УДК: 351.74:005.334:004.9

https://doi.org/10.52058/2786-6300-2025-2(32)-569-584

Моргунова Тетяна Іванівна кандидат технічних наук, доцент, доцент кафедри кримінального аналізу та інформаційних технологій, Одеський державний університет внутрішніх справ, м. Одеса, https://orcid.org/0000-0002-3512-2425

УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПРАВООХОРОННИХ ОРГАНІВ

Анотація. У статті досліджено процес цифрової трансформації правоохоронних органів та її роль у підвищенні ефективності управління ризиками в умовах сучасних викликів. Розглянуто ключові технології, які сприяють цифровізації правоохоронної діяльності, зокрема штучний інтелект, великі дані, блокчейн, біометричні системи, автоматизовані бази даних та Інтернет речей. Проаналізовано, як ці технології змінюють підходи до управління безпекою, дозволяючи правоохоронним органам ефективніше здійснювати моніторинг злочинності, ідентифікувати загрози та забезпечувати оперативне реагування на надзвичайні ситуації.

Висвітлено основні ризики, пов’язані з цифровою трансформацією у сфері безпеки, включаючи кіберзагрози, потенційні витоки конфіденційної інформації, етичні дилеми та проблеми правового регулювання. Підкреслено важливість розробки комплексної стратегії управління ризиками, що передбачає зміцнення кібербезпеки, адаптацію міжнародних стандартів цифрової безпеки, а також розробку правових механізмів регулювання використання цифрових технологій у правоохоронній діяльності.

Акцентовано увагу на необхідності забезпечення балансу між технологічним прогресом та дотриманням прав людини.

Стаття містить рекомендації щодо мінімізації загроз цифрової трансформації правоохоронних органів: впровадження системи незалежного аудиту цифрових технологій, посилення державного та громадського контролю за використанням інновацій, а також розробка механізмів прозорості у використанні штучного інтелекту. Розглянуто перспективи міжнародного співробітництва у сфері кібербезпеки, стандартизації цифрових рішень та спільної розробки ефективних моделей управління цифровими ризиками.

Показано, що цифрова трансформація у правоохоронній діяльності є невідворотним процесом, який має значний потенціал для покращення рівня громадської безпеки, але водночас вимагає чітко продуманих механізмів регулювання. Тільки комплексний підхід, що поєднує технологічні, правові та

етичні аспекти, може гарантувати ефективне та безпечне впровадження цифрових рішень у сфері правопорядку.

Ключові слова: цифрова трансформація, штучний інтелект, кібербезпека, правоохоронні органи, управління ризиками, великі дані, блокчейн, автоматизовані системи, етичні аспекти, правове регулювання.

Morhunova Tetiana Ivanivna Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Criminal Analysis and Information Technologies, Odesa State University of Internal Affairs, Odesa, https://orcid.org/0000-0002-3512-2425

RISK MANAGEMENT IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF LAW ENFORCEMENT AGENCIES

Abstract. The article examines the process of digital transformation in law enforcement agencies and its role in improving risk management efficiency in the face of contemporary challenges. It explores key technologies driving the digitalization of law enforcement activities, including artificial intelligence, big data, blockchain, biometric systems, automated databases, and the Internet of Things. The study analyzes how these technologies reshape security management approaches, enabling law enforcement agencies to more effectively monitor crime, identify threats, and ensure rapid responses to emergencies.

The primary risks associated with digital transformation in the security sector are highlighted, including cyber threats, potential leaks of confidential information, ethical dilemmas, and regulatory challenges. The importance of developing a comprehensive risk management strategy is emphasized, encompassing the strengthening of cybersecurity, the adaptation of international digital security standards, and the establishment of legal frameworks for regulating the use of digital technologies in law enforcement.

Particular attention is given to the necessity of maintaining a balance between technological progress and the protection of human rights. The article provides recommendations for mitigating threats associated with the digital transformation of law enforcement agencies, such as implementing independent auditing systems for digital technologies, enhancing governmental and public oversight of innovation deployment, and developing transparency mechanisms for the use of artificial intelligence. The prospects for international cooperation in cybersecurity, the standardization of digital solutions, and the joint development of effective digital risk management models are also examined.

The study demonstrates that digital transformation in law enforcement is an irreversible process with significant potential to enhance public safety. However, it

also necessitates well-defined regulatory mechanisms. Only a comprehensive approach that integrates technological, legal, and ethical aspects can ensure the effective and secure implementation of digital solutions in the law enforcement sector.

Keywords: digital transformation, artificial intelligence, cybersecurity, law enforcement agencies, risk management, big data, blockchain, automated systems, ethical aspects, legal regulation.

Постановка проблеми. У сучасних умовах глобальної цифровізації правоохоронні органи стикаються з необхідністю адаптації до швидких технологічних змін, які впливають на всі аспекти їхньої діяльності. З одного боку, цифрова трансформація відкриває нові можливості для оперативного реагування на злочини, збору та аналізу великих обсягів даних, прогнозування загроз та покращення комунікації між державними структурами. З іншого боку, використання інноваційних технологій породжує низку викликів, пов'язаних із забезпеченням кібербезпеки, захистом персональних даних громадян, етичними дилемами застосування алгоритмів штучного інтелекту та правовими аспектами використання цифрових рішень у сфері правопорядку.

Зокрема, правоохоронні органи все частіше використовують прогнозну аналітику (Predictive Policing), що базується на аналізі історичних даних та алгоритмах машинного навчання. Однак такі методи можуть містити приховані упередження, що ставить під загрозу рівноправний підхід до громадян. Крім того, інтеграція біометричних систем і технологій розпізнавання облич викликає занепокоєння щодо масового нагляду та порушення права на приватність.

Тому постає нагальна потреба у комплексному підході до управління ризиками цифрової трансформації правоохоронної системи, який включає розробку ефективних механізмів кіберзахисту, адаптацію міжнародних стандартів цифрової безпеки, створення прозорих алгоритмів штучного інтелекту, а також гармонізацію нормативно-правового регулювання з урахуванням прав і свобод громадян.

Аналіз останніх досліджень і публікацій. Проблеми теорії та практики управління ризиками в умовах цифрової трансформації вітчизняних інституцій, зокрема правоохоронних органів розглянуто в багатьох наукових працях [1…14]. Наукова спільнота активно досліджує проблематику цифрової трансформації у сфері безпеки, зокрема її вплив на діяльність правоохоронних органів. Багато досліджень присвячено питанням застосування штучного інтелекту у сфері боротьби зі злочинністю, автоматизації поліцейських процесів та впровадженню великих даних для аналізу криміногенних загроз.

Зокрема, автори багатьох публікацій акцентують увагу на перевагах використання цифрових технологій для підвищення ефективності розслідувань, ідентифікації підозрюваних, моніторингу громадських місць та аналізу фінансо-

вих операцій, пов'язаних із відмиванням коштів та фінансуванням тероризму. Дослідження також вказують на ключові ризики цифрової трансформації, серед яких: недостатній рівень захисту персональних даних, можливість хакерських атак на державні інформаційні системи, використання технологій прогнозного аналізу без належного правового регулювання та ризики дискримінаційного профілювання осіб на основі алгоритмічних розрахунків.

Однак, попри активні наукові розвідки, залишається недостатньо дослідженим питання розробки комплексних стратегій управління ризиками цифрової трансформації правоохоронної системи. Особливої уваги потребують аспекти міжнародного співробітництва у сфері кібербезпеки, адаптації стандартів цифрового правозастосування та забезпечення прозорості використання штучного інтелекту у правоохоронних органах.

Метою статті є аналіз основних ризиків цифрової трансформації правоохоронних органів, дослідження можливих шляхів їхнього мінімізації та розробка рекомендацій для забезпечення ефективного та безпечного використання цифрових технологій у сфері безпеки.

Виклад основного матеріалу. Цифровізація правоохоронної діяльності є однією з головних тенденцій сучасного розвитку системи безпеки, що змінює підходи до забезпечення правопорядку, розслідування злочинів і профілактики правопорушень.

Сучасний розвиток цифрових технологій впливає на всі аспекти суспільного життя, зокрема й на боротьбу зі злочинністю. Традиційні підходи правоохоронних органів поступово стають менш ефективними, адже злочинці активно використовують новітні технології для організації та приховування своєї діяльності. Це змушує правоохоронні структури впроваджувати цифрові рішення, адаптуючи свої методи роботи до нових реалій.

Використання сучасних цифрових технологій дозволяє значно покращити ефективність роботи правоохоронних органів. Зокрема, впровадження аналітичних систем на основі штучного інтелекту, аналіз великих обсягів даних, автоматизований моніторинг та вдосконалене відеоспостереження сприяють оперативнішому розслідуванню правопорушень і мінімізують вплив людського фактора. Водночас цифровізація породжує низку нових викликів, серед яких питання кібербезпеки, ризики витоку конфіденційної інформації та необхідність правового регулювання застосування інноваційних технологій.

Процес впровадження цифрових інструментів у сферу правоохоронної діяльності є складним і комплексним. Він охоплює не лише інтеграцію новітніх технологій, а й зміну методології аналізу кримінальних даних, прогнозування загроз, модернізацію систем відеоспостереження та створення міжнародних цифрових платформ для координації правоохоронних органів. Важливим залишається питання дотримання прав і свобод громадян під час використання

цифрових рішень, що вимагає чіткої регламентації та збалансованого підходу до правового регулювання.

Основними технологіями цифровізації у правоохоронній сфері є:

1. Штучний інтелект (укр. ШІ, англ. AI) – використовується для аналізу величезних масивів інформації, автоматизації процесу оцінки доказів, розпізнавання осіб та прогнозування потенційних злочинів.
2. Великі дані (Big Data) – дозволяють ефективно обробляти й аналізувати кримінальну статистику, визначати закономірності злочинної активності та оптимізувати стратегії боротьби з правопорушеннями.
3. Блокчейн – застосовується для захисту кримінальних доказів та реєстрації транзакцій, що унеможливлює підробку або несанкціоноване редагування даних.
4. Біометричні системи – забезпечують швидку ідентифікацію осіб на основі відбитків пальців, голосу, структури обличчя чи сітківки ока, що значно підвищує ефективність оперативних заходів.
5. Автоматизовані бази даних – дозволяють швидко обмінюватися інформацією між правоохоронними органами різних рівнів, підвищуючи оперативність реагування на загрози.
6. Інтернет речей (IoT) – інтегрується у системи розумного моніторингу міського простору, що дозволяє в режимі реального часу фіксувати порушення та забезпечувати безпеку громадян.

Впровадження цих технологій змінює формат роботи правоохоронних структур, підвищує їхню ефективність та сприяє запобіганню злочинам ще до їхнього вчинення.

У сучасних умовах правоохоронні органи активно використовують новітні технології для забезпечення безпеки та боротьби зі злочинністю. Одним із ключових напрямів є впровадження автоматизованих аналітичних систем, що допомагають прискорювати процеси розслідування, моніторингу та оцінки ризиків.

Серед найбільш поширених цифрових рішень можна виділити:

– автоматизацію оперативно-розшукових заходів. Використання штучного інтелекту для обробки великої кількості кримінальних даних, відстеження цифрових слідів та формування профілів потенційних злочинців;

– аналітику великих даних у боротьбі зі злочинністю. Використання алгоритмів для виявлення нелегальних фінансових схем, кіберзлочинності та ідентифікації злочинних угруповань;

– прогнозне поліцейське управління (Predictive Policing). Застосування алгоритмів прогнозного аналізу для визначення потенційних місць та часу вчинення злочинів, що дозволяє правоохоронцям діяти на випередження;

– цифрові системи відеоспостереження та розпізнавання облич. Використання інтелектуальних камер, які ідентифікують осіб у натовпі та передають інформацію в оперативні центри.

– штучний інтелект у правоохоронній діяльності. Використання чат-ботів для збору інформації, аналізу свідчень і автоматизації процесу взаємодії між громадянами та поліцією.

Застосування цих технологій дозволяє значно скоротити час розслідування, підвищити точність ухвалення рішень та мінімізувати можливі помилки, пов'язані з людським фактором.

Запровадження цифрових технологій у правоохоронну діяльність дає змогу суттєво підвищити ефективність роботи, забезпечити швидке реагування на загрози та покращити координацію між різними структурами безпеки.

До ключових переваг цифрової трансформації належать:

– підвищення швидкості розслідувань та аналізу доказів. Використання автоматизованих систем дозволяє оперативно обробляти велику кількість відеозаписів, текстових документів та цифрових слідів;

– оптимізація використання людських ресурсів. Автоматизація рутинних процесів звільняє правоохоронців від виконання технічних завдань, дозволяючи їм зосередитися на аналітичній роботі та стратегічному плануванні;

– зниження корупційних ризиків. Використання блокчейн-технологій та автоматизованих алгоритмів у фінансових та адміністративних процесах мінімізує можливість маніпуляцій та зловживань;

– посилення міжнародного співробітництва у боротьбі зі злочинністю. Використання цифрових платформ для обміну даними між правоохоронними органами різних країн дозволяє швидко реагувати на міжнародні загрози та злочинні мережі.

Цифрова трансформація правоохоронних органів сприяє підвищенню ефективності їхньої роботи, безпеки громадян і правопорядку. Проте її успіх залежить від комплексного підходу: правового регулювання, підготовки кадрів, кібербезпеки та етичного використання технологій.

Використання цифрових технологій, таких як штучний інтелект, аналітичні платформи, великі дані та блокчейн, покращує розслідування та запобігання злочинам. Однак цифровізація створює ризики – загрози кібербезпеці, порушення конфіденційності, алгоритмічні упередження. Дані правоохоронців можуть стати об'єктом атак, а технології прогнозування злочинів – маніпуляцій.

Особливо небезпечним є злом баз даних, що містять інформацію про розслідування, докази й підозрюваних. Викрадені дані можуть використовуватися для підробок, шантажу або спотворення слідства. Штучний інтелект також має вразливості – хакери можуть маніпулювати алгоритмами, спрямовуючи увагу правоохоронців у хибному напрямку.

Для безпечної цифровізації необхідно розвивати правові механізми, засоби кіберзахисту, громадський контроль та міжнародну співпрацю. Лише комплексний підхід дозволить реалізувати переваги цифрової трансформації без шкоди для безпеки та прав громадян.

Цифрова трансформація стає ключовим елементом діяльності правоохоронних органів, сприяючи покращенню ефективності розслідувань, запобіганню злочинам і швидкому реагуванню на загрози. Вона передбачає широке використання цифрових технологій, зокрема штучного інтелекту, аналітичних платформ, великих даних, блокчейн-систем та біометричних рішень. Проте, поряд із перевагами, цифровізація створює низку викликів, пов'язаних із захистом даних, правовими аспектами та етичними питаннями застосування технологій у правоохоронній діяльності.

Додатково варто враховувати, що самі злочинці активно використовують цифрові технології для ухилення від відповідальності. Шифрування комунікацій, анонімні мережі DarkNet, криптовалюти, deepfake-технології та інші засоби дозволяють злочинним угрупованням приховувати свою діяльність та ускладнюють їхнє переслідування правоохоронцями.

Таким чином, кібербезпека повинна стати пріоритетом у цифровій трансформації правоохоронних органів. Це передбачає впровадження сучасних систем шифрування даних, регулярний моніторинг кіберзагроз, багаторівневий захист баз даних і розвиток спеціалізованих підрозділів з кібербезпеки.

Один із найважливіших викликів цифрової трансформації правоохоронної сфери – забезпечення надійного захисту конфіденційної інформації. Оскільки правоохоронні органи обробляють великі обсяги персональних даних громадян, необхідно гарантувати, що вони не будуть використані зловмисниками чи потраплять у відкритий доступ.

Загроза витоку інформації може виникати як через зовнішні атаки, так і через внутрішні недоліки в управлінні даними. Недостатньо захищені сервери, слабкі паролі, відсутність системи моніторингу доступу – усе це створює передумови для витоку чутливих даних.

Окремою проблемою є використання технологій стеження без належного контролю. Системи розпізнавання облич, GPS-трекери, інтернет речей та біометричні дані можуть бути використані не лише для боротьби зі злочинністю, а й для незаконного стеження за громадянами, журналістами чи політичними опонентами.

Щоб мінімізувати ці ризики, необхідно впроваджувати жорсткі заходи контролю за доступом до даних, встановлювати незалежні механізми аудиту цифрових систем, а також розробляти міжнародні стандарти захисту персональних даних у правоохоронній сфері.

Цифровізація правоохоронних органів ставить перед суспільством не лише технічні, а й серйозні етичні та правові питання. Використання штучного інтелекту, великих даних та автоматизованих рішень може покращити боротьбу зі злочинністю, але водночас потребує чітких меж правового регулювання.

У сучасних умовах кіберзагрози залишаються однією з найбільших небезпек для цифрових правоохоронних систем. Кількість атак на урядові сервери, бази даних та інформаційні системи правоохоронних органів щороку зростає, що вимагає підвищеної уваги до питань інформаційної безпеки та ефективного впровадження засобів кіберзахисту.

Один із головних викликів – відсутність єдиних міжнародних стандартів щодо використання цифрових технологій у правоохоронних органах. Наприклад, у деяких країнах уже активно використовуються системи Predictive Policing, що передбачають прогнозування ймовірних місць скоєння злочинів. Проте дослідження показують, що такі алгоритми можуть бути упередженими, оскільки ґрунтуються на історичних даних, що містять соціальні або етнічні диспропорції.

Іншою серйозною проблемою є масове використання систем розпізнавання облич без згоди громадян. У багатьох містах світу вже діють подібні системи, проте правозахисники висловлюють занепокоєння щодо можливого зловживання цими технологіями, що може призвести до незаконного стеження та порушення права на приватність.

Важливо також враховувати ризики автоматизованого ухвалення рішень. Якщо алгоритми штучного інтелекту будуть застосовуватися без належного людського контролю, це може призвести до помилкових звинувачень, дискримінації або навіть до переслідувань невинних осіб.

Таким чином, цифрова трансформація повинна супроводжуватися розробкою чітких правових норм, що регулюватимуть використання цифрових технологій у правоохоронній діяльності. Впровадження міжнародних стандартів, етичних кодексів та незалежного контролю допоможе забезпечити баланс між ефективністю цифрових технологій і дотриманням прав людини.

Цифрова трансформація правоохоронних органів є необхідним кроком для підвищення ефективності правозастосування, однак вона супроводжується серйозними викликами. Кібербезпека, захист персональних даних, правові та етичні аспекти впровадження цифрових технологій потребують ретельного регулювання.

Для зменшення ризиків необхідно розробити комплексні заходи захисту цифрових систем, впроваджувати міжнародні стандарти та посилювати громадський контроль. Лише в умовах прозорості та підзвітності цифровізація правоохоронних органів може стати ефективним інструментом у боротьбі зі злочинністю без загрози для прав і свобод громадян.

Швидке впровадження цифрових технологій у правоохоронну діяльність створює не лише нові можливості для забезпечення громадської безпеки, але й викликає численні ризики, пов'язані з кіберзагрозами, витоком даних, дискримінацією та етичними викликами. Ці виклики вимагають комплексного підходу до управління ризиками, оскільки технологічний прогрес супроводжується зростанням нових загроз, які потребують ретельного аналізу та ефективних контрзаходів.

Один із ключових аспектів управління ризиками – це забезпечення балансу між інноваціями та правами громадян [15]. Використання штучного інтелекту, великих даних та автоматизованих систем повинно бути регламентоване на законодавчому рівні, аби уникнути потенційних загроз, таких як зловживання технологіями або надмірне втручання у приватне життя.

При цьому важливо враховувати, що боротьба з цифровими загрозами є не лише внутрішньою проблемою окремої країни, а й глобальним викликом, який вимагає міжнародного співробітництва та обміну досвідом між правоохоронними органами різних держав.

Однією з найсерйозніших загроз цифровізації є кіберзлочинність, яка постійно еволюціонує, стаючи дедалі складнішою та небезпечнішою. Для ефективного захисту цифрових систем правоохоронних органів необхідно впроваджувати передові методи кібербезпеки, які дозволять не лише запобігати атакам, але й своєчасно виявляти та нейтралізувати потенційні загрози.

Серед найбільш перспективних підходів – використання технологій штучного інтелекту для кіберзахисту. Алгоритми машинного навчання здатні аналізувати великі обсяги трафіку, виявляти аномалії та реагувати на підозрілі дії в реальному часі. Наприклад, системи раннього попередження можуть автоматично блокувати шкідливі спроби входу до баз даних або відслідковувати підозрілі з'єднання.

Захист правоохоронних баз даних від кібератак є одним із ключових завдань сучасної безпеки. Витік або компрометація інформації може спричинити серйозні правові та безпекові ризики. Саме тому важливо впроваджувати передові технології шифрування, застосовувати багаторівневу аутентифікацію, контролювати доступ до конфіденційних даних і здійснювати постійний моніторинг інформаційних систем.

Дотримання міжнародних стандартів кібербезпеки сприяє зміцненню захисту цифрових ресурсів і полегшує міжнародну співпрацю у сфері протидії кіберзлочинності. Використання напрацьованих методик таких організацій, як Європол, Інтерпол та ENISA, допомагає уніфікувати підходи до захисту правоохоронних систем і підвищує їхню стійкість до загроз.

Оцифрування правоохоронної діяльності вимагає чіткого правового регулювання, яке визначатиме межі застосування цифрових технологій та

запобігатиме можливим зловживанням. Якщо не встановити належний контроль над використанням штучного інтелекту, Predictive Policing та інших інноваційних рішень, це може створити ризики для прав і свобод громадян.

Пріоритетним напрямком державної політики має стати розробка нормативно-правових актів щодо застосування штучного інтелекту та аналітики великих даних у правоохоронній сфері. Законодавчі норми повинні чітко регулювати процеси збору, збереження та обробки інформації, забезпечувати прозорість цих дій і передбачати відповідальність за неправомірне використання цифрових технологій.

Також необхідно впровадити механізми контролю за використанням цифрових технологій. Зокрема, важливим інструментом є незалежний аудит алгоритмів, які використовуються у правоохоронній діяльності, а також створення комісій, які здійснюватимуть моніторинг їхнього застосування.

Громадський нагляд та аудит цифрових систем безпеки сприятимуть підвищенню довіри до цифрової трансформації. Участь незалежних правозахисних організацій у перевірці цифрових правоохоронних рішень забезпечить об’єктивну оцінку їхньої ефективності та відповідності стандартам захисту прав людини.

Окрім технічних і правових аспектів, важливою складовою управління ризиками є вирішення етичних питань, пов’язаних із використанням штучного інтелекту та аналітичних алгоритмів у правоохоронній діяльності.

Штучний інтелект, який використовується у Predictive Policing, може містити приховані упередження, що призводить до дискримінації певних соціальних груп. Тому необхідно розробити етичні кодекси застосування ШІ у правоохоронній діяльності, які регламентуватимуть відповідальність за ухвалення автоматизованих рішень та гарантуватимуть дотримання прав людини.

Механізми прозорості у Predictive Policing повинні передбачати відкритість алгоритмів для незалежного аудиту. Це дозволить уникнути ситуацій, коли цифрові системи приймають рішення на основі упереджених даних або необґрунтовано спрямовують правоохоронні ресурси на певні категорії населення.

Важливо також забезпечити належну підготовку правоохоронців щодо етичного використання сучасних цифрових технологій. Поліцейські та слідчі повинні розуміти принципи функціонування штучного інтелекту, щоб приймати виважені рішення та уникати помилок, які можуть вплинути на об'єктивність їхньої роботи.

Розвиток цифрових технологій у правоохоронній сфері неможливий без міжнародної співпраці, оскільки кіберзлочинність не знає державних кордонів. Об'єднання зусиль на міжнародному рівні сприяє ефективнішій протидії цифровим загрозам та формуванню уніфікованих стандартів безпеки.

Спільні ініціативи у сфері кібербезпеки між правоохоронними структурами різних країн допоможуть швидше виявляти та нейтралізувати глобальні загрози. Наприклад, міжнародні центри аналітики, які застосовують алгоритми штучного інтелекту для моніторингу кіберзлочинності, здатні ідентифікувати потенційні загрози ще на ранніх стадіях їхнього розвитку.

Запровадження єдиних стандартів цифрового правозастосування значно спростить координацію між державами та сприятиме оперативному обміну важливою інформацією.

Досвід міжнародного співробітництва у сфері цифрового правосуддя дозволить впроваджувати ефективні практики боротьби з кіберзлочинністю та адаптувати сучасні технології до специфіки кожної країни.

Забезпечення ефективного управління ризиками, пов'язаними з цифровою трансформацією правоохоронної системи, є одним із ключових аспектів її успішної модернізації. Це вимагає комплексного підходу, що включає зміцнення заходів кібербезпеки, створення належного правового регулювання, запобігання дискримінації та розширення міжнародного співробітництва.

Лише комплексний підхід, що поєднує технічні, правові та етичні аспекти, дозволить ефективно використовувати цифрові інструменти, забезпечуючи при цьому захист основних прав людини та суспільної безпеки.

Цифрова трансформація правоохоронних органів кардинально змінює методи забезпечення правопорядку, відкриваючи нові можливості для аналізу великих масивів даних, підвищення оперативної ефективності та боротьби зі злочинністю. Проте, поряд із цими перевагами, виникають нові виклики, пов’язані з кіберзагрозами, правовими колізіями, порушенням конфіденційності та можливістю зловживань технологічними засобами. У таких умовах стратегічне управління цифровими ризиками стає необхідним елементом успішної цифровізації правоохоронних структур.

Інтеграція передових технологій у боротьбу з кіберзлочинністю має супроводжуватися розробкою ефективних правових механізмів регулювання та систем захисту персональних даних. Без належного законодавчого врегулювання та міжнародної співпраці навіть найпрогресивніші технології можуть стати інструментом зловживань або порушення прав людини. Тому питання безпечного використання цифрових інструментів у глобальній системі безпеки є ключовим аспектом сучасного правозастосування.

Забезпечення інформаційної безпеки та протидія кіберзагрозам мають стати пріоритетними напрямами цифрової трансформації правоохоронних органів. Зі зростанням рівня цифрової злочинності виникає необхідність у впровадженні інноваційних рішень, які допоможуть ефективно нейтралізувати загрози та захистити критично важливі дані.

Одним із найбільш перспективних підходів є використання блокчейн-технологій для захисту баз даних. Завдяки своїй децентралізованій структурі блокчейн забезпечує неможливість несанкціонованого доступу, зміни чи видалення інформації, що робить його ефективним інструментом для зберігання доказової бази, інформації про підозрюваних та інших важливих матеріалів. Це дозволяє мінімізувати ризик фальсифікацій і підвищити прозорість у правозастосуванні.

Також перспективним напрямом є розробка автоматизованих алгоритмів для виявлення підозрілої поведінки. Штучний інтелект у системах відеоспостереження, кримінальній аналітиці та моніторингу може виявляти потенційні загрози ще до їхнього переростання у реальні злочини. Наприклад, алгоритми аналізу поведінкових моделей здатні визначати аномальні дії, що можуть свідчити про небезпеку.

Ще одним важливим вектором є інтеграція технологій Інтернету речей (IoT) у правоохоронну діяльність. Використання мережі розумних пристроїв, сенсорів і камер дозволяє створити ефективну систему моніторингу в реальному часі. Це дає змогу не лише виявляти, а й запобігати злочинам на ранніх етапах. Наприклад, сучасні камери спостереження можуть автоматично аналізувати підозрілі ситуації та передавати дані до аналітичних центрів.

Попри значний потенціал цих технологій, їхнє ефективне впровадження потребує розробки відповідного правового регулювання. Створення чітких законодавчих норм щодо використання штучного інтелекту, автоматизованого аналізу та цифрових баз даних допоможе уникнути ризиків зловживання та забезпечить баланс між безпекою і дотриманням прав людини.

Цифровізація правоохоронної діяльності не може відбуватися без належного правового регулювання. Відсутність чітких законодавчих норм може призвести до зловживань, неправомірного застосування технологій або порушення прав людини. Саме тому одним із головних напрямів подальшого розвитку має стати вдосконалення законодавства про штучний інтелект у сфері безпеки**.**

Розробка нормативно-правових актів, які чітко регулюють використання ШІ у правоохоронних органах, дозволить уникнути правових колізій, що можуть виникати при автоматичному ухваленні рішень. Наприклад, алгоритми прогнозного аналізу злочинності мають бути прозорими, щоб уникнути можливих дискримінаційних упереджень.

Ще одним важливим напрямом є співпраця міжнародних організацій у розробці цифрових стандартів. Координація між державами у сфері цифрової безпеки сприятиме уніфікації підходів до використання технологій у правоохоронній діяльності. Єдині міжнародні стандарти щодо застосування цифрових технологій у сфері правопорядку дозволять запобігти ситуаціям, коли одна країна використовує недопустимі методи цифрового стеження чи аналізу.

Окрему увагу слід приділити захисту персональних даних у правоохоронних системах. Використання технологій розпізнавання облич, біометричних систем та великих даних повинно супроводжуватися строгими заходами безпеки, щоб запобігти несанкціонованому доступу та використанню конфіденційної інформації.

Штучний інтелект відкриває нові можливості у боротьбі з міжнародною злочинністю, тероризмом та кіберзагрозами. Завдяки здатності швидко аналізувати великі масиви даних та виявляти приховані закономірності, він може суттєво покращити міжнародну співпрацю у сфері безпеки.

Фундаментальні технології ШІ покликані сприяти трансформації економіки, ринку праці, державних інституцій та суспільства в цілому [16].

Одним із ключових напрямів є розширення міжнародного моніторингу кримінальних загроз. Впровадження глобальних платформ для обміну аналітичною інформацією дозволить правоохоронним органам різних країн краще координувати свої дії та ефективніше протидіяти організованій злочинності.

Окрім цього, цифрові технології можуть бути дієвим інструментом у боротьбі з такими загрозами, як тероризм та фінансова злочинність. Автоматизовані системи моніторингу фінансових потоків здатні виявляти підозрілі операції, що можуть свідчити про відмивання коштів або незаконне фінансування.

Водночас важливо дотримуватися балансу між технологічним прогресом і захистом прав людини. Використання сучасних цифрових рішень не повинно призводити до надмірного контролю над громадянами або порушення демократичних принципів.

Оцифрування правоохоронної діяльності відкриває широкі можливості для підвищення рівня безпеки, проте потребує ретельного управління ризиками. Серед основних пріоритетів – розробка інноваційних технологій, створення чіткої правової бази та посилення міжнародної координації у сфері цифрового правозастосування.

Впровадження блокчейн-рішень, штучного інтелекту та Інтернету речей у діяльність правоохоронних органів може значно підвищити ефективність їхньої роботи. Проте водночас необхідно забезпечити надійний захист персональних даних, контроль за використанням прогнозної аналітики та розробку єдиних міжнародних стандартів безпеки.

Створення ефективної та безпечної цифрової екосистеми для правоохоронних органів майбутнього можливе лише за умови комплексного підходу, що поєднує технологічні інновації, правове регулювання та міжнародну співпрацю.

Висновки. Цифрова трансформація правоохоронних органів є ключовим елементом сучасної безпеки, що змінює методи боротьби зі злочинністю та громадського порядку. Використання штучного інтелекту, аналітики даних,

блокчейн-технологій і біометричних систем підвищує ефективність роботи, але водночас створює ризики, пов'язані з кібербезпекою, захистом даних, правовими та етичними викликами.

Основні загрози цифровізації включають необхідність посилення кіберзахисту, запобігання витоку персональних даних та регулювання штучного інтелекту. Кіберзлочинці також використовують цифрові технології для ухилення від відповідальності, що вимагає нових стратегій боротьби. Алгоритмічні упередження у ШІ можуть призводити до дискримінації.

Ефективне управління цифровими ризиками потребує комплексного підходу: сучасних систем кібербезпеки, правового регулювання, громадського контролю та міжнародної співпраці. Важливими є алгоритми раннього виявлення загроз, прозорість технологій та етичні кодекси для роботи зі ШІ.

Подальший розвиток цифровізації включає інтеграцію блокчейну для захисту баз даних, Інтернету речей для моніторингу та автоматизованих систем виявлення загроз. Водночас необхідно вдосконалювати законодавство, міжнародну співпрацю та єдині стандарти цифрової безпеки.

Цифрова трансформація значно підвищує ефективність правоохоронних органів, але її реалізація має збалансовувати технологічний прогрес із захистом прав громадян. Лише комплексний підхід дозволить створити безпечну цифрову екосистему для правоохоронної діяльності.

***Література*:**

1.Гуржій С.В. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки. *Інформація і право.* 2023. № 4 (47). С. 207-216.

2.Данченко О.Б., Занора В.О. Проєктний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень. Черкаси: ПП Чабаненко Ю. А., 2019. 278 с.

3.Зварич Р., Дудник Ю., Гомотюк В., Боднар С. Ризик-менеджмент цифрової трансформації в умовах пандемії. *Науковий вісник Західноукраїнського національного університету.* 2023. № 4 (87). С. 56-72.

4.Корчак Н., Рачинський А., Ларіна Н. Цифрова трансформація та електронне врядування: наукові підходи дослідження в сфері публічного управління та адміністрування. *Аспекти публічного управління. Науковий журнал.* 2023. Т. 11, № 3. С. 43-49.

5.Луценко В.Р., Пікуля Т.О. Правове забезпечення цифрової трансформації в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 1, № 81. С. 61-67.

6.Малашко О.Є., Ковалів М.В. Теоретична конструкція поняття «інформаційна безпека». *Інтернаука. Серія: «Юридичні науки».* 2020. № 10. С. 20-33.

7.Онопрієнко С. Класифікація видів інформаційної безпеки як правової категорії. *Вісник Київського національного університету імені Тараса Шевченка. Серія: «Військово-спеціальні науки».* 2022. № 1 (49). С. 60-62.

8.Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2021. № 3 (31). С. 167-179.

9. Перевозова І.В., Шайбан В.М., Деделюк О.В. До питання ролі ризик-менеджменту в цифровій трансформації промислового підприємства: сутність та інноваційний потенціал. *Науковий журнал "Науковий збірник Луцького національного технічного університету".* 2023. № 2 (58). С. 120-135.

10. Пустоваров А.І. Інституційне забезпечення процесу цифрової трансформації управління розвитком національної економіки. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство.* 2019. Вип. 24, ч. 1. С. 164-169.

11. Сидоренко В.В. Вплив розвитку правового регулювання цифрової трансформації на економіку в Україні. *Юридичний науковий електронний журнал.* 2024. № 1. С. 214-217.

12. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2024. № 1 (41). С. 314-320.

13. Шопіна І.М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2023. № 1. С. 28-35.

14. Храпенко О.О., Меденцев А.М., Сперанський В.О. Цифровізація правоохоронної діяльності: використання штучного інтелекту для боротьби з кіберзлочинністю. *Юридичний науковий електронний журнал.* 2024. № 11. С. 505-508.

15. Інноваційна економіка: теоретичні та практичні аспекти: монографія / за ред. д.е.н., доц. Є.І. Масленнікова. Херсон: Грінь Д.С., 2016. 854 с.

16. Чукурна О.П., Тардаскіна Т.М. Менеджмент в цифровій економіці: навч. посіб. Одеса: Астропринт, 2024. 376 с.

References:

1.Hurzhii, S.V. (2023). Osoblyvosti vykorystannia shtuchnoho intelektu u pytanniakh zabezpechennia kiberbezpeky [Features of using artificial intelligence in cybersecurity]. Informatsiia i pravo – Information and Law, 4(47), 207-216. [in Ukrainian].

2.Danchenko, O.B., & Zanora, V.O. (2019). Proiektnyi menedzhment: upravlinnia ryzykamy ta zminamy v protsesakh pryiniattia upravlinskykh rishen [Project management: risk and change management in decision-making processes]. Cherkasy: PP Chabanenko Yu. A. [in Ukrainian].

3.Zvarych, R., Dudnyk, Yu., Homotiuk, V., & Bodnar, S. (2023). Ryzyk-menedzhment tsyfrovoi transformatsii v umovakh pandemii [Risk management of digital transformation in pandemic conditions]. Naukovyi visnyk Zakhidnoukrainskoho natsionalnoho universytetu – Scientific Bulletin of Western Ukrainian National University, 4(87), 56-72. [in Ukrainian].

4.Korchak, N., Rachynskyi, A., & Larina, N. (2023). Tsyfrova transformatsiia ta elektronne vriaduvannia: naukovi pidkhody doslidzhennia v sferi publichnoho upravlinnia ta administruvannia [Digital transformation and e-governance: scientific approaches in public administration and management]. Aspekty publichnoho upravlinnia – Aspects of Public Administration, 11(3), 43-49. [in Ukrainian].

5.Lutsenko, V.R., & Pikulia, T.O. (2024). Pravove zabezpechennia tsyfrovoi transformatsii v Ukraini [Legal support of digital transformation in Ukraine]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law, 1(81), 61-67. [in Ukrainian].

6.Malashko, O.Ye., & Kovaliv, M.V. (2020). Teoretychna konstruktsiia poniattia "informatsiina bezpeka" [Theoretical construction of the concept "information security"]. Internauka. Seriia: Yurydychni nauky – Internauka. Series: Legal Sciences, 10, 20-33. [in Ukrainian].

7.Onopriienko, S. (2022). Klasyfikatsiia vydiv informatsiinoi bezpeky yak pravovoi katehorii [Classification of types of information security as a legal category]. Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Seriia: Viiskovo-spetsialni nauky – Bulletin of Taras Shevchenko National University of Kyiv. Series: Military-Special Sciences, 1(49), 60-62. [in Ukrainian].

8.Ostapenko, O., & Baik, O. (2021). Administratyvno-pravova pryroda informatsiinoi bezpeky [Administrative and legal nature of information security]. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Yurydychni nauky – Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 3(31), 167-179. [in Ukrainian].

9.Perevozova, I.V., Shaiban, V.M., & Dedeliuk, O.V. (2023). Do pytannia roli ryzyk-menedzhmentu v tsyfrovoi transformatsii promyslovoho pidpryiemstva: sutnist ta innovatsiinyi potentsial [On the role of risk management in digital transformation of an industrial enterprise: essence and innovative potential]. Naukovyi zbirnyk Lutskogo natsionalnogo tekhnichnogo universytetu – Scientific Collection of Lutsk National Technical University, 2(58), 120-135. [in Ukrainian].

10. Pustovarov, A.I. (2019). Instytutsiine zabezpechennia protsesu tsyfrovoi transformatsii upravlinnia rozvytkom natsionalnoi ekonomiky [Institutional support for the process of digital transformation in managing the development of the national economy]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo – Scientific Bulletin of Uzhhorod National University. Series: International Economic Relations and World Economy, 24(1), 164-169. [in Ukrainian].

11. Sydorenko, V.V. (2024). Vplyv rozvytku pravovoho rehuliuvannia tsyfrovoi transformatsii na ekonomiku v Ukraini [Impact of legal regulation of digital transformation on the economy in Ukraine]. Yurydychnyi naukovyi elektronnyi zhurnal – Legal Scientific Electronic Journal, 1, 214-217. [in Ukrainian].

12. Syrovatchenko, M. (2024). Pravovi aspekty zabezpechennia kiberbezpeky v Ukraini: suchasni vyklyky ta rol natsionalnoho zakonodavstva [Legal aspects of cybersecurity in Ukraine: current challenges and the role of national legislation]. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Yurydychni nauky – Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 1(41), 314-320. [in Ukrainian].

13. Shopina, I.M. (2023). Informatsiina bezpeka tsyfrovoi transformatsii [Information security of digital transformation]. Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia: Yurydychna – Scientific Bulletin of Lviv State University of Internal Affairs. Series: Legal, 1, 28-35. [in Ukrainian].

14. Khrapenko, O.O., Medentsev, A.M., & Speranskyi, V.O. (2024). Tsyfrovyzatsiia pravookhoronnoi diialnosti: vykorystannia shtuchnoho intelektu dlia borotby z kiberzlochynnistiu [Digitalization of law enforcement: using artificial intelligence to combat cybercrime]. Yurydychnyi naukovyi elektronnyi zhurnal – Legal Scientific Electronic Journal, 11, 505-508. [in Ukrainian].

15. Maslennikov, Ye.I. (Ed.). (2016). Innovatsiina ekonomika: teoretychni ta praktychni aspekty: monohrafiia [Innovative economy: theoretical and practical aspects: monograph]. Kherson: Hrin D.S. [in Ukrainian].

16. Chukurna, O.P., & Tardaskina, T.M. (2024). Menedzhment v tsyfrovi ekonomitsi [Management in the digital economy]. Odesa: Astroprynt. [in Ukrainian].