УДК 004.056:343.9:351.74
DOI https://doi.org/10.32782/chern.v3.2025.19

Т. А. Латковська
доктор юридичних наук, професор
Чернівецького навчально-наукового юридичного інституту
Національного університету «Одеська юридична академія»
orcid.org/0000-0003-3159-5994

П. П. Латковський
кандидат юридичних наук, доцент
Національного університету «Одеська юридична академія»
orcid.org/0000-0002-2406-766X

Т. І. Демчук
доктор філософії,
Чернівецького навчально-наукового юридичного інституту
Національного університету «Одеська юридична академія»
orcid.org/0000-0002-0955-1816

ІНФОРМАЦІЙНІ РЕСУРСИ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: АСПЕКТИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ВИКЛИКИ

Стаття присвячена комплексному дослідженню сучасних викликів інформаційним ресурсам у правоохоронній діяльності, аспектам кібербезпеки, яка є одним із пріоритетів у системі національної безпеки будь-якої країни. Реалізація зазначеного пріоритету має здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Нові виклики несе зростання питомої ваги кіберзагроз у спектрі загроз національній безпеці країн, що в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. У статті акцентується увага на тому, що швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам безпечне функціонування національного сегмента кіберпростору, передбачати нові можливості для цифровізації всіх сфер суспільного життя.

Кожна країна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір, де враховуються права і свободи людини та громадянина, підтримуються соціальний, політичний і економічний розвиток. У статті відмічено складну взаємодію між технологічним прогресом, законодавчими рамками та оперативними викликами, які формують ефективність цифрових інструментів у правоохоронній діяльності та підкреслено, що глобальний характер кіберзагроз вимагає міжнародної співпраці для ефективного протидіяння транснаціональній кіберзлочинності.

Зроблено висновок про роль інформаційних ресурсів у правоохоронній діяльності, що виходить далеко за межі простого впровадження технологій. Вона вимагає комплексного підходу, який поєднує міжнародну співпрацю, постійну освіту та передові інновації для ефективного вирішення як поточних, так і майбутніх викликів.

Ключові слова: правоохоронна діяльність, інформаційні ресурси, цифровізація, кібербезпека, кіберзагрози, кіберзлочини.

Latkovska T. A., Latkovskyi P. P., Demchuk T. I. **INFORMATION RESOURCES IN LAW ENFORCEMENT ACTIVITIES: ASPECTS OF CYBERSECURITY AND CONTEMPORARY CHALLENGES**

The article is devoted to a comprehensive study of contemporary challenges to information resources in law enforcement, aspects of cybersecurity, which is one of the priorities in the national security system of any country. The implementation of this priority must be achieved by enhancing the capabilities of the national cybersecurity system to counter cyber threats in the modern security environment. New challenges arise from the increasing proportion of cyber threats within the spectrum of threats to national security, which will intensify over the next decade with the development of information technologies and their convergence with artificial intelligence technologies. The article emphasises that the rapidly evolving digital world necessitates the formation of a more balanced and effective national cybersecurity system capable of flexibly adapting to changes in the security environment, ensuring citizens' safe operation within the national segment of cyberspace, and anticipating new opportunities for digitisation across all spheres of public life.

Every country strives to create an open, free, stable, and secure cyberspace where the rights and freedoms of individuals and citizens are respected, and social, political, and economic development is supported. The article highlights the complex interplay between technological progress, legislative frameworks, and operational challenges that shape the effectiveness of digital tools in law enforcement. It further emphasises that the global nature of cyber threats necessitates international cooperation to effectively counter transnational cybercrime.

A conclusion has been drawn regarding the role of information resources in law enforcement, which extends far beyond the mere implementation of technologies. It necessitates a comprehensive approach that combines international

cooperation, continuous education, and cutting-edge innovations to effectively address both current and future challenges.

Key words: law enforcement activities, information resources, digitalisation, cybersecurity, cyber threats, cybercrime.

Постановка проблеми. Зростаюча залежність від інформаційних ресурсів у правоохоронній діяльності призвела до появи як можливостей, так і викликів, особливо у сфері кібербезпеки. Сучасна поліцейська та слідча діяльність тісно пов'язана з цифровими інструментами, базами даних та мережевими системами, які підвищують оперативну ефективність, але також роблять органи влади вразливими до кіберзагроз. Інтеграція передових технологій, таких як штучний інтелект, аналітика великих даних і хмарні обчислення, революціонізувала запобігання та виявлення злочинності, проте ці інновації одночасно створюють загрозу, якою можуть скористатися зловмисники. Кібербезпека в правоохоронних органах більше не є периферійним питанням, це центральний компонент підтримання довіри громадськості та забезпечення цілісності конфіденційних даних. Особливій увазі піддається характер інформації, яку обробляють правоохоронні органи, що часто включає персональні дані, кримінальні записи та спеціальну розвідку, яку ще називають класифікованою розвідкою – це збір та аналіз інформації, яка має особливу важливість і потребує захисту від розголошення.

Однією з основних проблем у цій сфері є постійне ускладнення кіберзагроз, що націлені на інфраструктуру правоохоронних органів. Кіберзлочинці використовують тактику, таку як атаки з вимогою викупу, фішингові схеми та розподілені атаки типу «відмова в обслуговуванні» (DDoS), щоб порушити роботу або викрасти критичну інформацію. Ці загрози посилюються через зростаюче використання кримінальними організаціями зашифрованих каналів зв'язку, що ускладнює законне перехоплення. Крім того, поширення пристроїв Інтернету речей (IoT) у поліцейській діяльності – від нагрудних камер до систем спостереження – розширює поверхню атаки, що вимагає надійних протоколів безпеки для зменшення ризиків. Динамічний характер кіберзагроз потребує постійної адаптації захисних стратегій, проте обмежені ресурси та бюрократична інерція часто перешкоджають своєчасному реагуванню.

Ще однією критичною проблемою є етичні та правові наслідки використання інформаційних ресурсів у правоохоронній діяльності. Хоча поліція, що базується на даних, підвищує точність і прозорість, це також викликає занепокоєння щодо порушень конфіденційності та алгоритмічної упередженості. Наприклад, використання інструментів прогностичної поліції критикували за збереження системних нерівностей через непропорційне націлювання на маргіналізовані спільноти. Збалансування безпекових імперативів із громадянськими свободами залишається суперечливим питанням, особливо в юрисдикціях із суворими нормами захисту даних, такими як Загальний регламент щодо захисту даних (GDPR). Політики та керівники правоохоронних органів мають долати ці складності, щоб гарантувати, що технологічний прогрес не підриває демократичні принципи та не підриває довіру громадськості.

Перетин кібербезпеки та правоохоронної діяльності також підкреслює важливість міжвідомчої співпраці та міжнародного співробітництва. Кіберзлочинність є за своєю природою транснаціональною, що вимагає узгоджених дій через кордони для ефективного протидіяння таким загрозам, як злочинні угруповання хакерів або державна шпигунська діяльність. Однак розбіжності в правових рамках і технічних можливостях між країнами часто перешкоджають спільним зусиллям. Отже, посилення глобальних партнерств із одночасним подоланням юрисдикційних викликів є необхідним для розвитку стійкої кібербезпеки в правоохоронній сфері. Оскільки цифрова трансформація прискорюється в усіх галузях, проактивні заходи – включаючи підготовку кадрів, модернізацію інфраструктури та гармонізацію політик – будуть вирішальними для захисту інформаційних ресурсів від нових загроз.

Метою статті є дослідження інформаційних ресурсів у правоохоронній діяльності в умовах воєнного стану, проблем їх використання, а також постійне ускладнення кіберзагроз.

Виклад основного матеріалу. Інтеграція інформаційних ресурсів у правоохоронну діяльність стала наріжним каменем сучасного поліцейського функціонування, особливо у протидії кіберзлочинності та забезпеченні кібербезпеки. Слід відмітити складну взаємодію між технологічним прогресом, законодавчими рамками та оперативними викликами, які формують ефективність цифрових інструментів у правоохоронній діяльності. Найбільш помітною є зростаюча залежність від прийняття рішень на основі даних, що трансформувало традиційні методи розслідування. Правоохоронні органи нині використовують величезні масиви даних, від кримінальних записів до потоків даних у реальному часі з систем спостереження, для виявлення закономірностей та прогнозування потенційних загроз. Однак цей перехід до поліцейської діяльності, орієнтованої на даних, порушує критичні питання щодо їх точності, проблем конфіденційності та етичних наслідків застосування прогностичних алгоритмів.

Важливий виклик стосується вразливостей, властивих базам даних правоохоронних органів. Незважаючи на їхню корисність, ці системи часто стають мішенню кіберзлочинців, які прагнуть маніпулювати або викрадати конфіденційну інформацію. Випадки несанкціонованого доступу до поліцейських мереж підкреслюють нагальну потребу в надійних заходах кібербезпеки. Статистичні дані доводять, що багато установ досі покладаються на застарілі протоколи шифрування та недостатні механізми автентифікації, що робить їх вразливими до порушень. Крім того, стрімкий розвиток кіберзагроз вимагає постійного оновлення оборонних стратегій – вимоги, яка часто перевищує інституційні можливості через бюджетні обмеження та бюрократичну інерцію [1]. Ця розбіжність між складністю загроз і готовністю до оборони становить постійний ризик для цілісності операцій правоохоронних органів.

Ще однією критичною проблемою, яка випливає з даних, є правові та юрисдикційні складнощі, пов'язані з розслідуванням транснаціональних кіберзлочинів. Транснаціональний характер багатьох кіберзлочинів ускладнює збір доказів і кримінальне переслідування, оскільки різниця в національному законодавстві часто перешкоджає співпраці. Наприклад, розбіжності в політиках зберігання даних між юрисдикціями можуть обмежувати доступ до ключових цифрових доказів. Крім того, відсутність стандартизованих протоколів для міжнародної співпраці посилює затримки у вирішенні кіберінцидентів. Тож результати свідчать, що хоча такі механізми, як договори про правову допомогу, існують, їх практична реалізація залишається неузгодженою через політичні та процедурні бар'єри. Ця фрагментація не лише підриває ефективність розслідувань, але й заохочує кіберзлочинців, які використовують юрисдикційні прогалини.

Роль штучного інтелекту (ШІ) у правоохоронній діяльності також є ключовим предметом аналізу. Інструменти на основі ШІ дедалі частіше використовуються для таких завдань, як розпізнавання обличчя, виявлення аномалій у фінансових операціях та автоматизована оцінка загроз. Хоча ці технології пропонують значні переваги з точки зору швидкості та масштабованості, їхнє впровадження супроводжується суперечками. Було висловлено занепокоєння щодо алгоритмічної упередженості – коли певні демографічні групи можуть бути непропорційно цільовими через недоліки в навчальних даних та відсутності прозорості в процесах прийняття рішень. Відмітимо те, що без суворого нагляду та механізмів відповідальності системи штучного інтелекту ризикують увіковічнити системні нерівності в рамках кримінальної юстиції. Крім того, громадська недовіра до автоматизованих інструментів поліції може підривати співпрацю з громадою, яка є необхідною для ефективного запобігання злочинності.

Людський фактор також відіграє вирішальну роль у впровадженні інформаційних ресурсів у правоохоронній діяльності. Дефіцит навчання серед співробітників часто називали як перешкоду для оптимального використання технологій. Багато працівників не мають спеціалізованих навичок у кібербезпеці чи цифровій криміналістиці, що обмежує їхню здатність ефективно реагувати на складні кіберзагрози. Ускладнює цю проблему також опір організаційним змінам.

Публічно-приватні партнерства стали перспективним напрямом для підвищення можливостей правоохоронних органів у кіберпросторі. Співпраця з технологічними компаніями забезпечує доступ до передових інструментів та експертизи, які в іншому випадку можуть бути недоступними для установ. Наприклад, партнерства з кібербезпековими компаніями сприяли обміну інформацією про загрози в режимі реального часу та спільним діям у відповідь на масштабні кібератаки. Однак такі співпраці не позбавлені викликів; питання, пов'язані з правами власності на дані, конфліктом мотивів отримання прибутку з цілями суспільних інтересів та регуляторним наглядом, залишаються нерозв'язаними [2]. Досягнення балансу між використанням інновацій приватного сектору та забезпеченням публічної відповідальності буде ключовим для підтримки цих партнерств у довгостроковій перспективі.

Наведені тут результати висвітлюють як трансформаційний потенціал, так і внутрішні ризики, пов'язані з інформаційними ресурсами у правоохоронній діяльності. Хоча технологічний прогрес надає безпрецедентні можливості для запобігання злочинам та розслідування, їхнє впровадження потребує ретельного управління для пом'якшення етичних дилем та оперативних уразливостей.

Зростаюча залежність від цифрових інформаційних ресурсів у правоохоронній діяльності спричинила значні виклики у підтриманні кібергігієни та захисті конфіденційних даних. Однією з найактуальніших проблем є вразливість баз даних правоохоронних органів до складних кібератак [2], що може підірвати операційну цілісність і довіру громадськості. Недавні дослідження свідчать, що кіберзлочинці часто націлюються на поліцейські бази даних через високу цінність інформації, яку вони містять, включаючи кримінальні записи, дані спостереження та особисті ідентифікатори. Запорукою успішного розвитку країни є безпечний кіберпростір.

Ще однією критичною проблемою є зростаюча складність методів соціальної інженерії, які використовують зловмисники для експлуатації людських слабкостей у правоохоронних органах. Наприклад, фішингові кампанії стають все більш

індивідуалізованими, імітуючи офіційні повідомлення, щоб обманом змусити персонал розкрити облікові дані або завантажити шкідливе програмне забезпечення. Такі атаки особливо небезпечні, оскільки вони обходять технічні засоби захисту, використовуючи психологічні маніпуляції.

Програми навчання, спрямовані на підвищення обізнаності щодо цих тактик, показали перспективні результати, але їх реалізація залишається нерівномірною в різних юрисдикціях. Дослідження свідчать, що організації з обов'язковим кібербезпековим навчанням фіксують менше випадків крадіжки облікових даних, що підкреслює важливість постійної освіти. Однак стрімкий розвиток методів соціальної інженерії вимагає регулярного оновлення навчальних програм для ефективного протидії новим загрозам.

Інтеграція штучного інтелекту (ШІ) у діяльність правоохоронних органів створює як можливості, так і ризики в контексті кібербезпеки. Інструменти на основі ШІ можуть покращити прогностичне полювання та аналіз даних, але також створюють нові вектори атак за відсутності належного захисту. Наприклад, методи ворожого машинного навчання використовувалися для маніпулювання системами ШІ шляхом надсилання їм оманливих даних, що призводило до помилкових слідчих висновків. Крім того, централізація систем штучного інтелекту створює єдині точки відмови, які можуть бути використані для одночасного порушення роботи кількох операцій. Таким чином, необхідно урівноважувати інновації з управлінням ризиками, встановлюючи суворі стандарти безпеки для впровадження ШІ у правоохоронній діяльності. Це включає ретельне тестування на вразливості та забезпечення прозорості алгоритмічного прийняття рішень для підтримки відповідальності.

Міжвідомча співпраця є ще однією сферою, де кібербезпека стикається зі значними викликами. Хоча обмін інформацією між правоохоронними органами є важливим для боротьби з транснаціональною злочинністю, це також підвищує ризик кіберзагроз, якщо канали зв'язку недостатньо захищені. Зашифровані платформи та системи верифікації на основі блокчейну були запропоновані як потенційні рішення для забезпечення безпеки міжвідомчого обміну. Однак розбіжності в технологічних можливостях між установами часто перешкоджають єдиному впровадженню. Наприклад, менші відділи можуть не мати ресурсів для запровадження передових інструментів шифрування, що створює слабкі ланки в загальному ланцюгу безпеки. Для усунення цих розбіжностей необхідне цільове фінансування та технічна підтримка з боку національних урядів, щоб гарантувати, що всі установи відповідають базовим стандартам кібербезпеки.

Етичні наслідки кібербезпекових заходів у правоохоронній діяльності не можна ігнорувати. Хоча технології спостереження та інструменти збору даних є життєво важливими для запобігання злочинності, їхнє неправильне використання або недостатній захист можуть порушувати громадянські свободи. Довіра громадськості до правоохоронних органів залежить від прозорості щодо того, як збираються, зберігаються та захищаються дані – принцип, який має керувати всіма ініціативами з кібербезпеки у цій сфері.

Нарешті, глобальний характер кіберзагроз вимагає міжнародної співпраці для ефективного протидіяння транснаціональній кіберзлочинності, адже кіберзагрози виступають складовою загроз у сучасному світі [3]. Дослідники зазначають, що до ефективної кібербезпеки необхідно підходити комплексно, що вимагає скоординованих дій на національному, регіональному та міжнародному рівнях [5].

Правоохоронні органи стикаються з проблемами юрисдикції при переслідуванні злочинців, які діють із інших територій. Договори про правову допомогу та спільні оперативні групи зарекомендували себе як корисні інструменти, але часто зазнають ускладнень через бюрократичні затримки та суперечливі правові стандарти. Узгодження міжнародних законів з кібербезпеки та розвиток довіри між державами залишаються вирішальними кроками як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги.

Висновки. Інтеграція інформаційних ресурсів у правоохоронну діяльність стала невід'ємною частиною вирішення сучасних викликів безпеки, особливо у сфері кібербезпеки. Швидка цифровізація критичної інфраструктури, разом із зростаючою складністю кіберзагроз, вимагає надійної системи управління та захисту інформаційних активів у поліцейській та слідчій роботі. Оскільки правоохоронні органи дедалі більше покладаються на цифрові інструменти – від криміналістичних баз даних до аналітики на основі штучного інтелекту – вразливості, притаманні цим системам, потребують ретельної уваги. Перетин кіберзагроз і злочинної діяльності створює динамічний ландшафт, у якому традиційні методи поліцейської роботи мають розвиватися, щоб протидіяти зловмисникам, які використовують технологічні досягнення для незаконних цілей.

Однією з найважливіших проблем є пошук балансу між доступністю та безпекою. Хоч вільний потік інформації підвищує оперативну ефективність, він також створює можливості для

витоку даних, несанкціонованого доступу та маніпуляцій з боку кіберзлочинців. Тож, правоохоронні органи мають запроваджувати суворі протоколи, щоб забезпечити захист конфіденційних даних без шкоди для оперативності розслідувань. Шифрування, багатофакторна автентифікація та системи постійного моніторингу мають стали невід'ємними компонентами зменшення ризиків, проте їхня ефективність залежить від регулярних оновлень і дотримання найкращих практик. Крім того, людський фактор залишається критичною вразливістю: недостатнє навчання або процедурні помилки серед персоналу можуть підірвати навіть найдосконаліші технологічні засоби захисту.

Роль інформаційних ресурсів у правоохоронній діяльності виходить далеко за межі простого впровадження технологій. Вона вимагає комплексного підходу, який поєднує реформування політики, міжнародну співпрацю, постійну освіту та передові інновації для ефективного вирішення як поточних, так і майбутніх викликів.

Література

1. Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. Criminal Justice and Behavior, 50(1), 3–25. https://doi.org/10.1177/0032258X221107584

2. Ferrante, D. J., & Holt, T. J. (2024). Assessing cyberattacks in response to police actions in physical space. Deviant Behavior. Advance online publication. https://doi.org/10.1080/01639625.2024.2429730

3. Bezzubov, D., Ihonin, R., & Diorditsa, I. (2017). Cyberthreats as a component of threats in the contemporary world (a legal aspect). Journal of Advanced Research in Law and Economics, 8(7), 2086–2093. https://doi.org/10.14505/jarle.v8.7(29).04

4. Ilchenko, M., Uryvsky, L., & Osypchuk, S. (2021). The main directions of improving information and communication technologies in the global trends. In M. Ilchenko, L. Uryvsky, & L. Globa (Eds.), Advances in information and communication technology and systems (Lecture Notes in Networks and Systems, Vol. 152, pp. 1–10). Springer. https://doi.org/10.1007/978-3-030-58359-0_1

5. Svintsytskyi, A. V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20(38), 287–305. https://doi.org/10.21830/19006586.903

6. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури. Закон України від 27 березня 2025 року № 4336-IX. https://zakon.rada.gov.ua/laws/show/4336-20#Text

7. Зміни щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, що вносяться до постанов Кабінету Міністрів України. Постанова Кабінету Міністрів України від 28.03.2025 № 447. https://zakon.rada.gov.ua/laws/show/447-2025-%D0%BF#Text

8. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 5 липня 1994 року № 80/94-ВР. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text