механізмів державного контролю.

У мирний час застосування інформаційних технологій охоплює практично всі основні напрями роботи правоохоронних органів: криміналістичний аналіз, оперативно-розшукову діяльність, профілактику правопорушень, забезпечення громадського порядку, контроль за безпекою дорожнього руху, документування подій та міжвідомчу взаємодію [1]. Важливе місце в цьому процесі займає створення інтегрованих інформаційних систем, які дозволяють об'єднувати різні бази даних і забезпечувати швидкий обмін відомостями між підрозділами та іншими уповноваженими структурами.

Одним із найбільш помітних напрямів використання сучасних цифрових рішень є системи відеоспостереження з функцією автоматизованого розпізнавання облич. Такі технології поєднують технічні засоби відеофіксації з алгоритмами штучного інтелекту, що дозволяє

ідентифікувати осіб, відстежувати пересування, виявляти потенційно небезпечні ситуації та використовувати відеоматеріали у процесі розслідування [3].

Водночас потенціал штучного інтелекту у правоохоронній діяльності є значно ширшим, ніж просто ідентифікація осіб за зображенням. Такі технології можуть застосовуватися для виявлення атипової поведінки, аналізу великих масивів інформації, автоматизованого сортування даних, підтримки кримінального аналізу та цифрової криміналістики. Крім того, у міжнародній практиці активно застосовуються інструменти штучного інтелекту у сфері превенції злочинності, аналітичного прогнозування та підвищення ефективності діяльності правоохоронних структур [2, 4].

Не менш важливим напрямом є функціонування централізованих баз даних, які дозволяють накопичувати відомості про осіб, причетних до правопорушень, їхні біометричні дані, кримінальні записи, інформацію про судимості та інші відомості, необхідні для службової діяльності. Наявність таких ресурсів суттєво пришвидшує встановлення осіб, перевірку зв'язків між ними та виявлення певних закономірностей у структурі злочинної діяльності.

Суттєві можливості відкриває також використання прогностичних систем аналізу даних. Їх функціонування ґрунтується на обробці статистичних, соціально-економічних, демографічних та інших відомостей з метою виявлення криміногенних тенденцій і прогнозування ризиків скоєння правопорушень у конкретних місцях або за певних обставин [3]. Подібні інструменти дають змогу ефективніше планувати профілактичну діяльність, оптимізувати використання сил і засобів та приймати більш обґрунтовані управлінські рішення.

У цьому контексті предиктивна аналітика поступово стає одним із найбільш перспективних напрямів розвитку цифрових рішень у правоохоронній сфері. Її значення полягає не лише у виявленні вже наявних закономірностей, а й у здатності прогнозувати можливі ризики, своєчасно виявляти потенційно небезпечні тенденції та посилювати превентивну складову діяльності правоохоронних органів [2].

Проте в умовах воєнного стану роль інформаційних технологій у правоохоронній діяльності набуває зовсім іншого масштабу. Якщо у звичайних умовах цифрові інструменти переважно спрямовані на оптимізацію службової діяльності, то під час війни вони стають елементом стратегічної стійкості держави, забезпечують координацію між силовими структурами та швидке реагування на кризові ситуації для підтримання функціонування критично важливих механізмів безпеки [5]. Крім того, формування спеціалізованих електронних реєстрів, пошукових систем та захищених каналів обміну інформацією дає можливість швидше встановлювати осіб, систематизувати відомості, координувати дії між різними структурами та ефективніше реагувати на складні ситуації.

У цьому контексті особливої актуальності набуло питання ведення обліку осіб, зниклих безвісти за особливих обставин. Правові засади функціонування відповідного механізму визначені Законом України «Про правовий статус осіб, зниклих безвісти за особливих обставин», який передбачає функціонування Єдиного реєстру осіб, зниклих безвісти за особливих обставин.

Ведення Реєстру покладено на Міністерство внутрішніх справ України, яке в межах своїх повноважень забезпечує інформаційну взаємодію з іншими державними ресурсами, у тому числі із використанням персональних даних. Такий обмін здійснюється в електронній формі з обов'язковим застосуванням технічних і криптографічних засобів захисту інформації відповідно до вимог законодавства України [3].

Ще одним важливим цифровим інструментом є база даних «Розшук», порядок формування та ведення якої визначена наказом МВС України від 28 червня 2023 року № 534.

База даних «Розшук» функціонує як автоматизований банк даних, у якому накопичується інформація про осіб, що переховуються від органів досудового розслідування або суду, ухиляються від відбування покарання, зникли безвісти, підлягають примусовій психіатричній допомозі, а також інших осіб, передбачених відповідними нормативними актами [1; 3].

Отже, подальший розвиток правоохоронної системи України безпосередньо пов'язаний із поглибленням цифрової трансформації, упровадженням автоматизованих реєстрів, інтелектуальних аналітичних систем, безпечних платформ обміну даними та інших сучасних технологічних рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Застосування інформаційних технологій у правоохоронній діяльності: матеріали круглого столу (м. Харків, 14 груд. 2023 р.). Харків: ХНУВС, 2023. С. 122–125.
2. Вікторчук М. В., Багатко А. С. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності // *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 3. № 86. С. 238–244.
3. Сучасні інформаційні технології в діяльності Національної поліції: матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 02 листоп. 2023 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2024. 184 с.
4. Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності: теоретико-правовий аспект // *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 3. № 90. С. 184–190.
5. Базові аспекти цифровізації та їх правове забезпечення: монографія / за ред. К. В. Єфремової. Харків: НДІ ПЗІР, 2021. 180 с.

МАЦЮК МИКОЛА МИКОЛАЙОВИЧ
курсант 214 н. гр. факультету забезпечення державної безпеки Київський інститут Національної гвардії України

КОБА МАРІЯ МИКОЛАЇВНА
доктор філософії в галузі права, доцент, доцент кафедри правового забезпечення та правоохоронної діяльності, Київський інститут Національної гвардії України

КІБЕРПРОСТІР У ГІБРИДНІЙ ВІЙНІ ПРОТИ УКРАЇНИ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Проблема кібербезпеки набуває багатовимірного характеру та є критично важливою для забезпечення глобальної стабільності в умовах цифровізації суспільства. Зростання кількості та складності кібератак зумовлює необхідність посилення міжнародної співпраці та вироблення узгоджених правових підходів до протидії кіберзагрозам. Розвиток високотехнологічних форм кіберзлочинності та потреба у забезпеченні конфіденційності даних спонукають держави до формування нових правових механізмів регулювання кіберпростору [1].

Актуальність обраної нами проблематики посилюється безпрецедентним зростанням інформаційних загроз, що супроводжують сучасні збройні конфлікти. Гібридна війна, яку проводить рф проти України, характеризується поєднанням традиційних і нетрадиційних методів ведення війни, серед яких кібератаки та інформаційні операції займають ключове місце [2, с. 23]. Це формує нові виклики для міжнародного права та потребує переосмислення існуючих підходів до регулювання.

Проблематику міжнародно-правового регулювання кіберпростору та кіберконфліктів досліджують як вітчизняні науковці, зокрема Д. Дубов, О. Пазюк, О. Мережко, так і зарубіжні вчені, серед яких Michael N. Schmitt, Wolff Heintschel von Heinegg та Heather Harrison Dinniss.

Кібербезпека є однією з політичних сфер глобального управління даними. В умовах ескалації кіберзагроз, особливо у контексті збройних конфліктів, нагальною є потреба у створенні гармонізованої міжнародно-правової бази. Вирішення міжнародних проблем кібербезпеки та захисту даних потребує багатогранного підходу, що поєднує співпрацю між державами, зміцнення технічних і правових можливостей, а також формування глобальної культури кібербезпеки [1].