УДК 343.9:004.8
DOI https://doi.org/10.32782/2524-0374/2024-11/117

ЦИФРОВІЗАЦІЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

DIGITALIZATION OF LAW ENFORCEMENT ACTIVITIES: USE OF ARTIFICIAL INTELLIGENCE TO FIGHT CYBERCRIME

Храпенко О.О., к.ю.н.,
доцент кафедри організації судових, правоохоронних органів та адвокатури
Національний університет «Одеська юридична академія»

Меденцев А.М., к.ю.н.,
доцент кафедри кримінального права, процесу та криміналістики
Міжнародний гуманітарний університет

Сперанський В.О., к.т.н.,
доцент кафедри комп'ютеризованих систем та програмних технологій
Національний університет «Одеська політехніка»

Статтю присвячено висвітленню актуальної проблеми впровадження новітніх технологій у правоохоронну діяльність, які мають значний потенціал для прискорення обробки даних та підвищення ефективності роботи правоохоронних органів.

У статті розглянуто питання цифровізації правоохоронної діяльності як ключового елементу сучасної боротьби з кіберзлочинністю. Особливу увагу приділено використанню технологій штучного інтелекту для аналізу даних, виявлення кіберзагроз, прогнозування злочинної активності та автоматизації правоохоронних процесів.

Досліджено роль цифровізації у трансформації правоохоронної діяльності в умовах стрімкого розвитку інформаційних технологій. Основний акцент зроблено на інтеграції систем штучного інтелекту в процеси забезпечення кібербезпеки, аналізі великих обсягів даних та автоматизації оперативних і слідчих дій. Проаналізовано ключові технологічні інструменти: алгоритми машинного навчання для розпізнавання шаблонів злочинної поведінки, засоби виявлення аномалій у кіберпросторі, системи моніторингу соціальних мереж і «темного вебу», платформи прогнозної аналітики.

Розглянуто сучасні підходи до інтеграції штучного інтелекту у практику забезпечення кібербезпеки, зокрема розпізнавання аномальної поведінки в мережі, моніторинг «темних» веб-ресурсів та використання систем машинного навчання для підвищення оперативної ефективності. Висвітлено основні переваги та ризики впровадження таких технологій, включаючи етичні, правові та технічні аспекти.

Проаналізовано практичні кейси застосування штучного інтелекту для протидії різним типам кіберзлочинів: фінансовим шахрайствам, крадіжці даних, атакам на критичну інфраструктуру та поширенню шкідливого програмного забезпечення. Розглянуто правові, етичні та технічні виклики впровадження таких технологій, зокрема питання приватності, прозорості алгоритмів і ризиків автоматизації прийняття рішень.

У статті наголошується, що цифровізація правоохоронної діяльності є не лише інструментом підвищення ефективності, а й необхідною умовою адаптації правоохоронних органів до нових викликів цифрової епохи.

Ключові слова: правоохоронні органи, правоохоронна діяльність, цифровізація, штучний інтелект, кіберзлочинність, кібербезпека, кіберзагрози, міжвідомча співпраця.

The article is devoted to the topical problem of introducing the latest technologies in law enforcement, which have a significant potential for accelerating data processing and improving the efficiency of law enforcement agencies.

The article discusses the issues of digitalization of law enforcement as a key element of the modern fight against cybercrime. Particular attention is paid to the use of artificial intelligence technologies for data analysis, identifying cyber threats, predicting criminal activity and automating law enforcement processes.

The role of digitalization in the transformation of law enforcement in the context of the rapid development of information technologies is investigated. The main emphasis is on the integration of artificial intelligence systems into cybersecurity processes, the analysis of large amounts of data and the automation of operational and investigative actions.

Key technological tools are analyzed: machine learning algorithms for recognizing patterns of criminal behavior, tools for detecting anomalies in cyberspace, monitoring systems for social networks and the dark web, and predictive analytics platforms.

Modern approaches to the integration of artificial intelligence into the practice of cybersecurity are considered, in particular, the recognition of anomalous behavior in the network, monitoring of dark web resources and the use of machine learning systems to improve operational efficiency. The main advantages and risks of implementing such technologies, including ethical, legal and technical aspects, are highlighted.

Practical cases of using artificial intelligence to counter various types of cybercrime are analyzed: financial fraud, data theft, attacks on critical infrastructure, and the spread of malicious software. The legal, ethical and technical challenges of the introduction of such technologies are considered, in particular, the issues of privacy, transparency of algorithms and risks of automating decision-making.

The article notes that the digitalization of law enforcement is not only a tool for increasing efficiency, but also a necessary condition for the adaptation of law enforcement agencies to the new challenges of the digital era.

Key words: law enforcement agencies, law enforcement activities, digitalization, artificial intelligence, cybercrime, cyber security, cyber threats, interagency cooperation.

Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією усіх сфер життєдіяльності, що сприяє не лише економічному зростанню та технологічному прогресу, а й формуванню нових загроз, пов'язаних із кіберпростором. Кіберзлочинність стала глобальною проблемою, яка охоплює різні аспекти: від фінансових шахрайств і крадіжки персональних даних до атак на критичну інфраструктуру держав. Це вимагає від правоохоронних органів впровадження інноваційних підходів до забезпечення безпеки та адаптації до цифрових викликів.

Одним із ключових напрямів модернізації правоохоронної діяльності є інтеграція технологій штучного інтелекту (далі – ШІ), які дозволяють значно підвищити ефективність оперативно-розшукової та аналітичної роботи. Використання алгоритмів машинного навчання, систем автоматизованого аналізу даних і прогнозної аналітики

відкриває нові можливості для протидії кіберзлочинності, зокрема, для виявлення складних кіберзагроз, моніторингу злочинної активності в реальному часі та автоматизації рутинних процесів.

Актуальність теми дослідження зумовлено не лише необхідністю реагування на швидкі темпи розвитку кіберзлочинності, а й потребою у формуванні комплексного підходу до використання ШІ у правоохоронній діяльності. У статті ставиться за мету проаналізувати сучасні можливості, перспективи та виклики впровадження штучного інтелекту для забезпечення кібербезпеки, а також висвітлити правові, етичні та технологічні аспекти цього процесу.

Штучний інтелект революціонізує боротьбу з кіберзлочинністю, дозволяючи аналізувати величезні масиви даних у режимі реального часу, виявляти нові загрози та автоматизувати рутинні операції. Це значно підвищує ефективність правоохоронних органів та встановлює нові стандарти в галузі кібербезпеки.

Сьогодні штучний інтелект – це не просто технологічний тренд, модне слово чи тимчасове захоплення, це третя, комп'ютерна ера, заснована на інноваціях і передових технологіях [1, с. 13].

Впровадження ШІ у боротьбу з кіберзлочинністю сприяє вдосконаленню механізмів моніторингу, підвищенню точності і швидкості ухвалення рішень, а також оптимізації використання ресурсів. Разом з тим це ставить нові вимоги до правових, етичних та технічних аспектів діяльності правоохоронних органів, які повинні адаптуватися до викликів цифрової епохи, забезпечуючи баланс між ефективністю технологій та захистом прав людини.

Поглиблене розуміння значення цифровізації у правоохоронній сфері та її впливу на боротьбу з кіберзлочинністю сприятиме не лише вдосконаленню діяльності правоохоронних органів, а й підвищенню рівня безпеки у суспільстві загалом.

Зацікавленість держави у цифровому розвитку України віддзеркалено у прийнятому 17 листопада 2021 року Розпорядженні Кабінету Міністрів України «Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації» [2]. Метою цієї Стратегії є побудова сучасної та ефективної системи управління інформаційними технологіями для забезпечення підтримки і подальшого цифрового розвитку ефективної та прозорої системи управління державними фінансами.

Результатом реалізації цієї Стратегії повинне стати запровадження Єдиної інформаційно-телекомунікаційної системи управління державними фінансами, побудованої на інтероперабельності електронних інформаційних ресурсів з одночасним комплексним захистом інформації, дотриманням технологічної незалежності і забезпеченням обміну інформацією в режимі реального часу [2].

Сьогодні людство доволі широко послуговується технологіями ШІ в різних галузях як повсякденного життя, так і професійної діяльності (зокрема, у юриспруденції) [3]. Штучний інтелект активно використовується для автоматизації рутинних процесів, генерації типових документів, аналізу великих обсягів юридичної інформації, прогнозування рішень судів, а також для виявлення порушень у нормативно-правових документах.

Ці технології відкривають нові можливості для підвищення ефективності та точності роботи, знижують витрати часу та людських ресурсів. Проте їх впровадження потребує дотримання правових і етичних норм, зокрема забезпечення прозорості алгоритмів, дотримання конфіденційності інформації та запобігання дискримінації у процесі ухвалення автоматизованих рішень.

У контексті цифровізації правоохоронної діяльності штучний інтелект стає не лише інструментом оперативної ефективності, а й важливим чинником трансформації підходів до боротьби з кіберзлочинністю, моніторингу кіберпростору та захисту прав людини у цифрову епоху.

Цифровізація відіграє ключову роль у трансформації правоохоронної діяльності, сприяючи підвищенню ефективності боротьби з кіберзлочинністю в умовах стрімкого розвитку інформаційних технологій. Цей процес передбачає перехід від традиційних методів роботи до використання інноваційних технологій, що дозволяють оперативніше реагувати на виклики сучасного кіберпростору.

Основна увага зосереджується на інтеграції систем штучного інтелекту, які мають потенціал значно покращити діяльність правоохоронних органів. За рахунок використання можливостей ШІ для аналізу великих обсягів даних з'являється можливість швидше ідентифікувати кіберзагрози та виявляти приховані закономірності в злочинній активності. Автоматизація оперативних і слідчих дій за допомогою технологій машинного навчання і нейронних мереж сприяє підвищенню точності розслідувань та зменшенню навантаження на співробітників, що знижує помилки пов'язані з людським фактором.

У цьому контексті цифровізація не лише оптимізує правоохоронні процеси, але й вимагає переосмислення традиційних підходів до кібербезпеки, адаптації до нових загроз та розвитку правових і етичних засад використання технологій. Вона є необхідною умовою для забезпечення ефективної протидії кіберзлочинності у сучасному глобалізованому цифровому середовищі.

Важливим аспектами впровадження ключових технологічних інструментів є алгоритми машинного навчання для розпізнавання шаблонів злочинної поведінки, засоби виявлення аномалій у кіберпросторі, системи моніторингу соціальних мереж і «темного вебу», а також платформи прогнозної аналітики. Ці алгоритми дозволяють виявляти повторювані дії, типові для злочинців, і прогнозувати їхню можливу подальшу активність.

Доречним вбачається проаналізувати засоби виявлення аномалій у кіберпросторі, які використовуються для моніторингу мережевої активності з метою ідентифікації потенційних загроз, таких як спроби несанкціонованого доступу, розповсюдження шкідливого програмного забезпечення чи відстеження підозрілих фінансових операцій. Вони допомагають оперативно реагувати на інциденти та мінімізувати ризики.

Системи моніторингу соціальних мереж і «темного вебу» забезпечують можливість відстеження злочинної діяльності, виявлення контенту, пов'язаного із шахрайством, тероризмом, торгівлею забороненими товарами та іншими видами злочинів. Вони дозволяють збирати інформацію про загрози та визначати ключових учасників злочинних мереж.

Платформи прогнозної аналітики застосовуються для аналізу історичних даних, створення моделей ризиків і прогнозування можливих сценаріїв розвитку злочинної діяльності. Це дозволяє правоохоронним органам розробляти проактивні стратегії, спрямовані на запобігання злочинам до їхнього здійснення.

У комплексі ці інструменти формують потужну технологічну основу для ефективної протидії кіберзлочинності, підвищення безпеки суспільства та оптимізації роботи правоохоронних органів.

Сучасні підходи до інтеграції штучного інтелекту у практику кібербезпеки охоплюють широкий спектр технологій, спрямованих на посилення здатності ідентифікувати, запобігати та реагувати на кіберзагрози. Одним із найбільш поширених методів є розпізнавання аномальної поведінки в мережі. За допомогою алгоритмів машинного навчання аналізуються великі обсяги трафіку для виявлення відхилень від нормальної діяльності, таких як підозріла активність користувачів, незвичні патерни доступу до даних чи атаки типу «відмова в обслуговуванні» (DDoS).

Моніторинг «темних» веб-ресурсів є ще одним важливим напрямом. ШІ використовується для автоматичного аналізу контенту у «темній мережі», що дозволяє ідентифікувати нелегальну діяльність, пов'язану з продаванням заборонених товарів, розповсюдженням шкідливого програмного забезпечення чи обміном конфіденційною інформацією. Згідно аналізу щорічного звіту «The Chainalysis 2024 Crypto Crime Report» [4, с. 90] загальний обсяг ринку за переліченими напрямами складає майже 2 млрд. доларів та постійно зростає.

Системи машинного навчання сприяють покращенню оперативної ефективності завдяки автоматизації рутинних завдань, таких як класифікація загроз, обробка інцидентів безпеки та створення рекомендацій для подальших дій. Вони також використовуються для прогнозування ризиків на основі історичних даних, що дозволяє здійснювати проактивні заходи безпеки.

До основні переваг систем машинного навчання слід віднести:

1. Штучний інтелект швидко та ефективно забезпечує миттєву обробку великих обсягів інформації, що дозволяє скоротити час на реагування;

2. Завдяки самооновлюваним алгоритмам зменшується ймовірність помилкових спрацювань і підвищується точність результатів;

3. Зниження навантаження на людський персонал та автоматизація повторюваних процесів, за цей рахунок відбувається оптимізація ресурсів.

А.В. Кубаєнко зазначає, що цифровізація висуває нові вимоги до навичок співробітників державних органів, і вони мають своєчасно відповідати цьому запитові [5]. Це стосується не лише базового розуміння принципів роботи сучасних цифрових технологій, але й здатності застосовувати спеціалізовані інструменти, зокрема системи штучного інтелекту, для аналізу даних, прогнозування ризиків і виявлення загроз.

Крім того, важливим аспектом є формування цифрової грамотності, яка включає навички роботи з великими масивами інформації, розуміння принципів кібергігієни та дотримання етичних стандартів під час використання технологій. Також потребується постійне навчання та підвищення кваліфікації, оскільки технологічний прогрес обумовлює швидке «старіння» знань і підходів.

Інтеграція цифрових рішень у діяльність правоохоронних органів вимагає від співробітників не лише технічної компетенції, а й міждисциплінарного підходу, що включає правові, соціальні та психологічні аспекти роботи у цифровому середовищі. Такі зміни створюють необхідність розвитку спеціалізованих навчальних програм і створення умов для постійного професійного розвитку кадрів, аби забезпечити їхню готовність до ефективної діяльності в умовах цифрової трансформації.

Для повноти дослідження слід проаналізувати практичні кейси застосування ШІ для протидії різним типам кіберзлочинів, включаючи фінансові шахрайства, крадіжку даних, атаки на критичну інфраструктуру.

Кейс 1: крадіжка даних. ШІ-системи аналізу трафіку здатні виявляти несанкціоноване виведення великих обсягів даних із серверів компаній, а також пристрої та хмарне програмне забезпечення, які використовуються співробітниками. Наприклад, компанії застосовують такі системи для захисту конфіденційної інформації клієнтів в межах концепції BYOD (bring your own device). Результатом є швидке виявлення загроз і запобігання витокам даних.

Кейс 2: атаки на критичну інфраструктуру. Системи ШІ використовуються для моніторингу мереж енергетичних компаній. Алгоритми аналізують дані в реальному часі, виявляючи аномальні сигнали, які можуть вказувати на спробу злому або саботажу. Результатом є зниження ризиків збоїв у роботі критичних систем.

Кейс 3: поширення шкідливого програмного забезпечення. Антивірусні програми з елементами ШІ здатні виявляти нові види шкідливих програм та уразливості нульового дня на основі поведінкових характеристик, а не лише за попередньо відомими сигнатурами. Результатом є покращення ефективності захисту від нових і раніше невідомих загроз.

Об'єднані платформи розширеного виявлення та реагування (extended detection and response, XDR) інцидентів із безпекою, які використовують ШІ та автоматизацію, надають можливість формування цілісного і ефективного способу захисту та попередження від складних кібератак і реагуванню на них [6].

Доцільно також розглянути правові, етичні та технічні виклики, які виникають під час впровадження таких технологій, зокрема питання приватності, прозорості алгоритмів і ризиків автоматизації ухвалення рішень.

Зрозумілим є те, що використання ШІ передбачає аналіз великих обсягів персональних даних, що може порушувати право на приватність. Тому необхідним є впровадження чітких політик щодо збору, зберігання та використання даних, дотримання норм GDPR або аналогічних регламентів.

Алгоритми ШІ часто є «чорними ящиками» і зрозуміти, як саме ухвалюється те чи інше рішення, складно. Це створює ризики для довіри до систем. Вирішенням такої проблем є розробка прозорих та підзвітних алгоритмів, а також можливість перевірки їхньої роботи незалежними експертами.

Наступною проблемою є надмірна автоматизація, яка може призвести до ухвалення необґрунтованих рішень, таких як хибна ідентифікація підозрюваних. Вирішити це можливо завдяки запровадженню механізмів для перевірки та підтвердження рішень людиною, що дозволяє уникнути помилкових дій.

Проблемою може стати і те, що ШІ може працювати з упередженими даними, що призводить до дискримінаційних результатів. В цьому може допомогти регулярний аудит алгоритмів на предмет упередженості та розробка етичних принципів використання ШІ в правоохоронній діяльності.

Щодо кібербезпеки самих ШІ-систем, то проблеми із алгоритмами можуть стати мішенню для кібератак, таких як маніпуляція даними для збоїв у роботі системи. Вирішенням може стати постійне вдосконалення механізмів захисту ШІ-систем, зокрема шифрування даних та перевірки джерел інформації.

Інтеграція ШІ у практику кібербезпеки дозволяє значно підвищити ефективність боротьби з кіберзлочинами, але вимагає уважного врахування ризиків і викликів для забезпечення збалансованого та відповідального використання технологій.

Цифрові технології докорінно трансформують правоохоронну діяльність, створюючи принципово нові можливості для комунікації, аналізу та протидії злочинності. Інтегровані інформаційні системи забезпечують миттєвий обмін даними між правоохоронними органами на національному та міжнародному рівнях, що підвищує ефективність реагування на транснаціональні злочини.

Сучасні автоматизовані системи моніторингу та глибокого аналізу даних дозволяють не просто фіксувати правопорушення, але й упереджено виявляти потенційні загрози, прогнозувати криміногенні тенденції та координувати міжвідомчі дії з небаченою раніше оперативністю та точністю.

Міжнародна співпраця у сфері протидії кіберзлочинності набуває дедалі більшого значення через транснаціональність сучасних кримінальних загроз. Інтернет-середовище не має географічних кордонів, що створює унікальні можливості для злочинців здійснювати протиправні дії з будь-якої точки світу.

Ключовими інституціями міжнародної координації протидії кіберзлочинності виступають потужні глобальні організації: Інтерпол, структури Європейського Союзу, профільні підрозділи ООН. Їхня діяльність спрямована на формування уніфікованих механізмів виявлення, переслідування та превенції кримінальних діянь у цифровому просторі.

Принципово важливим інструментом міжнародної співпраці стають багатосторонні угоди та конвенції. Зокрема, Будапештська конвенція Ради Європи про кіберзлочинність створює уніфіковану правову базу для міждержавної взаємодії. Такі документи дозволяють долати юрисдикційні обмеження, забезпечувати швидкий трансконтинентальний обмін оперативною інформацією та координувати розслідування складних кримінальних справ.

Попри численні переваги цифровізації правоохоронної діяльності, постають фундаментальні етичні, правові та соціальні виклики. Принципово необхідно дотримати тонкий баланс між ефективністю протидії кіберзлочинності та забезпеченням недоторканності приватного життя громадян.

Ключовими пріоритетами міжнародної співпраці стають:

– уніфікація нормативних баз у сфері кібербезпеки;

– стандартизація процедур розслідування транснаціональних злочинів;

– створення уніфікованих протоколів обміну інформацією;

– гармонізація підходів до захисту персональних даних;

– розробка спільних освітніх і тренінгових програм для правоохоронців.

Цифровізація правоохоронної діяльності виступає визначальним фактором забезпечення безпеки в динамічному глобальному середовищі. Для її успішної реалізації потрібно комплексно враховувати технологічні можливості, правові, етичні та соціальні контексти з метою гарантування справедливості, рівності та захисту прав людини.

Міжнародна співпраця є не просто бажаною, а життєво необхідною умовою ефективної протидії сучасним кримінальним загрозам. Лише консолідація зусиль на національному, регіональному та глобальному рівнях здатна створити дієву систему кібербезпеки, спроможну адекватно реагувати на виклики цифрової епохи.

ЛІТЕРАТУРА

1. Сніґоля Матуєлене, Віктор Шевчук, Юрґіта Балтрунене. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. DOI: 10.32353/khrife.4.2022.02

2. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами до 2025 року та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 листопада 2021 р. № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text

3. Пилипчук В. Г., Баранов О. А., Гиляка О. С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. *Вісник Національної академії правових наук України.* 2022. Т. 29. № 2. С. 35–62. DOI: 10.37635/jnalsu.29(2).2022.35-62

4. The Chainalysis 2024 Crypto Crime Report. URL: https://go.chainalysis.com/crypto-crime-2024.html

5. Кубаєнко А. В. Цифровізація як сучасна умова функціонування правоохоронної системи *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.).* Одеса. 2022. Т. 2. С. 194–197.

6. Що таке розширене виявлення й реагування (XDR)? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-xdr