СЕРІЯ «Право»

УДК 351.74:004.5:006.8:343.3

https://doi.org/10.52058/2786-6300-2024-11(29)-447-461

Баєва Лілія Вікторівна кандидат юридичних наук, доцент кафедри конституційного, адміністративного та трудового права, Національний університет «Запорізька політехніка», вул. Жуковського, 64-а, м. Запоріжжя, 69063, https://orcid.org/0000-0001-8161-9005

Геращенко Олександр Сергійович кандидат юридичних наук, доцент кафедри психології, Національний університет «Одеська юридична академія», вул. Академічна, 2, м. Одеса, 65000, https://orcid.org/0000-0002-8552-0878

Кундеус Владислав Геннадійович кандидат юридичних наук, доцент кафедри кримінального права та кримінології, Навчально-науковий інститут № 5, Харківський національний університет внутрішніх справ, пр. Льва Ландау, 27, м. Харків, 61080, https://orcid.org/0000-0002-2430-5437

ІННОВАЦІЇ У КІБЕРПОЛІЦІЇ УКРАЇНИ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА КІБЕРАНАЛІТИК

Анотація. Швидке зростання кіберзагроз, зокрема кіберзлочинності та кібертероризму, суттєво вплинуло на міжнародну безпеку. Україна як країна, що бере участь у геополітичному конфлікті та здійснює цифрову трансформацію, зазнала численних кібератак, що зумовило необхідність удосконалення її інфраструктури кібербезпеки. Кіберполіція України посідає перше місце в реагуванні на ці виклики, а останні інновації базуються на інтеграції штучного інтелекту та кібераналітиків у її діяльність. У статті розглянуто актуальність технологій на основі штучного інтелекту для підвищення ефективності кіберполіції України та їх наслідки для боротьби з кіберзлочинністю в більш широкому сенсі.

Мета статті – проаналізувати, як впровадження штучного інтелекту та використання можливостей аналітики трансформували операційні можливості кіберполіції України. Завдяки використанню штучного інтелекту кіберполіція може автоматизувати виявлення кіберзагроз, оптимізувати аналіз загроз і покращити реагування на кіберінциденти в режимі реального часу. Кібер-

аналітики, оснащені інструментами штучного інтелекту, допомагають проаналізувати величезні обсяги цифрових даних, виявити моделі поведінки кіберзлочинців і визначити вразливості в мережах.

За результатами дослідження виокремлено кілька ключових інновацій, зокрема розробку алгоритмів штучного інтелекту, які можуть виявляти аномалії в мережевому трафіку, ідентифікувати фішингові схеми та відстежувати діяльність кіберзлочинців у «темній мережі». Застосування ШІ для автоматизації рутинних завдань, таких як виявлення шкідливого програмного забезпечення та цифрова криміналістика, дозволило підвищити швидкість і точність проведення розслідувань.

Отже, інтеграція технологій штучного інтелекту та стратегічне залучення кібераналітиків підвищили ефективність та адаптивність кіберполіції України. Ці інновації не лише зміцнюють національну кібербезпеку, а й позиціонують Україну як провідного учасника міжнародних заходів у боротьбі з кіберзлочинністю.

Ключові слова: цифрова безпека, алгоритми AI, кіберзагрози, аналітика даних.

Baieva Liliia Viktorivna Candidate of Legal Sciences, Associate Professor, Department of Constitutional, Administrative and Labor Law, National University Zaporizhzhya Polytechnic, Zhukovskii St., 64-a, Zaporizhzhya, 69063, https://orcid.org/0000-0001-8161-9005

Herashchenko Oleksandr Serhiyovych Candidate of Legal Sciences, Associate Professor, Department of Psychology, Odesa Law Academy National University, Akademichna St., 2, Odesa, 65000, https://orcid.org/0000-0002-8552-0878

Kundeus Vladyslav Gennadiyovych Candidate of Legal Sciences, Associate Professor, Department of Criminal Law and Criminology, Educational and Scientific Institute № 5, Kharkiv National University of Internal Affairs, L. Landau Ave., 27, Kharkiv, 61080,https://orcid.org/0000-0002-2430-5437

INNOVATIONS IN UKRAINE'S CYBER POLICE: THE USE OF ARTIFICIAL INTELLIGENCE AND CYBER ANALYTICS

Abstract. The rapid rise of cyber threats, including cybercrime and cyberterrorism, has significantly impacted international security. Ukraine, as a country involved in a geopolitical conflict and undergoing digital transformation, has faced numerous cyberattacks, which has necessitated the improvement of its cybersecurity infrastructure. The Cyber Police of Ukraine is at the forefront of



responding to these challenges, with recent innovations focused on the integration of artificial intelligence (AI) and cyber analysts into its operations. This article examines the relevance of AI-based technologies for enhancing the effectiveness of Ukraine's Cyber Police and their implications for combating cybercrime on a broader scale.

The aim of this article is to analyze how the implementation of artificial intelligence and the use of analytical capabilities have transformed the operational capacities of Ukraine's Cyber Police. Through AI, the Cyber Police can automate threat detection, optimize threat analysis, and improve real-time responses to cyber incidents. Cyber analysts equipped with AI tools play a crucial role in analyzing vast amounts of digital data, identifying cybercriminal behavior patterns, and detecting vulnerabilities in networks.

The research highlights several key innovations, including the development of AI algorithms that can detect anomalies in network traffic, identify phishing schemes, and track cybercriminal activities in the dark web. The application of AI to automate routine tasks such as malware detection and digital forensics has improved the speed and accuracy of investigations.

Thus, the integration of AI technologies and the strategic involvement of cyber analysts have increased the efficiency and adaptability of Ukraine's Cyber Police. These innovations not only strengthen national cybersecurity but also position Ukraine as a leading participant in international efforts to combat cybercrime.

Keywords: digital security, AI algorithms, cyber threats, data analytics.

Постановка проблеми. Останніми роками проблема кіберзлочинності значно зросла, вплинувши на держави, організації та окремих осіб у світовому масштабі. Швидка цифрова трансформація в різних секторах створила нові вразливості, перетворюючи кіберпростір на поле бою як для злочинної діяльності, так і для атак, що фінансуються державою. Україна як країна, що бере участь як у геополітичному конфлікті, так і в технологічному розвитку, стала ключовою ціллю для кібератак, які варіюються від масштабних витоків даних і саботажу критичної інфраструктури до складних дезінформаційних кампаній і кібершпигунства. З огляду на складність й частоту цих загроз, традиційних методів кібербезпеки та правоохоронних органів уже недостатньо.

Український уряд відреагував на цей виклик, зміцнивши спроможність своєї кіберполіції – спеціалізованого підрозділу, завданням якого є боротьба з кіберзагрозами. Однак зі зростанням масштабів і складності кіберзлочинності потреба в інноваціях у кіберполіції стає щоразу нагальнішою. Зокрема, інтеграція штучного інтелекту (далі – ШІ) та стратегічне використання

кібераналітиків є сьогодні критично важливими компонентами в боротьбі з кіберзлочинністю. Технології ШІ пропонують значні переваги, такі як можливість опрацьовувати великі обсяги даних у режимі реального часу, автоматизувати рутинні завдання та виявляти закономірності, які можуть бути невидимими для аналітиків-людей. Кібераналітики, озброєні інструментами на основі ШІ, можуть ефективніше інтерпретувати дані, що дає змогу швидко й влучно реагувати на кіберзагрози.

Актуальність цієї проблеми посилюється тим, що Україна знаходиться на перетині поточної кібервійни та світових мереж кіберзлочинності. Кібератаки, спрямовані проти України, часто слугують своєрідним полігоном для відпрацювання тактик, які згодом можуть бути використані в інших країнах. Отож, інновації в стратегії кіберзахисту України мають усебічні наслідки для міжнародної кібербезпеки. Впроваджуючи технології на основі штучного інтелекту та підвищуючи кваліфікацію кібераналітиків, українська кіберполіція може ефективніше реагувати на різноманітні сучасні загрози, з якими вона стикається. Крім того, ці інновації пропонують модель для інших країн, які борються з такими ж викликами [1].

Розв'язання проблеми кіберзлочинності в Україні є не лише національним пріоритетом, а й питанням міжнародного значення. Досвід, отриманий в Україні в процесі інтеграції ШІ та кібераналізу в правоохоронну діяльність, може стати основою для світових практик, сприяючи створенню стійкіших інфраструктур кібербезпеки в усьому світі. З огляду на це, вивчення таких інновацій є надзвичайно актуальним, оскільки вони відображають майбутню траєкторію розвитку кіберполіції. Використання спеціальних знань та програмного забезпечення може істотно знизити рівень кримінальних правопорушень як в Україні, так і у світі [2].

Аналіз останніх досліджень і публікацій. Сучасна академічна наукова література свідчить про трансформаційний потенціал ШІ в правоохоронних органах і кібербезпеці [3–4]. Зокрема, А. Патрика, О. Герасимчук, О. Нємкова, Я. Савин, В. Дудикевич [5], О. Голубенко та співавтори [6] розглядають особливості застосування методів машинного навчання для масштабного вивчення даних, що може бути застосовано безпосередньо для виявлення кіберзлочинів. Роботи науковців, що стосуються нейронних мереж, здатних розпізнавати закономірності в неструктурованих даних, є надзвичайно актуальними для виявлення аномалій у мережевому трафіку та ідентифікації потенційних кіберзагроз. Дослідження В. Довганя та І. Коцмана [7] зосереджене на інструментах для аналізу цифрових доказів на основі штучного інтелекту, які українська кіберполіція може використати для покращення своїх слідчих можливостей.

В Україні низка академічних і науково-дослідних установ зробили внесок у дослідження інновацій у сфері кібербезпеки. Ю. Добришин [8]



присвятив свої праці застосуванню штучного інтелекту в кібербезпеці, зокрема автоматизованим системам виявлення фішингових атак і шкідливого програмного забезпечення. Дослідження автора висвітлює переваги використання машинного навчання для боротьби із загрозами, які стрімко видозмінюються. О. Бугера [9] вивчав використання штучного інтелекту для скорочення часу реагування на інциденти у справах про кіберзлочини. Такі наукові дослідження свідчать про щоразу більше зацікавлення до кіберполіції з використанням штучного інтелекту, водночас виявляючи певні обмеження щодо впровадження на рівні правоохоронних органів.

Проте, незважаючи на ці досягнення, залишається кілька нерозв'язаних питань. Однією з найважливіших проблем є зрозумілість та прозорість систем штучного інтелекту в контексті правоохоронної діяльності. Незважаючи на те, що ШІ може обробляти величезні обсяги даних і виявляти кіберзагрози, природа «чорного ящика» багатьох алгоритмів машинного навчання ускладнює розуміння й пояснення рішень, які генерує ШІ, для операторів-людей. Така непрозорість створює етичні та практичні проблеми для кіберполіції, оскільки може поставити під сумнів юридичну прийнятність доказів, отриманих за допомогою ШІ, у суді та знизити довіру громадськості до автоматизованих систем.

Окрім цього, хоча ШІ забезпечує автоматизацію й ефективність, він не позбавлений обмежень у точному розрізненні діяльності, спрямованої на добро, та зловмисної діяльності. Помилкові ідентифікації можуть перевантажувати аналітиків і переспрямовувати ресурси від реальних загроз, що особливо актуально для української кіберполіції, яка вже працює під значним тиском через велику кількість кібератак.

Мета статті – проаналізувати, як впровадження штучного інтелекту та використання можливостей аналітики трансформували операційні можливості кіберполіції України.

Виклад основного матеріалу. Розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій у всі сфери суспільного життя, зокрема і в діяльність органів державної влади й органів місцевого самоврядування, потребує забезпечення інформаційної безпеки як однієї з найважливіших функцій держави [10, с. 504–505].

У сучасній діяльності кіберполіції штучний інтелект (ШІ) став важливим інструментом, який відіграє провідну роль в підтримці цифрової безпеки та боротьбі з кіберзлочинністю. Зі зростанням складності та масштабності кіберзагроз правоохоронні органи все більше використовують штучний інтелект задля зміцнення своїх розслідувальних можливостей, автоматизації повсякденних завдань та виявлення кіберзагроз із більшою ефективністю.

Технології штучного інтелекту, що використовують у діяльності кіберполіції, охоплюють низку найсучасніших методів, зокрема машинне навчання

(ML), обробку природної мови (NLP), глибинне навчання (DL) та автоматизовані системи прийняття рішень. Завдяки цим технологіям сили кіберполіції можуть аналізувати значні обсяги даних, виявляти закономірності, що вказують на злочинну діяльність, а також швидше та ефективніше реагувати на кіберзагрози.

Так, наприклад, алгоритми машинного навчання здатні виявляти аномалії в мережевому трафіку, допомагаючи органам влади виявляти потенційні кібератаки ще до того, як вони відбудуться. Обробка природної мови використовується для вивчення комунікації між кіберзлочинцями в соціальних мережах, на форумах і зашифрованих платформах. Моделі глибинного навчання досягли неабияких результатів у визначенні підписів шкідливих програм, розпізнаванні спроб фішингу і навіть у прогнозуванні майбутніх кіберзагроз на основі історичних даних.

Автоматизовані системи, що підтримують штучний інтелект, допомагають кіберполіції визначати пріоритетність загроз, скорочуючи час, що витрачається на другорядні інциденти, і дозволяючи співробітникам зосередитися на пріоритетних справах. Інструменти на основі штучного інтелекту, такі як чат-боти та віртуальні агенти, використовують також для того, щоби допомогти населенню ефективніше повідомляти про кіберінциденти, забезпечуючи миттєве реагування в ситуаціях із низьким рівнем ризику, а також вказуючи на важливі події, які потребують подальшого розслідування.

Одне з основних застосувань штучного інтелекту в роботі як поліції, так і кіберполіції – це виявлення кіберзагроз і запобігання їм та покращення судової експертизи в поліції [11]. Для цього використовується кілька алгоритмів ШІ, кожен з яких має свої унікальні можливості, пристосовані до різних типів загроз.

Алгоритми виявлення аномалій знаходять відхилення від нормальної поведінки мережі або користувача. Виявлення аномалій активно використовується для знаходження заражень шкідливим програмним забезпеченням, програм-вимагачів, інсайдерських загроз і навіть розподілених атак на кшталт «розподілена відмова в обслуговуванні» (DDoS). Такі алгоритми, як k-найближчих сусідів (KNN), ізоляційні ліси та машини опорних векторів (SVM), використовуються для виявлення відхилень у даних мережевого трафіку.

Алгоритми класифікації машинного навчання, такі як дерева рішень, випадкові мережі та нейронні мережі, активно використовуються для класифікації електронних листів як спроб фішингу, розрізнення легітимних і шкідливих URL-адрес, а також для позначення спам-повідомлень. Алгоритми класифікації також застосовуються в розпізнаванні зображень для виявлення фальшивих профілів і фішингових вебсайтів.



Алгоритми розпізнавання шаблонів, глибинне навчання, зокрема згорткові нейронні мережі (CNN), використовують для розпізнавання шаблонів, таких як аналіз метаданих файлів і виявлення підписів шкідливих програм. Моделі розпізнавання образів мають важливе значення для виявлення нових варіацій шкідливого програмного забезпечення, оскільки вони можуть вивчати основну структуру шкідливого коду і позначати підозрілі файли.

Інструменти поведінкового аналізу на основі штучного інтелекту відстежують активність користувачів в інтернеті та виявляють аномальні моделі поведінки, які можуть свідчити про зловмисні наміри, наприклад, спроби отримати доступ до несанкціонованих даних або передати конфіденційну інформацію. Алгоритми навчання з використанням підкріплення дедалі частіше використовуються в поведінковому аналізі для навчання та адаптації до тактик кіберзлочинців, що постійно вдосконалюються.

Моделі NLP використовуються для аналізування величезних обсягів неструктурованих даних, зокрема електронних листів, повідомлень на форумах і чатах [12]. Обробляючи мовні дані, ці моделі допомагають ідентифікувати комунікації кіберзлочинців, виявляти атаки соціальної інженерії та розкривати наміри, що стоять за спробами фішингу (табл. 1).

Таблиця 1

Застосування алгоритмів ШІ в запобіганні злочинності в Україні

Алгоритми ШІ	Застосування в кіберполіції	Приклади
Виявлення аномалій	Виявлення нерегулярного мережевого трафіку та загроз	К-найближчих сусідів, ізольовані ліси
Класифікація	Класифікація електронних листів, URL-адрес і повідомлень як шкідливих	Дерева рішень, нейронні мережі
Розпізнавання шаблонів	Виявлення підписів шкідливих програм та ідентифікація фішингу	Згорткові нейронні мережі (CNN)
Поведінковий аналіз	Моніторинг активності користувачів і виявлення внутрішніх загроз	Навчання з підкріпленням
Обробка природної мови (NLP)	Аналіз кіберзлочинних комунікацій і загроз	Моделі NLP для виявлення фішингу, розвідки загроз

Джерело: сформовано авторами на підставі [13]

ШІ відіграє провідну роль в забезпеченні цифрової безпеки, допомагаючи кіберполіції виявляти кіберінциденти в режимі реального часу, запобігати їм та реагувати на загрози. Однією з важливих переваг штучного інтелекту є його здатність постійно навчатися та адаптуватися, покращуючи свої можливості виявлення загроз завдяки обробці більшого обсягу даних. Системи на основі штучного інтелекту надзвичайно ефективно виявляють як відомі, так і невідомі раніше загрози, які зазвичай називають атаками «нульового дня», і які часто не помічають традиційні рішення для забезпечення безпеки.

ШІ використовується в декількох сферах цифрової безпеки, зокрема в захисті кінцевих точок, системах виявлення вторгнень (IDS) і автоматизованих системах реагування на інциденти. У захисті кінцевих точок алгоритми ШІ використовуються для сканування пристроїв на наявність шкідливого програмного забезпечення або підозрілої активності, забезпечуючи швидку ізоляцію уражених пристроїв від мережі, щоби запобігти подальшій шкоді. Системи виявлення вторгнень, вдосконалені ШІ, аналізують вхідний трафік і виявляють ознаки потенційних порушень, що дає змогу швидко вжити заходів для захисту.

До того ж штучний інтелект допомагає автоматизувати реагування на кіберінциденти. Системи, керовані штучним інтелектом, можуть реагувати на низькорівневі кіберзагрози без участі людини, скорочуючи час реагування та вивільняючи ресурси для більш складних перевірок. Наприклад, коли ШІ виявляє незвичний виплеск передачі даних, що може свідчити про витік інформації, він може автоматично вжити заходів безпеки, наприклад, заблокувати доступ до певних файлів або сповістити команду безпеки.

Кіберполіція України є однією з перших, хто впроваджує технології штучного інтелекту для боротьби з посилюваною загрозою кіберзлочинності в регіоні. Одним із вагомих успіхів стало використання систем на основі штучного інтелекту для виявлення та пом'якшення наслідків DDoS-атак на українську інфраструктуру. Інструменти ШІ були застосовані для моніторингу моделей трафіку, що дозволяє кіберполіції блокувати зловмисний трафік до того, як він може завдати шкоди основним послугам.

У 2023 році кіберполіція України співпрацювала з місцевими компаніями з кібербезпеки для впровадження алгоритмів штучного інтелекту, які можуть виявляти фішингові вебсайти та шахрайські дії в інтернеті, спрямовані на громадян України. Підсумком цієї співпраці стало закриття сотень фейкових вебсайтів і акаунтів у соціальних мережах, які використовувалися для шахрайства та поширення шкідливого програмного забезпечення. Для пошуку цих шахрайських сайтів в інтернеті використовувалися вебсканери на основі штучного інтелекту, про які невдовзі повідомлялося провайдерам послуг для негайного видалення.

Ще одним яскравим прикладом використання штучного інтелекту в діяльності кіберполіції стала розробка чат-бота, який допомагає громадянам повідомляти про кіберзлочини. Чат-бот використовує обробку природної мови, щоби розуміти скарги й швидко позначати термінові справи для подальшого вивчення. Завдяки цій ініціативі покращилася можливість громадян повідомляти про інциденти та пришвидшилася реакція поліції на критичні кіберзлочини, такі як крадіжка особистих даних і фінансове шахрайство.

ШІ використовується також для відстеження та моніторингу діяльності кіберзлочинних угруповань, що діють в Україні. З допомогою використання



алгоритмів машинного навчання кіберполіція може аналізувати схеми комунікації злочинних мереж, відстежувати незаконні транзакції з криптовалютами та прогнозувати потенційні атаки на об'єкти критичної інфраструктури. Такі системи штучного інтелекту надають правоохоронцям важливу інформацію, що дозволяє їм запобігати кібератакам і припиняти злочинні операції до того, як буде завдано значної шкоди.

Аналіз даних стає важливим компонентом у боротьбі з кіберзагрозами, особливо для кіберполіції, завданням якої є підтримка цифрової безпеки. В Україні, де ситуація з кіберзагрозами стрімко розвивається, аналіз даних відіграє вирішальну роль у виявленні кіберінцидентів, запобіганні їм та реагуванні на небезпеку [14]. Кіберполіція України використовує сучасні методи аналізу даних для моніторингу мережевого трафіку, виявлення закономірностей, що вказують на кіберзлочини, та отримання інформації, яка допомагає захистити критично важливу інфраструктуру та громадян. Використовуючи величезні обсяги даних, зібраних із різних джерел, кіберполіція може реагувати на загрози в режимі реального часу та впроваджувати проактивні заходи безпеки [14].

Боротьба з кіберзагрозами значною мірою залежить від спроможності виявляти аномальні закономірності в даних, які можуть свідчити про зловмисну діяльність. Аналіз даних дає змогу кіберполіції розглядати величезні обсяги даних, що генеруються мережами, пристроями та онлайн-активністю, у пошуках ознак кібератак, таких як фішинг, поширення шкідливого програмного забезпечення та спроби несанкціонованого доступу до мережі. Аналізуючи ці дані, кіберполіція може виявити раніше невідомі загрози, які часто називають атаками «нульового дня», а також спрогнозувати ймовірність майбутніх кіберінцидентів. Підходи, що базуються на таких даних, як виявлення аномалій і поведінковий аналіз, дають можливість правоохоронцям виявляти відхилення від нормальної поведінки в мережі, що може свідчити про кібератаки або спроби злому, що тривають.

Одним із ключових аспектів ефективної аналітики даних є можливість збирати та обробляти дані з різних джерел. Українська кіберполіція збирає дані з різних осередків, зокрема від інтернет-провайдерів, фірм, що працюють у сфері кібербезпеки, каналів розвідданих про загрози та урядових установ. Дані також збирають із платформ соціальних мереж, публічних форумів і «темної мережі», де кіберзлочинці часто обговорюють свої плани та торгують нелегальними товарами. Публічні звіти та скарги громадян на кіберзлочинність є важливими джерелами даних для виявлення нових загроз.

Обробка такої великої кількості даних вимагає ефективних методів перевірки, трансформації та підготовки їх до аналізу. Кіберполіція нерідко постає перед викликами, пов'язаними з управлінням величезним обсягом і

різноманітністю даних, а також із забезпеченням їхньої якості та релевантності. Методи обробки даних, такі як дедуплікація, нормалізація та фільтрація аномалій, застосовуються для того, щоб аналізувати лише точну та корисну інформацію. Після обробки дані зберігаються в захищених, масштабованих базах даних, часто хмарних, щоб забезпечити доступ до них для аналізу в режимі реального часу [15].

Інструменти, що використовує кіберполіція України для аналізу даних, різноманітні й містять як відкриті, так і закриті платформи. Одним із найпоширеніших інструментів є Splunk, який дозволяє кіберполіції відстежувати та аналізувати згенеровані машиною дані в режимі реального часу. Splunk доволі ефективний у виявленні нетипових патернів у мережевому трафіку, які можуть свідчити про порушення безпеки або кібератаки. Ще одним важливим інструментом є ELK Stack (Elasticsearch, Logstash і Kibana), який надає комплексне рішення для пошуку, візуалізації та аналізу великих наборів даних. ELK Stack використовується для управління та моніторингу логів, які мають ключове значення для відстежування діяльності потенційних кіберзлочинців. Wireshark, аналізатор мережевих протоколів, застосовується для перехоплення та перевірки пакетів даних, що передаються мережею, допомагаючи виявляти зловмисну активність в режимі реального часу.

На доповнення до цих інструментів, кіберполіція застосовує сучасніші платформи аналізу даних, які використовують алгоритми ШІ й машинного навчання. Такі платформи забезпечують предиктивну аналітику, що дозволяє кіберполіції прогнозувати потенційні кіберзагрози на основі історичних даних і поточних тенденцій. Інструменти на основі ШІ, такі як IBM QRadar і Cortex XDR від Palo Alto Networks, використовують машинне навчання для автоматизації виявлення загроз і реагування на них, що значно підвищує ефективність операцій із кібербезпеки [16–17].

Взаємодія між штучним інтелектом і аналітикою даних відіграє важливу роль у сфері кібербезпеки. На основі аналітики даних будуються алгоритми штучного інтелекту, зокрема моделі машинного навчання. Наприклад, алгоритми машинного навчання покладаються на історичні набори даних, щоби вивчити моделі поведінки легітимних користувачів, що дозволяє системі виявляти аномалії, які можуть свідчити про кібератаки. Наприклад, у випадку виявлення фішингу, аналітика даних використовується для вивчення великого обсягу електронних листів, виокремлення ключових характеристик, таких як електронна адреса відправника, URL-посилання та зміст повідомлення, і введення цих даних у модель штучного інтелекту, яка класифікує електронний лист як фішинговий або легітимний.

Ще одним прикладом інтеграції ШІ з аналітикою даних у кібербезпеці є обробка природної мови (Natural Language Processing, NLP), яка використо-

вується для аналізу величезних обсягів неструктурованих даних, таких як онлайн-форуми, чати та повідомлення в соціальних мережах. Алгоритми NLP здатні розуміти та інтерпретувати людську мову, що дає змогу кіберполіції виявляти кіберзлочинну діяльність в обговореннях, пов'язаних із хакерством, поширенням шкідливого програмного забезпечення або продажем викрадених даних. Така форма аналізу даних допомагає кіберполіції виявляти нові тенденції кіберзлочинності та прогнозувати потенційні атаки на основі мовних особливостей кіберзлочинців.

Синергія між ШІ та аналітикою даних поширюється також на платформи розвідки загроз, які агрегують дані з різних джерел і використовують алгоритми ШІ для кореляції та аналізу цих даних. Такі платформи допомагають кіберполіції визначати пріоритетність загроз, оцінюючи їхню серйозність та актуальність на основі аналізу даних. ШІ може швидко обробляти великі масиви даних, надаючи практичні висновки, допомагаючи командам кібербезпеки реагувати на загрози швидше й точніше.

Автоматизація на основі ШІ – ще одна важлива перевага, яку дає інтеграція штучного інтелекту та аналітики даних. Інструменти автоматизації на основі ШІ можуть виконувати такі завдання, як блокування шкідливих IP-адрес, відправлення на карантин заражених пристроїв і сповіщення співробітників служби безпеки під час виявлення підозрілої активності. Ці автоматизовані реакції, що ґрунтуються на аналітиці даних, значно скорочують час, необхідний для усунення кіберзагроз і запобігання подальшим збиткам.

Аналітика даних довела свою ефективність в широкому спектрі застосувань у сфері кібербезпеки для кіберполіції України. Кіберполіція використовує аналітику даних для відстежування діяльності кіберзлочинних груп, виявлення шахрайських схем в інтернеті та захисту критичної інфраструктури від кібератак. Останніми роками Україна зазнає дедалі більшої кількості політично вмотивованих кібератак, спрямованих на державні установи та об'єкти критичної інфраструктури. Використовуючи аналітику даних та інструменти на основі штучного інтелекту, кіберполіція змогла виявити та запобігти цим атакам, нерідко на ранніх стадіях (табл. 2).

Наприклад, під час серії DDoS-атак на українські банки та урядові вебсайти аналіз даних допоміг визначити походження атаки та відрізнити законний трафік від зловмисного. Проаналізувавши структуру трафіку, кіберполіція змогла переспрямувати шкідливий трафік подалі від передбачених цілей та мінімізувати шкоду, завдану атакою. Аналіз даних також допоміг визначити джерело атаки, що призвело до скоординованої міжнародної реакції з метою нейтралізації причетних до неї суб'єктів загрози.

Таблиця 2

Характеристика методів та інструментів у кібербезпеці

Інструмент/ метод	Функція в кібербезпеці	Приклади
Збір даних	Збір даних із різних джерел (інтернет-провайдери, форуми, темний інтернет)	Інтернет-провайдери, соціальні мережі, канали аналітики загроз
Обробка та перевірка даних	Фільтрація, нормалізація та підготовка даних до аналізу	Дедуплікація, фільтрація аномалій, методи нормалізації
Інструменти аналізу даних	Аналіз, візуалізація та моніторинг великих наборів даних	Splunk, ELK Stack, Wireshark
Інтеграція штучного інтелекту	Покращення аналітики за допомогою машинного навчання та NLP	IBM QRadar, NLP для аналізу соціальних мереж, розвідка загроз
Автоматизація	Автоматизація реагування на загрози на основі інсайтів даних	Блокування IP-адрес, карантин пристроїв, сповіщення команд безпеки

Джерело: сформовано авторами на підставі [18–19]

Висновки. Штучний інтелект змінив методи роботи кіберполіції, пропонуючи своїм користувачам унікальні можливості для виявлення кіберзагроз, запобігання їм та реагування на небезпеку. Завдяки використанню машинного навчання, виявленню аномалій, NLP та інших інструментів на основі ШІ сили кіберполіції України успішно посилили свої заходи з цифрової безпеки, створивши безпечніше онлайн-середовище для громадськості.

Аналітика даних є основою сучасних заходів із кібербезпеки, особливо для правоохоронних органів, таких як кіберполіція України. За допомогою використання інструментів та методів аналізу даних кіберполіція здатна виявляти кіберзагрози в режимі реального часу, обробляти та аналізувати величезні масиви даних, а також запобігати кібератакам до того, як вони завдадуть значної шкоди. Інтеграція штучного інтелекту з аналітикою даних значно розширює можливості команд кібербезпеки, дозволяючи їм автоматизувати реагування та приймати рішення на основі даних, які покращують загальну безпеку їхніх мереж.

Література:

1. Tymchyshyn A., Zvonarov O., Mokhonko O., Postryhan V., Popovych O. Application of the method of computer forensic simulation of crimes in the course of an armed conflict. *Cuestiones Políticas.* 2022. № 40 (75). DOI: https://doi.org/10.46398/cuestpol.4075.22

2. Тимчишин А. М. Деякі аспекти використання спеціальних знань у розслідуванні кримінальних правопорушень. *Історико-правовий часопис.* 2023. № 20 (1). С. 119–125. DOI: https://doi.org/10.32782/2409-4544/2023-1/16

3. Зачек О. І., Дмитрик Ю. І., Сеник В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2023. № 3. С. 148–156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19

4. Гуцалюк М. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. *Інформація і право*. 2024. № 2 (49). С. 164–177.

5. Патрика А., Герасимчук О., Нємкова О., Савин Я., Дудикевич В. Розроблення методу дослідження кіберзлочинів за типом вірусів-вимагачів з використанням моделей штучного інтелекту в системі менеджменту інформаційної безпеки критичної інфраструктури. *Social Development and Security*. 2024. № 14 (2). С. 52–63. DOI: https://doi.org/10.33445/sds.2024.14.2.6

6. Голубенко О. І., Лемешко А. В., Поліщук А. Р., Кузьменко М. В., Дегтяров Є. О. Дослідження застосування штучного інтелекту у кібербезпеці. *ITSynergy*. 2023. № 2. С. 71–81. DOI: https://doi.org/10.53920/ITS-2023-2-5

7. Довгань В., Коцман І. Основні аспекти державної політики забезпечення протидії кіберзлочинності в Україні. *Актуальні питання у сучасній науці*. 2023. № 3 (9). С. 220–229. DOI: https://doi.org/10.52058/2786-6300-2023-3(9)

8. Добришин Ю. Використання статистичних методів щодо прогнозування фішингових атак. *Кібербезпека: освіта, наука, техніка.* 2024. № 3 (23). С. 56–70. DOI: https://doi.org/10.28925/2663-4023.2024.23.5670

9. Бугера О. І. Сучасний стан та проблеми використання новітніх інтернет-технологій для запобігання злочинності. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки.* 2022. № 33 (72). С. 65–69. DOI: https://doi.org/10.32782/TNU-2707-0581/2022.1/12

10. Кримінальне *право України. Особлива частина : навч. посіб. / за заг. ред. О. М. Литвинова. Харків : Право, 2020. 656 с*

11. Недашківська О. А., Недашківська Т. Є. Експеримент як засіб дослідження когніції судового експерта щодо експертної ініціативи. *Криміналістичний вісник.* 2022. № 1 (37). С. 79–89. DOI: https://doi.org/10.37025/1992-4437/2022-37-1-79

12. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 8. С. 28–35. DOI: https://doi.org/10.31470/2786-6246-2024-8-28-35

13. Мельник О. Використання штучного інтелекту для кібербезпеки. *Наука і техніка сьогодні*. 2024. № 7 (35). С. 871–882. DOI: https://doi.org/10.52058/2786-6025-2024-7(35)-871-882

14. Гончарук О. М., Ісмайлов К. Ю. Кримінальний аналіз у системі правоохоронних органів України: поняття, мета й завдання. *Правовий часопис Донбасу*. 2023. № 2. С. 3–9. DOI: https://doi.org/10.32782/2523-4269-2023-83-3-9

15. Логвинський Г. В. Родовий об'єкт для посягання на захисника чи представника особи. *Нове українське право*. 2021. № 3. С. 249–254. DOI: https://doi.org/10.51989/NUL.2021.3.36

16. Користін О. Є., Демедюк С. В., Панченко Є. В., Користін О. О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис.* 2023. № 3. С. 53–59. DOI: https://doi.org/10.32850/sulj.2023.3.10

17. Самойленко О. А., Тітуніна К. В. Інтернет-шахрайства: технології вчинення, шляхи протидії та запобігання. *ScienceRise: Juridical Science*. 2021. № 2 (16). С. 65–70. DOI: 10.15587/2523-4153.2021.235769

18. Бурда А. С., Прудіус М. А., Стефанюк Я. Г., Фомічов О. О. Методи обробки та інтелектуального аналізу даних з використанням штучних імунних систем. *Національний університет «Полтавська політехніка імені Юрія Кондратюка».* 2024. № 3 (77). С. 93–96. DOI: 10.26906/SUNZ.2024.3.93

19. Шевченко С., Жданова Ю., Складанний П., Спасітєлєва С. Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*. 2021. № 1 (13). С. 133–144. DOI: https://doi.org/10.28925/2663-4023.2021.13.133144

References:

1. Tymchyshyn, A., Zvonarov, O., Mokhonko, O., Postryhan, V., & Popovych, O. (2022). Application of the method of computer forensic simulation of crimes in the course of an armed conflict. *Cuestiones Políticas,* 40 (75). DOI: https://doi.org/10.46398/cuestpol.4075.22

2. Tymchyshyn, A. M. (2023). Deiaki aspekty vykorystannia spetsialnykh znan u rozsliduvanni kryminalnykh pravoporushen [Certain Aspects of the Use of Specialized Knowledge in the Investigation of Criminal Offenses]. *Istoryko-pravovyi chasopys – Historical and Legal Chronicle,* 20 (1), 119–125. DOI: https://doi.org/10.32782/2409-4544/2023-1/16 [in Ukrainian].

3. Zachek, O. I., Dmytryk, Yu. I., & Senyk, V. V. (2023). Rol shtuchnoho intelektu v pidvyshchenni efektyvnosti pravookhoronnoi diialnosti [The Role of Artificial Intelligence in Enhancing the Efficiency of Law Enforcement Activities]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia yurydychna – Scientific Bulletin of Lviv State University of Internal Affairs. Legal Series,* 3, 148–156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19 [in Ukrainian].

4. Hutsalyuk, M. (2024). Stratehiyi protydiyi suchasnym kiberzahrozam ta zabezpechennya kiberstiikosti krytychnoyi infrastruktury Ukrayiny [Strategies for Countering Modern Cyber Threats and Ensuring Cyber Resilience of Critical Infrastructure in Ukraine]. *Informatsiya i pravo – Information and Law,* 2 (49), 164–177 [in Ukrainian].

5. Patryka, A., Herasymchuk, O., Niemkova, O., Savyn, Ya., & Dudykevych, V. (2024). Rozroblennia metodu doslidzhennia kiberzlochyniv za typom virusiv-vymahachiv z vykorystanniam modelei shtuchnoho intelektu v systemi menedzhmentu informatsiinoi bezpeky krytychnoyi infrastruktury [Development of a Method for Investigating Cybercrimes Related to Ransomware Viruses Using Artificial Intelligence Models in the Information Security Management System of Critical Infrastructure]. *Social Development and Security,* 14 (2), 52–63. DOI: https://doi.org/10.33445/sds.2024.14.2.6 [in Ukrainian].

6. Holubenko, O. I., Lemeshko, A. V., Polishchuk, A. R., Kuzmenko, M. V., & Dehtyarov, Ye. O. (2023). Doslidzhennya zastosuvannya shtuchnoho intelektu u kiberbezpetsi [Research on the Application of Artificial Intelligence in Cybersecurity]. *ITSynergy,* 2, 71–81. DOI: https://doi.org/10.53920/ITS-2023-2-5 [in Ukrainian].

7. Dovhan, V., & Kotsman, I. (2023). Osnovni aspekty derzhavnoyi polityky zabezpechennya protydiyi kiberzlochynnosti v Ukrayini [Key Aspects of State Policy on Combating Cybercrime in Ukraine]. *Aktualni pytannia u suchasnii nautsi – Current Issues in Modern Science,* 3 (9), 220–229. DOI: https://doi.org/10.52058/2786-6300-2023-3(9) [in Ukrainian].

8. Dobryshyn, Yu. (2024). Vykorystannya statystychnoho metodiv shchodo prohnozuvannya fishynhovykh atak [Use of Statistical Methods for Predicting Phishing Attacks]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technology,* 3 (23), 56–70. DOI: https://doi.org/10.28925/2663-4023.2024.23.5670 [in Ukrainian].

9. Buhera, O. I. (2022). Suchasnyi stan ta problemy vykorystannya novitnikh internet-tekhnolohii dlya zapobihannya zlochynnosti [Current State and Issues of Using Advanced Internet Technologies for Crime Prevention]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: yurydychni nauky – Scientific Notes of V. I. Vernadsky Taurida National University. Series: Legal Sciences,* 33 (72), 65–69. DOI: https://doi.org/10.32782/TNU-2707-0581/2022.1/12 [in Ukrainian].

10. *Kryminalne pravo Ukrainy. Osoblyva chastyna : navch. posib. [Criminal law of Ukraine. Special part: education. manual]* (2020). In O. M. Litvynova (Ed.). Kharkiv: Pravo.

11. Nedashkivska, O. A., & Nedashkivska, T. Ye. (2022). Eksperyment yak zasib doslidzhennya kohnitsiyi ssudovoho eksperta shchodo ekspertnoi initsiatyvy [Experiment as a Means of Studying the Cognition of a Forensic Expert Regarding Expert Initiative]. *Kryminalistychnyi visnyk – Criminalistic Bulletin,* 1 (37), 79–89. DOI: https://doi.org/10.37025/1992-4437/2022-37-1-79 [in Ukrainian].

12. Vovk, A. (2024). Suchasni problemy publichnoho upravlinnya zabezpechennyam kiberbezpeky v Ukrayini [Current Issues in Public Administration of Cybersecurity in Ukraine]. *Publichne upravlinnya: kontseptsii, paradyhma, rozvytok, udoskonalennya – Public Administration: Concepts, Paradigms, Development, Improvement,* 8, 28–35. DOI: https://doi.org/10.31470/2786-6246-2024-8-28-35 [in Ukrainian].

13. Melnyk, O. (2024). Vykorystannya shtuchnoho intelektu dlya kiberbezpeky [Use of Artificial Intelligence for Cybersecurity]. *Nauka i tekhnika sohodni – Science and Technology Today*, 7 (35), 871–872. DOI: https://doi.org/10.52058/2786-6025-2024-7(35)-871-882 [in Ukrainian].

14. Honcharuk, O. M., & Ismailov, K. Yu. (2023). Kryminalnyi analiz u systemi pravookhoronnykh orhaniv Ukrainy: poniattia, meta y zavdannia [Criminal Analysis in the System of Law Enforcement Agencies of Ukraine: Concepts, Goals, and Objectives]. *Pravovyi chasopys Donbasu – Legal Journal of Donbas,* 2, 3–9. DOI: https://doi.org/10.32782/2523-4269-2023-83-3-9 [in Ukrainian].

15. Lohvynskyi, H. V. (2021). Rodovyi obiekt dlia posiahannia na zakhysnyka chy predstavnyka osoby [Generic Object for Attacks on a Defender or Representative of a Person]. *Nove ukrayinske pravo – New Ukrainian Law,* 3, 249–254. DOI: https://doi.org/10.51989/NUL.2021.3.36 [in Ukrainian].

16. Korystin, O. Ye., Demedyuk, S. V., Panchenko, Ye. V., & Korystin, O. O. (2023). Natsionalni realii analizu kiberzlochynnosti za metodolohiieiu Yevropolu IOSTA [National Realities of Cybercrime Analysis According to the Methodology of Europol IOCTA]. *Pivdennoukrayins'kyi pravnychyi chasopys – Southern Ukrainian Legal Journal,* 3, 53–59. DOI: https://doi.org/10.32850/sulj.2023.3.10 [in Ukrainian].

17. Samoylenko, O. A., & Titunina, K. V. (2021). Internet-shakhrajstva: tekhnolohiyi vchynennya, shlyakhy protydiyi ta zapobihannya [Internet Fraud: Methods of Commission, Countermeasures, and Prevention]. *ScienceRise: Juridical Science*, 2 (16), 65–70. DOI: https://doi.org/10.15587/2523-4153.2021.235769 [in Ukrainian].

18. Burda, A. S., Prudius, M. A., Stefanyuk, Ya. H., & Fomichov, O. O. (2024). Metody obrobky ta intelektualnoho analizu danykh z vykorystanniam shtuchnykh imunnykh system [Methods of Data Processing and Intelligent Analysis Using Artificial Immune Systems]. *Natsionalnyi universytet «Poltavska politekhnika imeni Yuriia Kondratiuka» – National University Poltava Polytechnic named after Yuriy Kondratyuk,* 3 (77), 93–96. DOI: https://doi.org/10.26906/SUNZ.2024.3.93 [in Ukrainian].

19. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., & Spasitielieva, S. (2021). Matematychni metody v kiberbezpetsi: hrafy ta yikh zastosuvannya v informatsiyniy ta kibernetychniy bezpezi [Mathematical Methods in Cybersecurity: Graphs and Their Applications in Information and Cybersecurity]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technology*, 1 (13), 133–144. DOI: https://doi.org/10.28925/2663-4023.2021.13.133144 [in Ukrainian].