Львівський державний університет внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

20 грудня 2024 року

Львів 2025

УДК 004

І 78

Рекомендовано до розміщення в електронних сервісах ЛьвДУВС Вченою радою Львівського державного університету внутрішніх справ (протокол № 12 від 28.01.2025)

МОЗОЛЬ Станіслав – проректор, доктор юридичних наук, професор;

АНДРУСИШИН Роман – кандидат юридичних наук, доцент;

ВЕРБИЦЬКИЙ Петро – кандидат наук із соціальних комунікацій;

ФЕДЧАК Ігор – доктор юридичних наук, доцент;

ПОЛЯК Святослав – доктор філософії у галузі знань «Право»;

ЗАЧЕК Олег – кандидат технічних наук, доцент;

МОВЧАН Анатолій – доктор юридичних наук, професор;

ОГІРКО Ольга – кандидат технічних наук, доцент;

РУДИЙ Тарас – кандидат технічних наук, доцент;

МУСІЙОВСЬКА Мар’яна – кандидат технічних наук;

Д’ЯКОВ Андрій – кандидат технічних наук;

ГАЛАЙКО Наталія;

МАГЕРОВСЬКА Тетяна – кандидат фізико-математичних наук, доцент (відповідальний секретар).

І 78 **Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України**: матеріали Науково-практичної конференції (Львів, 20 грудня 2024) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2025. – 137 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України», що проводилася 20 грудня 2024 року у Львівському державному університеті внутрішніх справ.

УДК 004

Опубліковано в авторській редакції

© Львівський державний університет внутрішніх справ, 2025

Абзалов Денис Владиславович

курсант 2-го курсу факультету №3 Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, факультету №3 Донецького державного університету внутрішніх справ, доктор філософії, доцент

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЇНОГО ЗАБЕЗПЕЧЕННЯ СЕКТОРУ ОБОРОНИ УКРАЇНИ

Кібербезпека є одним із ключових компонентів сучасної системи інформаційної безпеки, особливо в контексті обороноздатності держави. Для України, яка перебуває під постійним тиском кіберзагроз, ефективний кіберзахист відіграє критичну роль у забезпеченні національної безпеки та стійкості державних інституцій.

Кібербезпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави у кіберпросторі. Її досягнення можливе завдяки системному впровадженню правових, організаційних та технічних заходів, спрямованих на мінімізацію ризиків, пов'язаних із використанням інформаційних технологій.

З початком повномасштабної агресії росії проти України кількість і масштаб кібератак суттєво зросли. Згідно з даними урядової команди CERT-UA, у другій половині 2023 року було зафіксовано та розслідувано 1,46 тисячі кіберінцидентів. Основними цілями атак стали міністерства, органи державної влади та об'єкти критичної інфраструктури. Зокрема, урядові організації зазнали атак 347 разів, місцеві органи влади – 276 разів, установи сектору безпеки та оборони – 175 разів, а комерційні організації – 127 разів. Особливу увагу хакери приділили енергетичному сектору (92 атаки), телекомунікаційному сектору (81 атака), освітнім закладам (38 атак), транспортній галузі (32 атаки) та фінансовому сектору (30 атак). Значні ризики також відчули IT-сектор (25 атак), засоби масової інформації (15 атак) і медичні установи (12 атак) [1].

Напередодні повномасштабного вторгнення, у січні 2022 року, кібератаки із застосуванням шкідливого програмного забезпечення, зокрема WhisperGate, завдали шкоди сайтам урядових установ України, зокрема Міністерству закордонних справ та Міністерству освіти. У жовтні 2022 року хакерська група Sandworm здійснила синхронізовану атаку на енергетичну систему України, поєднавши її з ракетними ударами, що призвело до пошкодження низки підстанцій.

Протягом війни активно використовувалися програми-вимагачі, такі як Caddy-Wiper і SwiftSlicer, метою яких було знищення даних. Масштабні DDoS-атаки, наприклад, на Київстар у грудні 2023 року, спричинили перебої у зв’язку для мільйонів користувачів. Додатково російські хакери застосовували методи дезінформації, включаючи злами медіа, поширення фейкових новин через соцмережі та фішингові розсилки [2].

Забезпечення кібербезпеки в Україні потребує комплексного підходу, який охоплює аспекти зазначені у Таблиці 1.

Отже, кібербезпека є фундаментальним компонентом інформаційної підтримки оборонного сектору України, особливо в умовах сучасних загроз, таких як кібертероризм, інформаційні війни та гібридні атаки. Надійний кіберзахист критично важливих

інфраструктур і військових систем забезпечує не лише збереження національної безпеки, але й ефективну адаптацію до зовнішніх викликів, що постають перед державою. З огляду на стрімкий розвиток технологій, постійне вдосконалення стратегій, методів та ресурсів кіберзахисту є ключовою умовою для забезпечення ефективності протидії кібератакам.

Табл 1. Забезпечення кібербезпеки в Україні

Категорія	**Результат**
Законодавство	Удосконалення нормативної бази відповідно до міжнародних стандартів (NIST, ISO 27001) та впровадження чіткої стратегії кібербезпеки.
Технології	Використання сучасних засобів захисту (шифрування, багаторівнева автентифікація), розробка національного ПЗ та систем моніторингу загроз.
Освіта	Підготовка фахівців через освітні програми й навчання, підвищення цифрової грамотності та регулярні симуляції для перевірки готовності до інцидентів.
Міжнародна співпраця	Участь у програмах NATO та міжнародних кібернавчаннях, обмін досвідом та інформацією про загрози.
Критична інфраструктура	Захист ключових секторів (енергетика, транспорт), впровадження резервних систем для безперервної роботи.
Боротьба з дезінформацією	Створення платформ для перевірки фактів, моніторинг та блокування шкідливих ресурсів.

Інтеграція заходів кібербезпеки з іншими складовими національної оборони створює потужну платформу для зміцнення безпеки держави. Важливо, щоб розвиток кібербезпеки розглядався як один із пріоритетів державної політики, оскільки саме він є вирішальним для забезпечення стабільності, стійкості та суверенітету України в умовах глобалізованого світу. Ефективне впровадження кіберзахисту стає не лише засобом протидії сучасним загрозам, а й важливим елементом формування технологічно оснащеної та адаптивної системи національної безпеки.

Література

1. Названа кількість кібератак в Україні за минулий рік. URL: https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik
2. Гендиректор «Київстару»: IT – інфраструктура компанії частково зруйнована внаслідок хакерської атаки. URL: https://ms.detector.media/withoutsection/post/33724/2023-12-12-gendyrektor-kyivstaru-it-infrastruktura-kompanii-chastkovo-zruynovana-vnaslidok-khakerskoi-ataky/

Абрамов Сергій Олексійович

старший науковий співробітник науково-дослідної лабораторії з підготовки військ Київського інституту Національної гвардії України, кандидат технічних наук, доцент

Кравченко Сергій Афанасійович

науковий співробітник науково-дослідної лабораторії з підготовки військ Київського інституту Національної гвардії України, кандидат біологічних наук, старший науковий співробітник

КІБЕРБЕЗПЕКА ЯК НЕВІД'ЄМНА СКЛАДОВА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СЕКТОРУ ОБОРОНИ УКРАЇНИ

У сучасних умовах розвитку інформаційного суспільства та зростання цифрових технологій питання кібербезпеки набувають стратегічного значення для забезпечення національної безпеки України. Сектор оборони стикається з постійно зростаючими кіберзагрозами, що спрямовані на порушення функціонування інформаційних систем, викрадення конфіденційних даних та дестабілізацію роботи ключових інфраструктур.

Гібридна війна, яку веде Російська Федерація проти України, значно підвищила ризики та інтенсивність кібернападів. Ворог активно застосовує методи кібершпигунства, інформаційних атак і дезінформації, що ставить під загрозу цілісність та ефективність оборонних операцій.

Розвиток кібербезпеки в секторі оборони України є важливим елементом інтеграції країни у систему колективної безпеки НАТО, де захист інформаційного простору є одним із ключових напрямків діяльності. Забезпечення кіберстійкості та протидія сучасним кіберзагрозам вимагають впровадження новітніх технологій, підготовки кваліфікованих фахівців, розробки сучасних нормативно-правових актів та посилення міжнародної співпраці. Таким чином, питання кібербезпеки є надзвичайно актуальним у контексті підвищення обороноздатності України та забезпечення надійності інформаційного простору у протистоянні сучасним викликам і загрозам.

Згідно закону України кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Методологія аналізу кібербезпеки як невід'ємна складова інформаційного забезпечення сектору оборони України може включати наступні етапи дослідження:

1. Визначення об'єкта та предмета дослідження. В якості об'єкту дослідження є система кібербезпеки сектору оборони України. В той же час, предмет дослідження – механізми, методи та засоби забезпечення кібербезпеки в умовах сучасних викликів і загроз.
2. Мета дослідження – оцінка сучасного стану, проблем і перспектив розвитку кібербезпеки у секторі оборони України може включати на наступних завданнях: вивчення сучасних кіберзагроз і викликів, що впливають на сектор оборони; аналіз нормативно-правової бази України у сфері кібербезпеки; оцінка технологій та інструментів, що використовуються для захисту інформаційного простору оборонного сектору та розробка рекомендацій щодо вдосконалення системи кіберзахисту.

3. Методи дослідження. До основних методів дослідження запропоновано включити наступні: теоретичний аналіз; порівняльний аналіз; емпіричні методи; методи моделювання та прогнозування та статистичний аналіз. Теоретичний аналіз: вивчення літератури, наукових статей, нормативних документів та звітів з питань кібербезпеки. Порівняльний аналіз: аналіз міжнародного досвіду у сфері кіберзахисту (зокрема, досвід НАТО). Емпіричні методи: проведення опитувань і інтерв'ю з фахівцями сектору оборони. Аналіз реальних кіберінцидентів, що вплинули на оборонний сектор України. Методи моделювання та прогнозування: розробка моделей розвитку кіберзагроз і оцінка їх впливу на сектор оборони. Статистичний аналіз: збір і обробка даних про кількість та типи кіберінцидентів у секторі оборони.
4. Етапи аналізу: збір даних; аналіз стану; розробка рекомендацій; оцінка ефективності.
5. Очікувані результати. Отримання чіткого розуміння стану кібербезпеки у секторі оборони України, розробка практичних рекомендацій для вдосконалення системи кіберзахисту, визначення перспективних напрямів розвитку кібербезпеки з урахуванням міжнародного досвіду.

Методологія аналізу дозволяє системно підійти до вивчення проблеми кібербезпеки, забезпечуючи наукову обґрунтованість отриманих результатів та рекомендацій.

До основних перспективних напрямків розвитку кібербезпеки як невід'ємна складова інформаційного забезпечення сектору оборони України потрібно віднести: розробку і впровадження національних стандартів кібербезпеки; посилення кіберстійкості критично важливої інфраструктури оборонного сектору; розвиток системи кіберрозвідки та контррозвідки; підготовка кваліфікованих кадрів у сфері кібербезпеки; використання новітніх технологій для забезпечення кіберзахисту; посилення міжнародної співпраці у сфері кібербезпеки; підвищення рівня обізнаності про кіберзагрози серед персоналу оборонного сектору; розробка систем оперативного реагування на кіберінциденти.

Розробка і впровадження національних стандартів кібербезпеки, з метою гармонізації українського законодавства із міжнародними стандартами у сфері кіберзахисту та створення єдиної платформи для моніторингу кіберзагроз і координації між державними та приватними структурами.

Посилення кіберстійкості критично важливої інфраструктури оборонного сектору, за рахунок впровадження багаторівневих систем захисту інформаційних мереж та захисту баз даних, що містять стратегічну інформацію, від атак із застосуванням штучного інтелекту.

Розвиток системи кіберрозвідки та контррозвідки, а саме використання інструментів відкритої розвідки (OSINT) для ідентифікації кіберзагроз та автоматизація збору, аналізу та прогнозування дій кіберзловмисників.

Підготовка кваліфікованих кадрів у сфері кібербезпеки, за рахунок створення спеціалізованих навчальних програм для військових і цивільних фахівців та організація навчань і тренувань із симуляцією кіберінцидентів.

Використання новітніх технологій для забезпечення кіберзахисту, з метою інтеграції штучного інтелекту та машинного навчання для виявлення аномалій у мережах та впровадження блокчейн-технологій для захисту комунікацій і передачі даних.

Підвищення рівня обізнаності про кіберзагрози серед персоналу оборонного сектору, за рахунок розробка освітніх кампаній із кібергігієни для військових та адміністративних працівників та інтеграції базових знань із кіберзахисту в регулярну підготовку військових.

Розробка систем оперативного реагування на кіберінциденти, з метою створення спеціалізованих центрів кіберзахисту, які здатні швидко реагувати на загрози та впровадження автоматизованих систем для аналізу та ліквідації наслідків атак.

Перелічені вище перспективні напрями розвитку кібербезпеки як невід'ємна складова інформаційного забезпечення сектору оборони України сприятимуть зміцненню кібербезпеки сектору оборони України та забезпеченню інформаційної стійкості в умовах сучасних загроз.

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Дата оновлення: 28.06.2024 URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 12.12.2024)

Бігун Маріанна

здобувач вищої освіти спеціальності 126 «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Галайко Наталія Володимирівна

старший викладач кафедри інформаційних систем та технологій Львівського державного університету внутрішніх справ

ВПЛИВ КВАНТОВИХ ОБЧИСЛЕНЬ НА ОБРОБКУ ДАНИХ І СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Сучасна галузь інформаційних систем стоїть на порозі нової епохи, в якій квантові технології відіграють ключову роль. Вони представляють новий клас інструментів, здатних радикально трансформувати традиційні підходи до обробки даних та забезпечення безпеки. Квантові комп'ютери та криптографія відкривають перспективи, які можуть суттєво підвищити ефективність систем управління даними, розширити можливості аналізу та забезпечити безпрецедентний рівень захисту інформації.

Значення цих технологій важко переоцінити, оскільки вони формують нові вектори розвитку у сфері інформаційних систем. На глобальному рівні спостерігається активне збільшення інвестицій у квантові дослідження, адже провідні країни, як-от США, Китай і країни ЄС, усвідомлюють стратегічну важливість цієї галузі та активно фінансують відповідні проєкти.

Квантові технології стають фундаментом для забезпечення технологічної переваги, оскільки вони пропонують революційні рішення у сфері обчислювальних потужностей і безпеки даних. Їхній вплив охоплює всі аспекти інформаційних систем, зокрема управління базами даних, розробку програмного забезпечення та оптимізацію інфраструктури.

Відмінною рисою квантової техніки є новий технологічний рівень, який дозволяє маніпулювати окремими квантовими об’єктами, зокрема: атомом; іоном; електроном; фотоном. Квантове обчислення визначається технологією, яка використовує квантово-механічні явища, такі як суперпозиція та заплутаність для виконання операцій над даними. Квантові комп’ютери будуються на квантових бітах або кубітах, які, на відміну від бітів традиційного комп’ютера, поєднують стани 0 і 1; обробляють великі обсяги даних з неймовірною швидкістю [1, с. 179]. Ця здатність проявляється завдяки своїм паралельним обчислювальним можливостям та має велике значення для обробки даних багатьох сферах (рис. 1).

Рис. 1. Квантові обчислення в обробці даних

Поруч з перевагами, які людство отримає у зв’язку з впровадженням квантових технологій, квантові обчислення стають однією з найбільших загроз для кібербезпеки. Ця потужна технологія, забезпечуючи революційні можливості, створює серйозний ризик для існуючих методів захисту даних.

Основними ризиками, які квантові комп’ютери створюють для кібербезпеки, є:

- Перехоплення та зловживання даними: зашифровані інформаційні потоки можуть бути вразливими до зламів за допомогою квантових технологій.
- Атаки «Зберіть зараз, розшифруйте пізніше»: зловмисники можуть накопичувати зашифровані дані сьогодні, з метою їх дешифрування у майбутньому, коли квантові комп’ютери стануть достатньо потужними.
- Порушення критично важливих систем: відсутність переходу на квантово-захищені алгоритми створює ризик атак на ключові бізнес-функції та інфраструктуру в таких сферах, як охорона здоров’я, фінансовий сектор і державне управління [2].

Усвідомлення цих викликів і своєчасна підготовка є критично важливими. З огляду на це, організації повинні негайно почати впроваджувати стратегії кібербезпеки, зокрема, адаптація систем до нових стандартів шифрування, стійких до квантових атак; впровадження квантового шифрування та розподілу ключів у захисну інфраструктуру; відстеження розвитку квантових технологій і перевірка нових криптографічних рішень для швидкого реагування на загрози.

Отже, квантові обчислення є водночас значним проривом і серйозним викликом, здатним революціонізувати обчислювальні процеси та поставити під загрозу сучасні системи кібербезпеки. Квантові технології відкривають нові можливості, сприяючи економічній ефективності, науково-технічному прогресу та покращенню якості життя. Однак, попри ці переваги, вони несуть і значні ризики. Саме тому організаціям слід уже сьогодні усвідомлювати ці загрози та впроваджувати квантово-захищені стратегії для забезпечення своєї безпеки в майбутньому.

Література

1. Корж Роман. Технологічні інновації епохи квантової економіки. Development Service Industry Management, (3), 2023, 178-182. https://doi.org/10.31891/dsim-2023-3(26).
2. Квантові обчислення: неминуча загроза інформаційній безпеці. URL: https://www.oksim.ua/2024/08/29/kvantovi-obchislennya-neminucha-zagroza-informaczijnij-bezpeczi/

Білас Христина Іванівна

курсант 3-го курсу, ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

в.о. завідувача кафедри оперативно-розшукової діяльності, ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ПСИХОЛОГІЧНОМУ ЗАБЕЗПЕЧЕННІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Сучасний світ переживає період стрімкого розвитку інформаційних технологій, що активно впливають на всі сфери життя, зокрема на правоохоронну діяльність. Застосування новітніх інформаційних технологій у психологічному забезпеченні правоохоронних органів не лише покращує ефективність роботи, а й відкриває нові можливості для більш точного та обґрунтованого застосування психологічних методів. Вони допомагають в аналізі поведінки правопорушників, організації психологічної підтримки правоохоронців, виявленні кримінальних тенденцій та розробці профілактичних заходів. Таким чином, враховуючи важливість психології в правозастосуванні, інновації в інформаційних технологіях стають не лише інструментом, а й необхідним елементом для досягнення більшої ефективності роботи правоохоронних органів. Тому потрібно визначити роль інформаційних технологій у психологічному забезпеченні правоохоронної діяльності.

Перш за все відмічаємо, що психологічне забезпечення правоохоронної діяльності включає різноманітні аспекти, такі як взаємодія правоохоронців з громадянами, аналіз психологічного стану підозрюваних та свідків, психологічна підтримка співробітників поліції та інших органів. Інформаційні технології відіграють важливу роль у всіх цих процесах, оскільки дозволяють швидше та точніше обробляти велику кількість даних, автоматизувати багато процесів і впроваджувати нові методи аналізу [1, с. 37].

Сучасні інформаційно-аналітичні системи допомагають правоохоронним органам проводити глибокий аналіз поведінки осіб, що мають певний зв’язок з кримінальною діяльністю. Це дозволяє збирати й обробляти дані про кримінальні події, взаємодіючи з базами даних на національному та міжнародному рівнях. Психологічні профілі осіб, що стали жертвами чи кривдниками, можуть бути оброблені за допомогою спеціальних програмних засобів, що допомагають ідентифікувати потенційно небезпечних осіб або створити передбачуваний профіль злочинця.

Отже, можемо констатувати, що використання технологій для психологічного профілювання злочинців відкриває нові горизонти у правоохоронній діяльності. Завдяки аналізу поведінкових патернів, використовуючи алгоритми машинного навчання, можна створювати точніші прогнози щодо можливих дій підозрюваних. Це допомагає не тільки в розслідуваннях, але й у попередженні злочинів, адже психологічний профіль злочинця дозволяє передбачити ймовірні місця й способи скоєння правопорушень.

Разом з тим, зауважимо, що інформаційні технології значно покращили взаємодію між правоохоронцями та психологами, а також спростили обмін інформацією між різними підрозділами. Вони дозволяють організувати ефективну систему консультативної підтримки, в тому числі у випадках, коли необхідна оперативна психологічна допомога або підготовка правоохоронців до стресових ситуацій. Психологи можуть отримувати доступ до результатів психологічних тестів, аналізу поведінки осіб, що проходять через правоохоронні органи, на основі чого швидше й точніше коригувати методи впливу [2, с. 77].

Для психологічної підготовки правоохоронців застосовуються віртуальні тренажери, які дозволяють їм у безпечному середовищі тренувати реакцію на стресові ситуації, відпрацьовувати взаємодію з громадянами та зберігати спокій у критичних ситуаціях. Це важливо для того, щоб співробітники правоохоронних органів могли реагувати на екстремальні ситуації без негативних емоційних наслідків. Завдяки інформаційним технологіям, правоохоронці можуть використовувати спеціалізовані програми для оцінки свого емоційного стану та визначення рівня стресу. Це дає змогу вчасно виявити проблеми, пов'язані з перенавантаженням або емоційним вигоранням, і вживати заходів щодо психологічної реабілітації.

Для постійного моніторингу психологічного стану співробітників правоохоронних органів використовуються мобільні додатки, які дають змогу у реальному часі відслідковувати психологічні показники, збирати дані про емоційний стан співробітників і при необхідності консультуватися з психологами або направляти на реабілітацію.

Психологічне забезпечення правоохоронної діяльності також включає роботу з громадянами, особливо в ситуаціях, що потребують надання правової або психологічної допомоги. Інформаційні технології дають змогу організувати ефективну взаємодію з населенням, забезпечуючи швидкий доступ до інформації та надання послуг.

За допомогою Інтернет-технологій громадяни можуть отримати консультації з юридичних і психологічних питань без необхідності відвідувати відділення правоохоронних органів. Такі послуги допомагають людям, які постраждали від злочинів, швидко отримувати необхідну допомогу та психологічну підтримку. Онлайн-платформи дозволяють розширити доступ до консультацій та підтримки для широкої аудиторії.

Мобільні додатки, які дозволяють громадянам швидко зв'язатися з правоохоронними органами, викликати поліцію або екстрену допомогу, є ще однією важливою

складовою психологічного забезпечення. Вони не тільки надають допомогу в екстремальних ситуаціях, а й забезпечують психологічну підтримку жертвам злочинів, допомагаючи їм відчувати себе безпечніше [3, с. 79].

Таким чином, інформаційні технології стали незамінним інструментом у психологічному забезпеченні правоохоронної діяльності. Вони дозволяють не лише підвищити ефективність роботи правоохоронних органів, а й покращити умови для психологічної підтримки як самих працівників, так і громадян. Створення нових технологічних рішень для психологічної підтримки та аналізу поведінки відкриває нові горизонти в досягненні більшої безпеки в суспільстві та покращенні взаємодії між правоохоронцями та громадянами. З розвитком технологій очікується, що в майбутньому роль інформаційних технологій у психологічному забезпеченні правоохоронної діяльності буде тільки зростати. Очікується подальший розвиток віртуальних тренажерів, а також використання штучного інтелекту для більш точного аналізу психологічних профілів осіб, що мають стосунок до кримінальних подій. Більш активне використання технологій дозволить правоохоронцям оперативніше реагувати на ситуації та надавати необхідну психологічну підтримку всім учасникам процесу.

Література

1. Охріменко І. М., Александров Д. О., Дрозд О. Ю. Особливості професійно-психологічної адаптації працівників Національної поліції України до правоохоронної діяльності. Наука і освіта. 2017. № 11. С. 35-45.
2. Зінченко Д.А, Гопко Д.О. Сучасні технології у сфері психологічного забезпечення працівників правоохоронних органів. Збірник Матеріалів IV міжнародної науково-практичної конференції Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів. (Київ, 31 жовтня 2023 року). С. 76-78.
3. Павлушенко С. Аналіз підходів до психологічного забезпечення професійної діяльності. Вісник Національного університету оборони України. 2020. Т. 55. № 2. С. 75-83.

Борецька Сніжана Миколаївна

курсант 3-го курсу, ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

в.о. завідувача кафедри оперативно-розшукової діяльності, ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

РОЛЬ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ УКРАЇНИ

Біометрична ідентифікація набуває дедалі більшого значення в інформаційно-аналітичному забезпеченні діяльності органів сектору безпеки та оборони України. У сучасному світі, де інформація є однією з ключових цінностей, інтеграція біометричних технологій у процеси збору, обробки та використання даних стає невід'ємною частиною ефективного функціонування силових структур. Впровадження таких технологій дозволяє не лише підвищити рівень безпеки, а й забезпечити оперативність і точність прийняття рішень.

Основним завданням біометричної ідентифікації є встановлення унікальності особи на основі її фізіологічних або поведінкових характеристик. В Україні до біометричних параметрів, що використовуються у секторі безпеки, належать відбитки пальців, зображення обличчя, аналіз голосу, сітківки ока та інші методи. У поєднанні з сучасними інформаційними системами ці дані створюють потужний інструмент для ідентифікації, верифікації та моніторингу як громадян, так і осіб, що становлять загрозу національній безпеці.

В умовах воєнного стану та постійних загроз територіальній цілісності України біометричні технології демонструють свою ефективність у розв'язанні низки завдань. Одним із таких є ідентифікація осіб, які намагаються приховати свою особу або використовують фальшиві документи. Завдяки інтеграції біометричних даних до систем прикордонного контролю, правоохоронні органи отримують можливість швидкого і точного виявлення таких випадків. Це, у свою чергу, сприяє зміцненню обороноздатності держави [2].

Не менш важливим є застосування біометричної ідентифікації у військових операціях. Наприклад, під час розслідування злочинів у зоні бойових дій ідентифікація тіл загиблих військовослужбовців та цивільних осіб, здійснена за допомогою біометричних технологій, дозволяє родинам отримати важливу інформацію про долю їхніх близьких. Крім того, використання біометричних даних у системах військового обліку сприяє чіткій організації мобілізаційних процесів і моніторингу військовозобов'язаних.

Ще однією ключовою сферою використання біометричних технологій є боротьба з тероризмом та організованою злочинністю. Сучасні системи розпізнавання обличчя та аналізу відбитків пальців дозволяють оперативно встановлювати зв'язки між підозрюваними, виявляти злочинні мережі та попереджати терористичні акти. У контексті транскордонної злочинності це стає особливо актуальним, оскільки Україна активно співпрацює з міжнародними партнерами у сфері обміну даними для протидії глобальним загрозам [1].

Водночас впровадження біометричних технологій викликає чимало дискусій щодо правових та етичних аспектів їхнього використання. З одного боку, застосування біометрії потребує високого рівня захисту персональних даних, оскільки витік такої інформації може призвести до серйозних наслідків для безпеки особи. З іншого боку, надмірний контроль над біометричними даними може породжувати ризики зловживань з боку державних структур. Таким чином, необхідно розробляти збалансовану правову базу, яка б забезпечувала ефективне використання біометричних технологій без шкоди для прав і свобод громадян.

Україна поступово інтегрує біометричні технології у свої державні системи. Наприклад, система «Безпечне місто» використовує розпізнавання обличь для моніторингу громадського порядку у великих містах. Крім того, біометричні дані активно застосовуються у процесах видачі паспортів нового зразка, що дозволяє значно підвищити рівень довіри до українських документів на міжнародному рівні. Однак для досягнення повного потенціалу біометричних технологій необхідно інвестувати у розвиток технічної інфраструктури, навчання кадрів та вдосконалення законодавства [3].

Окремо варто зупинитися на перспективах розвитку біометричної ідентифікації у секторі безпеки та оборони. Зокрема, використання штучного інтелекту у поєднанні з біометричними даними відкриває нові можливості для автоматизації процесів аналізу великих масивів інформації. Такі системи можуть прогнозувати поведінку потенційних порушників, ідентифікувати аномалії у великих базах даних та оптимізувати процеси

прийняття рішень. Наприклад, виявлення підозрілих осіб у натовпі за допомогою алгоритмів машинного навчання вже сьогодні є реальністю для багатьох країн.

Однак технологічний прогрес вимагає також відповідного оновлення нормативно-правової бази. У контексті інтеграції України до європейської спільноти особливе значення має гармонізація національного законодавства із загальноприйнятими стандартами ЄС. Це стосується не лише захисту персональних даних, а й забезпечення належного рівня прозорості у використанні біометричних технологій органами безпеки.

Таким чином, інформаційно-аналітичне забезпечення діяльності органів сектору безпеки та оборони України у поєднанні з біометричною ідентифікацією є перспективним напрямом, що сприяє підвищенню ефективності управлінських рішень, боротьбі з злочинністю та зміцненню національної безпеки. Успішна інтеграція цих технологій потребує зваженого підходу, який враховуватиме як технічні, так і правові аспекти їх використання.

Література

1. Розумний, С. М. Судова експертиза як ключовий інструмент забезпечення національної безпеки. 2024 р. URL: https://er.dduvs.edu.ua/bitstream/123456789/13860/1/14.pdf (дата звернення: 11.12.2024 року)
2. Негребецький, В. В. Роль цифрової трансформації органів кримінальної юстиції в підвищенні ефективності розслідування воєнних злочинів в Україні. 2022 р.URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/431/11491/24054-1?inline=1(дата звернення: 11.12.2024 року)
3. Єпринцева І.А. Актуальні питання криміналістичних обліків генетичних ознак людини. Молодий вчений. № 9 (85) (2020). URL: https://molodyivchenyi.ua/index.php/journal/article/view/703/679 (дата звернення: 11.12.2024 року)

Вергун Дмитро Сергійович

курсант 2-го курсу Факультету №3 Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, факультету №3 Донецького державного університету внутрішніх справ, доктор філософії, доцент

МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОБОРОННИХ ПРОЦЕСІВ

У сучасному світі інформація відіграє вирішальну роль у всіх сферах діяльності, особливо в оборонній сфері, де своєчасне отримання, обробка та використання даних визначають успіх операцій і загальну національну безпеку. Геополітична нестабільність, зростання кіберзагроз, активізація гібридних конфліктів та поширення сучасних технологій значно ускладнюють оборонні процеси. У таких умовах модернізація інформаційного забезпечення стає не лише бажаною, а й життєво необхідною для забезпечення ефективного управління військовими структурами, швидкого реагування на загрози та захисту критично важливої інформації.

Основними стратегічними цілями модернізації інформаційного забезпечення є створення умов для оперативного доступу до актуальних даних, інтеграція сучасних технологій у всі рівні оборонних структур, посилення кібербезпеки, підвищення рівня взаємодії між суб'єктами оборони та підтримка наукових досліджень у цій сфері. Перш за все, необхідно забезпечити доступ до інформації в реальному часі, що дозволить командним центрам швидко реагувати на зміни оперативної обстановки.

У процесі модернізації інформаційного забезпечення слід зосередитися на кількох ключових напрямках. Насамперед, це розробка цифрових платформ для управління обороннними процесами, автоматизація збору та обробки даних, використання технологій штучного інтелекту для аналізу загроз та прогнозування їхніх наслідків. Окремої уваги потребує вдосконалення систем розвідки та спостереження, зокрема супутникових технологій і безпілотних літальних апаратів. Крім того, важливо інтегрувати сучасні технології в єдину екосистему, яка забезпечить ефективну взаємодію всіх елементів оборонної системи.

Оборонна реформа, яка триває в Збройних Силах України, передбачає впровадження сучасних інформаційних систем (ІС), стандартів, доктрин і рекомендацій НАТО щодо управління військами, обороннними ресурсами та проведення оборонного планування. Одним із пріоритетних напрямів, направлених на підвищення ефективності оборонного планування та управління обороннними ресурсами є впровадження ІС управління обороннними ресурсами (Defense Resources Management Information System–DRMIS) [2]. Метою DRMIS є забезпечення органів військового управління інформаційно-аналітичною підтримкою прийняття рішень у сфері управління обороннними ресурсами за функціональними напрямами: особовий склад, організаційна структура, оборонне планування, матеріально-технічне забезпечення, медичне забезпечення, закупівлі, майно, фінанси та бюджет, адміністративна діяльність [1, 59].

Критичним елементом соціально-економічної безпеки будь-якої країни є Національна стратегія кібербезпеки (National Cybersecurity Strategy, NCS) [3]. Саме в ній кібербезпека та інформаційна безпека визнані як одні з головних пріоритетів у протидії загрозам національній безпеці. Кібербезпека займає ключове місце серед пріоритетів, адже сучасні конфлікти все частіше переносяться у цифровий простір. Захист інформаційних систем від зовнішніх і внутрішніх загроз є важливим аспектом стратегії національної безпеки. Також необхідно створити уніфіковані стандарти для забезпечення злагодженої роботи між військовими, цивільними та міжнародними партнерами. Підтримка наукових досліджень у сфері оборонної інформатики сприятиме розробці інноваційних рішень, що дозволять випереджати супротивника у технологічній гонці. Деталізацію реалізації Стратегії кібербезпеки відображено у щорічних планах уряду, в яких з боку органів влади передбачено заходи щодо запобігання і підготовки реагування на можливі кіберінциденти у рамках створення ефективної національної системи кібербезпеки [4, 151].

У сучасному світі, де військові конфлікти та оборонні стратегії еволюціонують з надзвичайною швидкістю, критично важливою стає потреба в адаптації та трансформації системи військової освіти [5, 467]. Створення та розвиток інтегрованого інтелектуального освітнього простору (E-learning) у рамках як формальної, так і неформальної військової освіти, що базується на досягненнях сучасних цифрових технологій і глибокій інтеграції цих технологій у повсякденне життя, видається особливо актуальним [5, 472]. Таким чином, інтеграція цифрових технологій в систему військової освіти не тільки сприятиме оптимізації навчального процесу та підвищенню ефективності

управління, але й забезпечить формування необхідних компетентностей у військовослужбовців, дозволяючи їм успішно адаптуватися та діяти в умовах інформаційного суспільства [5, 474].

Але слід зазначити, що процес модернізації інформаційного забезпечення супроводжується численними викликами та ризиками. Серед основних — високі фінансові витрати, необхідні для розробки і впровадження технологій, а також ризики кіберзагроз, які можуть виникати під час впровадження нових систем. Нестача кваліфікованих кадрів може стати значним бар'єром, а інертність організаційних структур уповільнити впровадження змін.

Очікуваними результатами модернізації стануть підвищення оперативності та точності управління оборонними процесами, ефективна протидія сучасним загрозам, а також зміцнення обороноздатності держави. У висновку сучасні технології дозволять скоротити час реагування, підвищити ефективність взаємодії між різними рівнями командування та сприяти інтеграції з міжнародними партнерами.

Література

1. Руденська, Г. В. (2020). Моделі та процеси життєвого циклу інформаційної системи управління оборонними ресурсами. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, 59-65.
2. Концепція інформатизації Міністерства оборони України : затв. наказом Міністра оборони України від 17.09.2014 р. No 650.
3. National Strategies. [Електронний ресурс]. Режим доступу: https://www.itu.int/en/ ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx
4. Трофименко, О. Г., Прокоп, Ю. В., Логінова, Н. І., & Задерейко, О. В. (2019). Кібербезпека України: аналіз сучасного стану. Ukrainian Information Security Research Journal, 21(3), 150-157.
5. Носенко, Ю. (2024). СУЧАСНІ ЦИФРОВІ ВИКЛИКИ В СИСТЕМІ ВІЙСЬКОВОЇ ОСВІТИ. Перспективи та інновації науки, (3 (37)).

Войтюк Олеся Романівна

здобувач вищої освіти спеціальності 126 «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Магеровська Тетяна Валеріївна

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

АНАЛІЗ ДАНИХ ТА НАДАННЯ ПІДТРИМКИ В ПРОЦЕСІ ПРИЙНЯТТЯ РІШЕНЬ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Анотація. Дана стаття досліджує важливість використання сучасних аналітичних методів і технологій для підтримки прийняття рішень у роботі правоохоронних органів. Особлива увага приділяється збору, обробці та аналізу великих обсягів даних, що дозволяють підвищити ефективність оперативної діяльності, виявляти кримінальні тенденції, прогнозувати злочинність та забезпечувати безпеку громадян. Стаття також

розглядає існуючі виклики та перспективи впровадження аналітичних інструментів у практику Національної поліції, зокрема в контексті автоматизації процесів та інтеграції з іншими державними структурами.

Вступ. Аналіз даних та підтримка ухвалення рішень є ключовими аспектами ефективного управління в діяльності Національної поліції України. Вони дозволяють поліції своєчасно отримувати необхідну інформацію для прийняття обґрунтованих рішень, що, в свою чергу, підвищувати ефективність їх роботи в умовах глобалізації та цифрових трансформацій. Це критично важливо для забезпечення належного виконання функцій поліції, що охоплюють не лише боротьбу зі злочинністю, а й покращення громадської безпеки та взаємодію з іншими державними органами.

Аналіз даних у контексті Національної поліції України є складним процесом, що охоплює кілька етапів. Початково здійснюється збір даних з різних джерел, як внутрішніх (звіти, бази даних) так і зовнішніх (ринкові дослідження, соціальні мережі), з використанням автоматизованих інструментів (веб-скрапінг, API) для ефективного збору великих обсягів інформації. На етапі обробки дані очищаються від непотрібних або застарілих записів, стандартизуються і агрегуються для подальшого аналізу. стандартизувати дані допомагають спеціалізовані мови програмування. Аналіз включає використання різних методів, від базових статистичних до складніших моделей машинного навчання, які дозволяють виявляти закономірності та робити прогнози. Останнім етапом є візуалізація даних у вигляді графіків або панелей для зручного сприйняття та інтерпретації, що забезпечує підтримку в прийнятті рішень для практичної діяльності поліції.

Для ефективного аналізу інформації застосовуються як традиційні, так і новітні методи. Основні інструменти включають програмне забезпечення, таке як Power BI та Tableau для створення інтерактивних дашбордів, а також Google Data Studio для базової аналітики. Серед мов програмування популярними є Python з бібліотеками pandas, scikit-learn, matplotlib та R для аналітичних задач. Технології великих даних, такі як Hadoop і Spark, дозволяють обробляти великі обсяги інформації, а алгоритми машинного навчання, зокрема регресії, дерева рішень та глибоке навчання, застосовуються для прогнозування та автоматизації процесів, що підвищує ефективність роботи правоохоронних органів.

Процес ухвалення рішень на основі аналізу даних у Національній поліції України включає кілька етапів. Спочатку визначається проблема, що дозволяє чітко сформулювати завдання, наприклад, покращення ефективності реагування на надзвичайні ситуації. Потім проводиться оцінка альтернатив, де порівнюються різні варіанти дій з урахуванням їхніх переваг та ризиків, що може бути здійснено за допомогою інструментів аналізу, таких як SWOT. Після цього приймається рішення з урахуванням різних критеріїв через методи багатокритеріального аналізу. Останнім етапом є моніторинг і корекція рішень, що включає оцінку ефективності реалізованих заходів та внесення необхідних коректив для досягнення оптимальних результатів у діяльності поліції.

Разом із перевагами застосування аналізу даних у практичній діяльності існують і певні виклики, що пов'язані з організацією ефективного збору, обробки та аналізу даних для прийняття обґрунтованих рішень у реальному часі, при цьому гарантуючи безпеку, конфіденційність та точність інформації.

Аналіз даних і підтримка прийняття рішень є важливими складовими роботи правоохоронних органів, зокрема Національної поліції України. Ось кілька прикладів успішного використання аналізу даних у діяльності поліції:

1. Одним із прикладів використання аналізу даних для забезпечення громадської безпеки є програма «Безпечне місто». Вона включає в себе інтеграцію відеокамер спостереження, датчиків і систем контролю за дорожнім рухом, а також використання аналітичних систем для збору і обробки даних. За допомогою цього аналізу поліція може:

   - виявляти правопорушення в режимі реального часу;
   - визначати місця з підвищеним ризиком злочинності;
   - оптимізувати розподіл патрулів і визначати пріоритетні зони для контролю.

2. Інтегровані інформаційні системи для боротьби з організованою злочинністю допомагають виявляти зв'язки між учасниками злочинних угруповань, відстежувати їхні фінансові транзакції, переміщення та інші аспекти діяльності. Це дозволяє організувати більш ефективну боротьбу з організованою злочинністю, виявляти та нейтралізувати небезпечні мережі до того, як вони зможуть реалізувати свої злочинні наміри.
3. Ще одним важливим інструментом є застосування методів машинного навчання та статистичного аналізу для передбачення злочинів. Аналіз даних про місця, час і типи правопорушень дозволяє прогнозувати ймовірність виникнення злочинів у певних районах і в певний час. На основі таких прогнозів поліція може оптимізувати свої ресурси, забезпечувати превентивні заходи і вчасно реагувати на потенційні загрози.
4. Використання аналізу даних для дослідження причин дорожньо-транспортних пригод (ДТП) дозволяє виявити небезпечні ділянки доріг та потенційно небезпечні фактори (наприклад, недостатнє освітлення, неякісне дорожнє покриття або високі швидкості). Ці дані допомагають поліції і місцевим органам влади впроваджувати відповідні заходи для покращення безпеки на дорогах, такі як встановлення камер автоматичної фіксації порушень, зміна розмітки чи встановлення додаткових знаків.
5. Використання аналізу даних з різних джерел (відеокамери, соціальні мережі, мобільні додатки тощо) допомагає Національній поліції виявляти надзвичайні ситуації або масові порушення правопорядку в реальному часі. Завдяки інтеграції даних з різних систем поліція може миттєво реагувати на ситуацію, направляти патрулі або навіть кооперувати з іншими силовими структурами для запобігання ескалації подій.
6. Аналіз даних про випадки домашнього насильства допомагає поліції виявляти тенденції та локалізувати найуразливіші регіони. Використання інформаційних систем дозволяє більш швидко реагувати на виклики та надавати необхідну допомогу постраждалим. Завдяки збору даних про правопорушення в цій сфері, поліція може розробляти більш ефективні стратегії підтримки жертв насильства та попередження таких злочинів.

Висновок. Використання сучасних методів аналізу даних і систем підтримки прийняття рішень значно підвищує ефективність діяльності Національної поліції України, дозволяючи оперативно реагувати на різноманітні виклики, знижувати рівень злочинності та забезпечувати більшу прозорість роботи правоохоронних органів. Інтеграція таких технологій дозволяє не лише удосконалити робочі процеси, а й підвищити рівень безпеки в країні, завдяки швидкому та точному аналізу інформації, що надходить у реальному часі.

Література

1. Збірник матеріалів Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи» Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с. URL: https://politkaf.kpnu.-edu.ua/wp-content/uploads/2023/04/zbirnyk-material-konfer.-inf_bezp_2023.pdf ;
2. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с. URL: https://kjourn.pnu.edu.ua/wp-content/uploads/sites/54/2018/04/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D1%87%D0%BD%D0%B0-%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C.pdf ;
3. Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України : матеріали наук.-практ. конф. (Київ, 25 квіт. 2024 р.) / упоряд.: В. М. Фурашев, С. О. Дорогих, О. В. Лебединська, О. Г. Радзієвська. – Київ; Одеса : Фенікс, 2024. – 150 с. URL: https://ippi.org.ua/sites/default/files/konferenciya_25.04.2024.pdf ;
4. Вагонова О. Г., Горпинич О. В., Чорнобаєв В. В. Організація діяльності органів державної влади : навч. посіб. ; М-во освіти і науки України, НТУ «Дніпровська політехніка». Дніпро : НТУ «ДП», 2019. 77 с.;
5. Демкова М., Фігель М. Інформація, як основа інформаційного суспільства: поняття та правове регулювання. URL: https://www.oa.edu.ua› loadnew›5.doc;
6. Ліпкан В. А., Сопілко І. М., Кір'ян В. О. Правові засади розвитку інформаційного суспільства в Україні : монографія / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2015. 664 с.;
7. Загуменна В. В., Кузьменко О. І. Інформаційно-аналітична діяльність як наукова та навчальна дисципліна: еволюція, тенденції розвитку. Бібліотекознавство. Документознавство. Інформологія. 2022. № 4. С. 102-107.

Haborets Olha Andriivna

Associate Professor of the Department of Operational and Search Activities and Information Security, Donetsk State University of Internal Affairs, PhD, Associate Professor

DEFENSE ANALYTICS: LEVERAGING ARTIFICIAL INTELLIGENCE FOR STRATEGIC INSIGHTS AND OPERATIONAL EXCELLENCE

Artificial intelligence (AI) has emerged as a revolutionary tool in the defense sector, fundamentally transforming the way analytical support is provided for operations and decision-making. In an era characterized by complex and evolving threats, such as cyberattacks, hybrid warfare, and asymmetric conflicts, AI plays a critical role in enabling defense organizations to maintain operational superiority. The ability to process and analyze vast amounts of data in real time, anticipate potential threats, and provide actionable intelligence makes AI indispensable for modern defense strategies.

One of the most prominent applications of AI in defense analytics is in the field of big data analysis and intelligence gathering. Defense operations generate immense volumes of data from a multitude of sources, including satellite imagery, sensors, open-source intelligence (OSINT), and social media platforms. AI algorithms excel in processing this data, identifying patterns, and drawing correlations that are often imperceptible to human analysts. For example, AI-driven natural language processing (NLP) systems can parse intelligence reports, extracting critical information and detecting early warning signs of emerging threats. These capabilities enable defense agencies to act proactively, addressing potential risks before they escalate.

Predictive analytics is another area where AI has made a significant impact. Machine learning (ML) models analyze historical data to identify trends and predict potential security risks. In the context of cybersecurity, AI algorithms can detect anomalies and vulnerabilities in networks, anticipating attacks such as phishing, malware intrusions, or distributed denial-of-service (DDoS) assaults. By providing a predictive framework, AI enhances the ability of defense organizations to mitigate risks and implement preemptive measures. For example, predictive models can forecast enemy troop movements or cyberattack strategies, allowing for more effective resource allocation and response planning.

AI also enhances situational awareness by integrating data from multiple sources and presenting it in a coherent and actionable format. This capability is particularly critical in complex and dynamic operational environments. For instance, AI-enabled image recognition systems can analyze satellite or drone imagery to detect enemy installations, identify equipment, or monitor unusual activities. By synthesizing geospatial data, battlefield sensor inputs, and real-time surveillance, AI provides commanders with a comprehensive understanding of the operational landscape. This enhanced situational awareness is pivotal for informed decision-making, minimizing risks, and maximizing mission success.

Automation is another area where AI significantly contributes to the efficiency of defense analytics. Routine tasks, such as categorizing data, generating reports, and indexing documents, can be automated using AI, allowing human analysts to focus on higher-level strategic analysis. Virtual assistants and chatbots powered by AI further enhance productivity by assisting with data retrieval, answering routine queries, and streamlining communication processes. This shift towards automation not only reduces the workload of personnel but also accelerates the decision-making process, which is often critical in time-sensitive defense operations.

Cybersecurity, a cornerstone of modern defense strategies, greatly benefits from AI-driven innovations. Advanced intrusion detection systems (IDS) powered by AI monitor network traffic, identifying and neutralizing threats in real time. AI algorithms are capable of recognizing suspicious patterns, such as unauthorized access attempts or abnormal data transfers, and can automatically deploy countermeasures to prevent data breaches. Furthermore, AI enhances the ability to secure sensitive information by employing techniques like encryption, anomaly detection, and user behavior analysis. This is particularly important in safeguarding classified information and ensuring the integrity of defense communication systems.

Despite its numerous advantages, the integration of AI into the defense sector is not without challenges. One of the primary hurdles is ensuring the availability of high-quality and diverse datasets for training AI models. Incomplete, biased, or corrupted data can lead to inaccurate results, undermining the reliability of AI systems. Additionally, ethical and legal concerns arise with the deployment of AI, particularly in autonomous systems capable of

lethal actions. The use of AI in defense must align with international laws and ethical guidelines to ensure accountability and prevent misuse.

Technical and organizational barriers also pose significant challenges. Integrating AI into existing defense infrastructure requires substantial investment in hardware, software, and personnel training. Resistance to change and a lack of AI literacy among staff can further hinder adoption. Moreover, the risk of adversarial AI, where opponents exploit vulnerabilities in AI systems, necessitates the development of robust countermeasures. Techniques such as adversarial training, continuous model updates, and advanced security protocols are essential to safeguard AI systems from manipulation.

Looking to the future, the role of AI in defense analytics is expected to expand exponentially. Emerging technologies, such as quantum computing, promise to enhance AI capabilities by enabling faster data processing and more complex analysis. The development of collaborative AI-human systems will further optimize decision-making by combining the strengths of machine precision with human intuition and ethical judgment. Additionally, advancements in autonomous systems, including drones, robotics, and unmanned vehicles, will revolutionize reconnaissance, logistics, and combat operations.

In conclusion, artificial intelligence represents a paradigm shift in the analytical support systems of the defense sector. By enabling real-time intelligence, predictive analytics, enhanced situational awareness, and automated processes, AI empowers defense organizations to address emerging threats with unprecedented efficiency and precision. However, to fully realize the potential of AI, it is crucial to overcome challenges related to data quality, ethical considerations, and adversarial risks. Continuous investment in AI research, infrastructure, and personnel training will be essential for ensuring that AI remains a reliable and secure asset in the defense sector. With strategic integration, AI has the potential to redefine the future of national and global security.

References

1. Prosvirina T.V., Haborets O.A., Lunhol O.M. Analysis of the organization of information and analytical support of police activities. Scientific innovations and advanced technologies. Issue № 1(15) 2023. Pp. 319 – 327.
2. Габорець О., Шаєц Є. Впровадження штучного інтелекту у системи моніторингу та прогнозування громадської безпеки. Збірник тез доповідей ІІ Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій» (06 груд. 2023 р., м. Черкаси) [Електронний ресурс] / упоряд. : Т. О. Прокопенко, Я. В. Тарасенко ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2023. С. 105-106.

Галайко Наталія Володимирівна

старший викладач кафедри інформаційних систем та технологій ННІУПБ Львівського державного університету внутрішніх справ

РОЛЬ CRM-ТЕХНОЛОГІЙ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ БІЗНЕСУ

Сучасні умови ведення бізнесу, що характеризуються високою конкуренцією, швидким розвитком технологій та змінюваними вимогами ринку, свідчать про те, що успіх можуть досягти лише ті компанії, які здатні ефективно інтегрувати сучасні

інформаційні технології у свої бізнес-процеси. Використання інноваційних технологій дозволяє підприємствам автоматизувати рутинні операції, покращувати якість обслуговування клієнтів, оптимізувати управлінські процеси та забезпечувати гнучкість у реагуванні на зміни. Ефективне застосування таких технологій сприяє підвищенню конкурентоспроможності компанії, дозволяє отримувати більше даних для прийняття рішень і забезпечує можливості для масштабування бізнесу.

У ході впровадження інформаційних комп'ютерних технологій для автоматизації бізнес-процесів, зокрема в сфері продажів, були створені спеціалізовані CRM-системи (Customer Relationship Management), що забезпечують ефективне управління взаємовідносинами з клієнтами. Ці системи дозволяють компаніям централізовано збирати, зберігати та обробляти дані про клієнтів, що дає змогу автоматизувати багато аспектів взаємодії з ними. В результаті компанії отримують можливість більш ефективно управляти процесом продажів, персоналізувати пропозиції для кожного клієнта, а також підвищувати рівень задоволеності та лояльності своїх споживачів.

CRM-системи стали першим видом інформаційних систем, які сфокусували увагу керівників не на бек-офісі, як в системах ERP, і не на виробничих процесах, як в системах MRP, MRP II, а на фронт-офісі – в маркетингу, продажах, сервісі та обслуговуванні [1].

Якщо розглядати будову CRM, то це складний бізнес-процес, набір додатків, що включає процес збору інформації і до прийняття рішень на його основі. Дана система дозволяє проводити автоматизацію відповідних бізнес-процесів в маркетингу, продажах і обслуговуванні клієнтів [2].

Застосування CRM-системи має численні переваги, які допомагають бізнесу покращити ефективність управління взаєминами з клієнтами, підвищити рівень продажів і задоволеності клієнтів (табл. 1).

ТАБЛИЦЯ 1. Переваги і можливості використання CRM

Переваги	**Можливості**
Покращення взаємодії з клієнтами	CRM дозволяє зберігати всю інформацію про клієнтів в одному місці, що дає можливість персоналізувати підхід до кожного клієнта. Завдяки цьому бізнес може краще розуміти потреби та побажання своїх клієнтів, створювати індивідуальні пропозиції і забезпечувати високий рівень обслуговування.
Автоматизація процесів	CRM-системи автоматизують рутинні завдання, такі як відправка email-розсилок, планування зустрічей, нагадування про важливі події та дати. Це дозволяє співробітникам зосередитися на важливіших аспектах їх роботи, що підвищує загальну ефективність.
Покращення управління продажами	За допомогою CRM можна відслідковувати весь процес продажів: від початкових контактів до заключення угоди. Система дозволяє бачити, на якому етапі знаходяться угоди, а також прогнозувати майбутні доходи. Це допомагає керівникам

	приймати обґрунтовані рішення та управляти продажами більш ефективно.
Аналіз і звітність	CRM-системи надають потужні інструменти для збору та аналізу даних, що дозволяє компаніям розуміти, які стратегії працюють найкраще, і де є можливості для покращення. Вони також дають змогу формувати різноманітні звіти, що спрощує прийняття стратегічних рішень.
Покращення лояльності клієнтів	Використання CRM дає змогу компаніям створювати довгострокові відносини з клієнтами, швидше реагувати на їх запити та потреби, що значно підвищує рівень лояльності. Задоволені клієнти більш схильні до повторних покупок і рекомендацій.
Координація між командами	CRM дозволяє командам з різних відділів (продажі, маркетинг, підтримка клієнтів) працювати в одному інформаційному середовищі, що забезпечує безперебійний потік інформації і зменшує ймовірність помилок та непорозумінь.
Зниження витрат	Завдяки автоматизації та покращеному управлінню процесами, CRM дозволяє знижувати витрати, пов'язані з операційною діяльністю. Можна оптимізувати витрати на маркетинг, ефективніше розподіляючи бюджет завдяки точним даним про поведінку клієнтів.
Масштабованість та гнучкість	Багато сучасних CRM-систем є масштабованими і можуть адаптуватися до зростаючого бізнесу. Це означає, що система може підтримувати все більше клієнтів і складніші процеси, зберігаючи ефективність роботи на будь-якому етапі розвитку компанії.

За результатами досліджень, проведених в Україні, встановлено, що витрати на утримання одного клієнта в 5 разів менші, ніж на залучення нового. Клієнти приносять прибуток у повному обсязі лише через рік після початку співпраці. Якщо комунікації з клієнтами неефективні, 65% з них не приносять значного прибутку. Збільшення числа постійних клієнтів на 5% може призвести до зростання обсягів продажів на понад 25%, а прибутку – на 50–100%.

Оскільки сучасні споживачі вимагають ідеального обслуговування, 75% з них очікують високого рівня сервісу. Підприємства, які впроваджують CRM-системи, збільшують конверсію лідів (кількість потенційних клієнтів, що перетворюються на реальних покупців або користувачів послуг) на 17% і підвищують продуктивність роботи на 21% [3].

Отже, інтеграція цифрових технологій у бізнес-процеси є ключовим напрямом розвитку в умовах сучасного світу. Впровадження інноваційних цифрових рішень може включати використання CRM-систем. CRM-система стає важливим інструментом для

компаній, які прагнуть оптимізувати час, покращити ефективність бізнес-процесів, просувати бренд і, в результаті, підвищити рівень задоволеності клієнтів і збільшити свої прибутки.

Література

1. Дорошкевич Д.В. CRM-система як інструмент персоніфікованого маркетингу. Наукові праці Полтавської державної аграрної академії. Полтава: ПДАА, 2013. Вип. 1 (6). Том 2. С. 157-161.
2. Ганущак-Єфіменко Л. М. CRM-система як ефективний інструмент розвитку готельного бізнесу в Україні. Вісник Київського національного університету технологій та дизайну. Серія: Економічні науки. 2017. № 4. С. 51–56.
3. Янчук Т. В., 11. Боєнко О. Ю. Впровадження CRM-систем як засіб підвищення ефективності маркетингової діяльності. Економіка та суспільство. Випуск № 48. 2023. https://doi.org/10.32782/2524-0072/2023-48-89

Гречаний Вячеслав Олександрович

викладач кафедри тактики та тактико-спеціальної підготовки факультету службово-бойової діяльності Національної гвардії України Київського інституту Національної гвардії України

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ЗАСОБІВ АТМОСФЕРНОГО ОПТИЧНОГО ЗВ'ЯЗКУ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

Швидкий розвиток інформаційних та телекомунікаційних систем в сфері безпеки та оборони держави вимагає постійного збільшення системних потужностей, покращення пропускної здатності каналів, підвищення рівня конфіденційності та завадозахищеності, вищих швидкостей передачі даних за для вирішення основної проблеми, а саме передачі надзвичайно різноманітного трафіку даних з чисельних мережевих пристроїв у базову мережу.

У той же час, вирішення зазначеної проблеми в умовах ведення бойових дій через прокладання оптоволоконного кабелю до користувачів, із зрозумілих причин, не завжди можливо реалізувати.

Використання радіоканалів (радіорелейний та супутниковий зв’язок) може забезпечити з’єднання на багато десятків, сотень і навіть тисяч кілометрів зі швидкістю до кількох сотень мегабіт за секунду. Однак безпроводові радіосистеми, що набули широкого поширення, мають занизьку надійність через залежність від політик операторів з надання послуг, відносно високу вартість орендної плати, вразливості радіоканалів з боку протидії РЕБ противника, необхідність оформлення дозволів на використання радіочастотного спектру та головне це технічні обмеження щодо спроможностей радіоканалів до збільшення швидкостей передачі даних.

В даний час підвищену зацікавленість, особливо як засіб доставки трафіку, викликають FSO технології, яка забезпечує швидкість передачі даних оптичного волокна з гнучкістю бездротового зв’язку. Технологія оптичного бездротового зв’язку

FSO (Free Space Optics – атмосферний оптичний зв'язок, атмосферні оптичні лінії зв'язку – АОЛЗ, бездротовий оптичний канал зв'язку (БОКЗ)) – це спосіб бездротової передачі даних в інфрачервоній частині оптичного спектра, де приймач і передавач повинні знаходитися в зоні прямої видимості, та яка дозволяє створювати надійні канали зв'язку на відстанях від 100 метрів до декількох кілометрів в умовах атмосфери і до 100 000 км у відкритому космосі, наприклад для зв'язку між супутниками. Будучи альтернативним рішенням атмосферні оптичні лінії передачі даних дозволяють надоперативно сформувати бездротовий оптичний канал зв'язку (мобільні системи з автонаведенням забезпечують встановлення зв'язку за 10-15 хвилин) та за значно менших витрат. АОЛЗ цілком здатні замінити дорогі рішення, що використовуються зараз на базі гібридних технологій.

Оптичний зв’язок у вільному просторі останнім часом захопив велику частину дослідників завдяки своїй широкій смузі пропускання, легкому розгортанню та захищеним з’єднанням, що робить його придатним для комунікаційних цілей. До основних переваг такого способу передачі інформації можна віднести: високі швидкості передачі (які неможливо досягти при використанні інших бездротових технологій), простота інсталяції, висока конфіденційність передачі даних, нечутливість до електромагнітних перешкод, а також відсутність необхідності платити за використання частотного діапазону. У даний час технологія забезпечує передачу цифрових потоків до десятків Гбіт/с та легко стикується із звичним телекомунікаційним обладнанням.

Бездротова оптика розглядається як рішення:

- на ділянках останньої милі (для зв'язку між вузловими точками мережі);
- для організації зв'язку від вузлів зв'язку при великих обсягах цифрового трафіку, що передається;
- для зв'язку між об'єктами, коли прокладання кабелю неможливе (промзони, гірська місцевість, залізниця, райони ведення бойових дій);
- як тимчасовий канал зв'язку, а також у випадках, коли необхідно терміново організувати канал зв'язку (оперативний зв'язок, гарячий резерв);
- коли потрібен закритий канал зв'язку, несприйнятливий до перешкод (за рахунок вузьконаправленості) і такий, що не буде їх створювати (аеропорти, близькість радіолокаторів, ліній електропередач, вплив засобів РЕБ);
- радіомаскування комунікацій системи зв'язку.

Потрібно відмітити також і чинники, що впливають на якість та надійність атмосферних оптичних ліній зв’язку. Їх, за великим рахунком, два, а саме:

- мікрорухи та вібрації несучих конструкцій, які використовуються для монтажу оптичного обладнання (компенсується автоматичним відстеженням налаштувань «антени» в режимі реального часу та вирішується системою автосупроводу (наведення та прицілювання));
- зміни погодних умов та тумани як фактор, що негативно впливає через згасання рівню сигналу (інфрачервоне випромінювання особливо сильно поглинається парами води (сніг, дощ), частинками пилу та диму (компенсується використанням «вікон прозорості» оптичного діапазону, в яких негативний вплив найменшій та впровадженням новітніх методів модулювання та мультиплексування сигналу).

Лише декілька роки тому бездротові оптичні лінії зв’язку розглядалися, скоріше, як екзотика. Зараз FSO – це перспективна оптична технологія, яка має великі шанси доповнити традиційні системи зв’язку та обміну інформацією між підрозділами сектору безпеки та оборони держави у забезпечені потреб зі збільшення швидкості обміну інформацією, необмеженої пропускну здатності, безпеки зв’язку, оперативності та завадозахищеності.

Денисенко Богдан Анатолійович
експерт з питань організованої злочинності (Консультативна місія Європейського Союзу)

ОНОВЛЕНА ІТ ЕКОСИСТЕМА ЯК ОСНОВА ДЛЯ РЕФОРМУВАННЯ ПРАВООХОРОННОЇ СИСТЕМИ

Реформування правоохоронної системи передбачає впровадження комплексу заходів з переналаштовування, вдосконалення та запровадження новел у ряді процесів, процедур, таке інше. Відображення цієї дорожньої карти у стратегічних документах є передумовою до початку їх впровадження. Тому, Консультативна місія ЄС в Україні (КМЄС) долучилась до створення Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки (КСП) як основний партнер у розробці та координації змісту документу. КСП був схвалений указом Президента України від 11 травня 2023 року № 273/2023. КСП є структурованим документом, дороговказом, який передбачає впровадження вказаного комплексу заходів. Зокрема, його впровадження деталізовано у плані заходів, спрямованих на виконання КСП (до створення якого КМЄС була залучена також). План був затверджений розпорядженням Кабінету Міністрів України від 23 серпня 2024 р. № 792-р «Про затвердження плану заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки». КСП та план заходів, спрямованих на його виконання передбачають впровадження ILP та комплексної цифрової трансформації. У той же час, план (КСП) та його план заходів не дають деталізованого роз’яснення яким чином впроваджувати ці заходи. Зокрема, чіткого алгоритму впровадження ILP не передбачено, його опис розмитий, хоча елементи для впровадження проактивної правоохоронної моделі (ILP) передбачені у різних його пунктах та розділах. Задля комплексного розуміння деталей цієї правоохоронної моделі, рекомендовано ознайомитись з монографією «Реалізація філософії. «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України». Монографія є продуктом спільної та кропіткої роботи практиків-представників різних правоохоронних органів та академічної спільноти. Монографія дає відповіді на ряд запитань щодо суті моделі та її елементів.

На необхідності впровадження ILP наголошується у Звітах Європейської Комісії щодо прогресу України в межах Пакету розширення 2023 та 2024. Зокрема, у Звіті 2024 року (від 30 жовтня 2024 року) зазначається, що «Рівень впровадження правоохоронної моделі «Правоохоронна діяльність, керована аналітичною розвідкою» (Intelligence-led Policing/ILP) є незначним». Починаючи з 2015 року КМЄС неодноразово наголошував представникам правоохоронних органів та академічної спільноти, що КМЄС готовий допомогти у комплексному впровадженні цієї правоохоронної моделі. За ініціативи КМЄС була створена робоча група щодо впровадження ILP з представників НПУ, МВС та ВУЗів МВС, однак робоча група функціонувала незначний період часу за відсутності

ініціативи зі сторони МВС та НПУ. У 2022 році КМЄС закликало МВС відновити роботу робочої групи, однак безрезультатно.

Першочерговими кроками для впровадження ILP вбачаю: 1) **Створення уніфікованого понятійного апарату**. Всі учасники процесу повинні стандартизовано підходити до всіх процесів роботи з даними, інформацією, говорити «однією мовою». 2) **Проведення функціонального аудиту бізнес-процесів (робочих процесів)** з інформаційного менеджменту задля визначення найбільш ефективної та результативної моделі. 3) **Перегляд, переналаштування, та/або новий дизайн ІТ-можливостей та відповідних процесів** регулювання з управління інформацією, баз даних, реєстрів, таке інше. Першочергові кроки стосуються всіх правоохоронних органів і не обмежуються лиш МВС та НПУ. Це також стосується ВУЗів, оскільки ILP повинно впроваджуватись всією правоохоронною системою одночасно. Тому, всі відомчі (і не тільки) ВУЗи (не обмежуючись лиш ВУЗами МВС) повинні приймати участь у цьому процесі. Головною умовою успіху впровадження є наскрізна стандартизація процесів, продуктів та понятійного апарату. Отже, із запропонованих першочергових кроків ми бачимо що перегляд ІТ-можливостей і є тим ключовим базисом, який формує можливість впровадження нових процесів інформаційного менеджменту, та, таким чином, - підвищення якості прийняття управлінських рішень, більш ефективного розподілу ресурсів, що і є основною метою запровадження цієї правоохоронної моделі (ILP).

Звіт Європейської Комісії щодо прогресу України в межах Пакету розширення 2024 року, також наголошує, що: «Україна не має уніфікованої (спільної/міжвідомчої) системи правоохоронних органів збору інформації та аналітичної розвідки (intelligence)». Отже, формування єдиної правоохоронної ІТ екосистеми є необхідним та критичним кроком на шляху Європейської інтеграції України. КМЄС неодноразово на цьому наголошувала з 2016 року. Серед запропонованих послідовних кроків щодо цього вбачаю наступні: 1) створення єдиної ІТ платформи для обміну даними, інформацією, аналітичною розвідкою, таке інше, 2) реалізація інтероперабельності (функціональної сумісності) реєстрів, баз даних, таке інше, та стандарти до їх формування, 3) перегляд та створення умов для підвищення якості та надійності даних, інформації, які зберігаються у державних реєстрах, базах даних, таке інше, 4) створення уніфікованого та комплексного підходу та процесів щодо збору, внесення, опрацювання, аналізу та поширення даних, інформації та аналітичної розвідки серед всіх правоохоронних органів.

Серед критично необхідних задач є впровадження нового поняття та підходу «аналітичної розвідки (intelligence)» до національних процедур управління інформацією. Це, у свою чергу, формує нову архітектуру інформаційних масивів, процедур збору та опрацювання, систем, таке інше. Враховуючи складність впровадження даного підходу, КМЄС готова допомогти НПУ, МВС та іншим правоохоронним органам у цьому процесі. Наступним кроком є створення уніфікованої (спільної/міжвідомчої) системи правоохоронних органів збору інформації та аналітичної розвідки. Оскільки НПУ є одним з найбільших генераторів та споживачів інформаційних ресурсів серед правоохоронних органів, формування цієї системи можливо почати на базі ІПНП, або/та ЄІС МВС. У той же час, рішення щодо формування системи на базі існуючої, чи нової інформаційно-аналітичної пошукової системи, вибір архітектури та технологій повинно бути прийнято консенсусом, всіма правоохоронними органами. Формування архітектури системи повинно відповідати робочим процесам, реальним потребам. У зв’язку з чим, серед запропонованих першочергових кроків впровадження ILP вказаний: «**Прове-**

дення функціонального аудиту бізнес-процесів (робочих процесів) з інформаційного менеджменту задля визначення найбільш ефективної та результативної моделі», який повинен сформувати алгоритми процесів, які, у свою чергу, повинні бут основою для наступного кроку: «**Перегляд, переналаштування, та/або новий дизайн ІТ-можливостей та відповідних процесів**». Формування єдиної правоохоронної системи, або платформи є складним процесом. У той же час, першочерговою задачею цього процесу є формування транспортної архітектури. Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» вже є готовою основою цього процесу. Єдиний портал державних послуг «Дія» є гарним прикладом впровадження цієї ідеї. Крім того, прийшов час розглянути розгортання інформаційних та транспортних можливостей та систем у хмарі та залучення можливостей штучного інтелекту, який, у свою чергу, передбачає внесення змін до законодавства та підзаконних нормативно-правових актів, перегляд технологій та технологічної сумісності, таке інше.

Створення оновленої ІТ екосистеми передбачає оновлення, перегляд та внесення змін до архітектури та технологій систем обміну та зберігання інформації, аналітичної розвідки, організаційно-штатних структур правоохоронних органів, перегляду процедур інформаційного менеджменту (включаючи, але не обмежуючись збором інформації, оцінкою та упорядкування інформації, стандартизованого аналізу інформації, таке інше), законів та підзаконних нормативно-правових актів, таке інше. Цей процес є складним та передбачає перегляд, впровадження та поєднання стандартів та форматів, технологій та бачення. КМЄС готовий долучитись до цього процесу заради досягнення амбітної мети – якнайшвидшої Європейської інтеграції України.

Література

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Р., Денисенко Б. та ін., за заг. ред. Користіна О.Є. – Київ: «ВАІТЕ», 2024. 444 с.
2. «Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки», схвалений указом Президента України від 11 травня 2023 року № 273/2023.
3. Розпорядження Кабінету Міністрів України від 23 серпня 2024 р. № 792-р «Про затвердження плану заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки».
4. Звіт щодо прогресу України в межах Пакету розширення 2023 № SWD(2023) 699 final від 8 листопада 2023 року, Режим доступу: https://op.europa.eu/en/publication-detail/-/publication/a0f3eaa6-7eee-11ee-99ba-01aa75ed71a1/language-en
5. Звіт щодо прогресу України в межах Пакету розширення 2024 № SWD(2024) 699 final від 30 жовтня 2024 року, Режим доступу: https://neighbourhood-enlargement.ec.europa.eu/document/download/1924a044-b30f-48a2-99c1-50edeac14da1_en?filename=Ukraine%20Report%202024.pdf

Д’яков Андрій Володимирович
доцент кафедри інформаційних систем та технологій ННІУПБ Львівського державного університету внутрішніх справ, кандидат технічних наук

РАЦІОНАЛЬНА СТРУКТУРА ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ПРАВООХОРОННИХ ОРГАНІВ

Збільшення кількості і інтенсивності інформаційних потоків, зменшення часу на їх обробку та підвищення вимог до прийняття відповідного рішення породжує актуальну задачу по розробці раціональної структури інформаційної системи правоохоронних органів, яка б була здатна вирішувати завдання по забезпеченню цивільної безпеки.

Сучасний підхід до створення автоматизованого управління підрозділами правоохоронних органів передбачає впровадження у вказаний процес геоінформаційних систем. Можливості геоінформаційних систем ефективно збирати, зберігати, аналізувати та візуалізувати просторові дані визначають їх виключно важливу роль в правоохоронній діяльності. Сьогодні геоінформаційні системи поєднують у собі можливості систем керування базами даних, редакторів растрової й векторної графіки й аналітичних засобів і застосовуються в картографії, геології, метеорології, землевпорядженні, екології.

Концептуально геоінформаційні системи передбачають наступний функціонал:

- обробка та поєднання різних видів даних – супутникових знімків, розвідданих, інформацію про місцевість та інфраструктуру для створення комплексної картини оперативної обстановки;
- прогнозування та моделювання різних сценаріїв розвитку подій, оцінка можливих наслідків та ризиків;
- управління логистикою та ресурсами, оптимізація маршрутів переміщення, а також планування розташування логістичних центрів;
- проведення моніторингу та аналізу, аналіз динаміки розвитку подій, виявлення та прогнозування загроз. Моніторинг довкілля та оцінки збитків від природних або антропогенних катастроф;
- координація з міжнародними партнерами, обмін геопросторовими даними з міжнародними організаціями та партнерами для координації спільних дій у сфері безпеки та оборони.

Зрозуміло, що функціональна структура геоінформаційної системи правоохоронних органів визначається сукупністю її функцій, що здатна виконувати вказана система. Відповідно до цього можна визначити функціональні складові геоінформаційної системи правоохоронних органів, виходячи з необхідних завдань, що має виконувати система:

Збір даних. Інструменти для збору просторових даних із різних джерел, таких як супутникові знімки, аерофотознімки, GPS-трекери, відеокамери та датчики.

Зберігання даних. Бази даних для зберігання великих обсягів просторових даних та метаданих, які забезпечують швидкий доступ і обробку інформації.

Аналіз даних. Аналітичні інструменти для виявлення закономірностей, аналізу тенденцій та прогнозування, які допомагають у плануванні та прийнятті рішень.

Візуалізація даних. Графічні інтерфейси, які дозволяють відображати просторові дані у вигляді карт, діаграм і моделей, що полегшує інтерпретацію та аналіз.

Інтеграція даних. Можливість інтеграції даних з інших інформаційних систем, таких як бази даних кримінальних записів, реєстри транспортних засобів та системи моніторингу безпеки.

Моніторинг та відстеження. Інструменти для реального часу моніторингу та відстеження руху підозрюваних осіб, транспортних засобів та об'єктів, що сприяє оперативному реагуванню.

Звітування. Автоматичне генерування звітів і статистичних даних для аналізу ефективності операцій і підготовки до майбутніх завдань.

Все це дозволить правоохоронним органам ефективно виконувати свої завдання, забезпечуючи точність, оперативність та покращення процесів прийняття рішень.

Зачек Микола Олегович

здобувач вищої освіти 3 курсу ННІУПБ Львівського державного університету внутрішніх справ

Леськів Галина Зіновіївна

професор кафедри менеджменту та економічної безпеки ННІУПБ Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЗМІНА ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ТА ЯКОСТІ В СУЧАСНОМУ БІЗНЕСІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний бізнес вступає в еру, де технологічні інновації та використання штучного інтелекту (ШІ) змінюють традиційні підходи до управління якістю та конкурентоспроможністю. Інтеграція ШІ у бізнес-процеси дозволяє компаніям не лише покращувати якість продукції та послуг, але й формувати нові конкурентні переваги, що забезпечують стабільний розвиток у мінливих умовах ринку.

Однією з ключових сфер застосування ШІ є управління виробничими процесами. Використання інтелектуальних систем автоматизації дозволяє підприємствам ефективно контролювати та оптимізувати виробничі операції, знижуючи витрати і підвищуючи продуктивність. У цьому контексті наша робота спрямована на аналіз змін підходів до конкурентоспроможності та якості через використання ШІ у сучасному бізнесі.

Ще однією важливою сферою застосування ШІ є розробка та впровадження нових продуктів. Інтелектуальні системи дозволяють проводити швидкий і точний аналіз ринкових тенденцій, враховуючи широкий спектр факторів. Такий підхід сприяє створенню інноваційних продуктів, адаптованих до змін потреб споживачів, що значно підвищує конкурентоспроможність компаній.

Традиційні підходи до управління якістю, такі як стандартизація за ISO, методології Lean та Six Sigma, показали свою ефективність у створенні стабільних процесів та зменшенні кількості дефектів. Однак вони мають обмеження у швидкості реагування, адаптації до змін та аналізі великих обсягів даних. У сучасному світі необхідно впроваджувати технології, які забезпечують не лише контроль якості, але й її прогнозування та вдосконалення [1].

ШІ відкриває перед бізнесом нові можливості для аналізу, прогнозування та управління якістю. Інтеграція ШІ в управлінські процеси дозволяє оптимізувати кожен етап життєвого циклу продукту або послуги, починаючи від проектування та закінчуючи після продажним обслуговуванням.

Основні напрями використання ШІ в управлінні якістю [2]:

- аналіз даних у реальному часі. Завдяки алгоритмам ШІ підприємства можуть отримувати детальну інформацію про стан обладнання, процесів і продукції в реальному часі, що дозволяє вчасно виявляти та усувати відхилення;
- прогнозування дефектів. Моделі машинного навчання використовують історичні дані для ідентифікації шаблонів, що можуть призводити до дефектів. Це дає змогу компаніям вживати превентивні заходи, зменшуючи кількість браку;
- оптимізація виробничих процесів. Використання ШІ для автоматизації виробничих процесів дозволяє зменшити вплив людського фактору, підвищити точність операцій і адаптувати процеси під змінні умови;
- індивідуалізація продуктів і послуг. Аналітичні можливості ШІ допомагають краще розуміти потреби клієнтів та адаптувати продукцію чи послуги для задоволення індивідуальних вимог.

Класична теорія конкуренції підкреслює роль ефективного використання ресурсів, де конкуренція є рушійною силою розвитку ринку.

Теорія конкурентних переваг М. Портера акцентує увагу на трьох стратегічних підходах: диференціація, лідерство за витратами та фокусування на окремому сегменті ринку [3].

Ресурсна теорія стверджує, що конкурентоспроможність залежить від здатності компанії створювати та ефективно використовувати унікальні ресурси – матеріальні, інтелектуальні, технологічні.

Інноваційний підхід у світі швидких змін: інновації стають головним чинником забезпечення довготривалого успіху [4].

У сучасному світі технології відіграють вирішальну роль у формуванні конкурентних переваг. ШІ – це набір технологій, що дозволяють системам аналізувати дані, навчатися та приймати рішення з мінімальним втручанням людини. Його впровадження створює нові можливості для бізнесу, роблячи процеси більш ефективними, швидкими та точними [5]. ШІ стає не лише інструментом для підвищення конкурентоспроможності, а й визначальним фактором успіху у сучасному бізнесі. Його впровадження змінює бізнес-моделі, створює нові можливості для розвитку та відкриває нові горизонти у побудові конкурентних стратегій. Завдяки адаптації алгоритмів машинного навчання та аналітичних моделей, компанії здатні досягти нових рівнів продуктивності.

Наприклад, Amazon, один із глобальних лідерів у сфері електронної комерції, активно впроваджує технології ШІ для оптимізації свого ланцюга постачання. Одним із ключових рішень стало використання роботизованих систем Kiva та алгоритмів ШІ для управління складськими процесами. ШІ аналізує дані про попит на товари, прогнозує обсяги замовлень і розподіляє ресурси таким чином, щоб зменшити час обробки замовлення. Завдяки інтеграції машинного навчання роботизовані системи ефективно переміщують товари на складі, забезпечуючи зниження ризику помилок у формуванні замовлень. На сьогодні понад 300,000 роботів діють на складських об'єктах компанії.

Впровадження змін підвищує точність виявлення дефектів на 30%, що зменшує частку браку на 15%. Це також скорочує витрати на контроль якості та ремонти, покращуючи економічну ефективність підприємства [6].

Штучний інтелект у Amazon працює шляхом збору та обробки великих обсягів даних, які включають історію покупок, пошукові запити, перегляди товарів і взаємодії з платформою. Системи ШІ аналізують ці дані для виявлення шаблонів і вподобань кожного індивідуального клієнта. На основі отриманих відомостей алгоритми створюють персоналізовані рекомендації, які допомагають споживачам знаходити ті продукти, які найбільше відповідають їхнім інтересам і потребам. Персоналізація, заснована на ШІ, приносить Amazon відчутні переваги в плані фінансових результатів. Зокрема, дослідження показують, що персоналізовані рекомендації формують до 35% доходів компанії.

Залучення споживачів завдяки персоналізованим пропозиціям створює відчуття індивідуального підходу, що підвищує їхню лояльність до бренду. В результаті клієнти починають сприймати Amazon не тільки як платформу для покупок, але й як надійного партнера, що допомагає їм знаходити потрібні товари. Цей аспект особливо важливий у конкурентному середовищі, де споживачі мають безліч альтернатив.

Крім того, використання ШІ у Amazon сприяє оптимізації логістичних процесів. Алгоритми ШІ допомагають прогнозувати попит на товари, що дозволяє компанії більш ефективно управляти запасами та зменшувати витрати. Зокрема, завдяки прогнозам попиту компанія може своєчасно забезпечити наявність необхідних товарів у відповідних регіонах, що мінімізує випадки дефіциту або надлишку товарів на складах. Це не тільки знижує витрати на логістику, але й сприяє своєчасній доставці замовлень, що покращує рівень обслуговування клієнтів.

Таким чином, впровадження ШІ дозволяє Amazon не лише залишатися конкурентоспроможною на сучасному ринку, але й створювати стійкі конкурентні переваги, які зберігаються у довгостроковій перспективі. Завдяки цьому компанія зміцнює своє лідерство в електронній комерції, забезпечуючи своїм клієнтам високу якість обслуговування, персоналізовані рекомендації та швидку доставку товарів [7].

Оптимізація якості продуктів і послуг за допомогою ШІ вимагає системного підходу, інтеграції передових технологій та організаційних змін. Ефективне впровадження ШІ у процеси виробництва та обслуговування здатне значно покращити якість продукції, скоротити витрати та забезпечити конкурентні переваги на ринку. Одним із головних аспектів є впровадження автоматизованих систем контролю якості, що використовують алгоритми машинного зору та глибинного навчання. Ці системи можуть виявляти навіть найдрібніші дефекти на етапі виробництва. Це дозволяє значно скоротити час перевірок і підвищити ефективність виявлення браку у продуктах, що робить процеси більш надійними та знижує ймовірність людських помилок.

Стратегічні заходи, що включають застосування ШІ, повинні бути інтегровані в загальну стратегію компанії, відповідати її місії та цілям. Вони повинні включати довгостроковий план розвитку, навчання персоналу, інвестиції у новітні технології, а також заходи, спрямовані на збереження конкурентних переваг у постійно змінюваному середовищі. Всі ці заходи сприяють створенню стійкої бізнес-моделі, що може адаптуватися до змін ринку і підтримувати високий рівень конкурентоспроможності.

Загалом, інтеграція ШІ в стратегію компанії є важливим кроком для створення стійкої бізнес-моделі, яка здатна адаптуватися до змінюваного середовища та підтримувати високий рівень конкурентоспроможності. Такий підхід включає довгостроковий

план розвитку, інвестиції у новітні технології, навчання персоналу і забезпечення етичних і правових норм, що сприяє підвищенню загальної ефективності і сталого розвитку компанії. Впровадження ШІ є ключовим для трансформації сучасного бізнесу, роблячи його більш ефективним, гнучким і готовим до викликів майбутнього.

Література

1. Brem, A., & Irrgang, E. (2020). Artificial Intelligence and the Future of Quality Management: A Literature Review and Conceptual Framework. Journal of Business Research, 119, с.105-118.
2. Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company, 83, с. 101-109.
3. Deming, W. E. (1986). Out of the Crisis. Massachusetts Institute of Technology, Center for Advanced Educational Services.
4. Juran, J. M., & Godfrey, A. B. (1999). Juran's Quality Handbook: The Complete Guide to Performance Excellence. McGraw-Hill.
5. Rai, A., & Tang, X. (2019). Artificial Intelligence in Operations Management: Research Opportunities and Future Directions. Journal of Operations Management, 65(5), с.473-491.
6. Інноваційні підходи до використання штучного інтелекту і роботів: Досвід Amazon. URL: http://surl.li/ompuji (дата звернення 23.11.2024).
7. Dastin, Jeffrey. "How Amazon Innovates in Ways that Google and Apple Can't." Reuters, 2018.

Зачек Олег Ігорович

доцент кафедри інформаційних технологій факультету № 2 Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ПРОБЛЕМИ ЗЛОЧИННОГО ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (ШІ) є дуже корисним в багатьох галузях діяльності. В тому числі він може бути використаний для покращення ефективності роботи правоохоронних органів та забезпечення публічної безпеки [1]. Але є і незаконні методи застосування ChatGPT [2]. Злочинне застосування ШІ є важливою проблемою, яка вимагає уваги як з боку суспільства, так і з боку влади.

Наприклад, злочинці легко обходять вбудований розробниками ChatGPT захист: заборону на створення шкідливого коду. Для цього вони просто розбивають завдання на кілька частин, щоб запити виглядали нейтральними. А потім за інструкціями від самого ж штучного інтелекту збирають їх в одну програму. Навіть ті, хто нічого не тямлять у програмуванні, створюють шкідливі програмні засоби під свої потреби, використовуючи ChatGPT як інструктора.

Ще одна популярна ніша незаконного використання нейромережі – соціальна інженерія. ChatGPT здатний без зусиль написати переконливий текст для фішингового сайту або листування, без помилок і з такими деталями, які введуть в оману користувача. Він може вести діалоги та переконувати людей у своїй правоті, створювати привабливі пропозиції для розсилок і наслідувати конкретну манеру спілкування, щоб видати себе за реально існуючу людину. ШІ може створювати дуже реалістичні

фішингові листи, повідомлення чи навіть телефонні дзвінки за допомогою голосових ботів.

Наступний спосіб застосування ChatGPT – можливість безпосередньо запитати його, як скоїти злочин з найбільшою вигодою, дізнатися про нові афери, схеми обману, отримати статистику щодо скоєних злочинів, щоб не конкурувати з іншими злочинцями, а також отримати розуміння, які помилки роблять інші шахраї, на чому їх ловить поліція і як цього уникнути. Таким чином, нейромережа перетворилася на інструмент, який приносить як користь, так і шкоду [2].

Також можливе використання алгоритмів ШІ для прогнозування або підбору паролів під час скоєння кіберзлочинів.

Ще одним напрямком використання штучного інтелекту в злочинних цілях є поширення дезінформації шляхом створення діпфейків для створення фальшивих відео чи аудіо, що імітують відомих людей, а також шляхом використання автоматизованих ботів, які масово розповсюджують дезінформацію в соціальних мережах.

Можливе використання технологій відтворення голосу людини з метою шахрайського отримання грошей або інформації. Також за допомогою інструментів ШІ можливо генерувати підроблені документи, підписи чи фото.

У процесі нелегальної діяльності у фінансовій сфері за допомогою ШІ можливе зловживання біржовими алгоритмами для маніпуляцій на фінансових ринках та аналізу схем відмивання грошей та пошуку способів їх оптимізації.

ШІ може використовуватись для аналізу великих обсягів даних із метою крадіжки ідентифікації осіб. Також можливе нелегальне застосування технології розпізнавання обличь для стеження за особами.

Для запобігання злочинному використанню ШІ необхідні законодавчі заходи, а саме створення чітких нормативів та правил використання ШІ. Але на думку адвоката Анастасії Клян правове визначення та регулювання застосування штучного інтелекту в українському законодавстві відсутні і відповідальність за неправомірне використання штучного інтелекту на даний час нормативно не закріплена [3]. Глоба Костянтин та Вахліс Інна вважають, що зміни у законодавство України для створення правових інструментів регулювання діяльності об’єктів штучного інтелекту є нагальними, крім цього необхідно передбачити юридичну відповідальність за шкоду, спричинену використанням штучного інтелекту [4].

Законодавство, що регулює використання штучного інтелекту, у інших країнах світу також не прийняте. Європейська Комісія запропонувала регламент щодо регулювання використання штучного інтелекту Artificial Intelligence Act, який активно обговорюється законодавцями ЄС, і 6 грудня 2022 року Рада ЄС ухвалила спільну позицію щодо цього регламенту. Але законом він стане лише після узгодження спільної версії тексту закону Радою ЄС та Європарламентом. У Канаді розробляється Закон про штучний інтелект і дані – Artificial Intelligence and Data Act (AIDA). Також на стадії розроблення подібні законодавчі акти є у США, Бразилії та інших країнах [5].

Роль ШІ у майбутньому буде лише зростати. Але є і значні проблеми, які необхідно вирішувати нагально. Найбільш значною проблемою є відсутність нормативно-правового регулювання застосування штучного інтелекту як у світі, так і в Україні. Тому необхідно розробити належне законодавство, яке б визначало правила використання технологій штучного інтелекту у різних галузях, що забезпечувало б захист

особистої інформації та запобігало б використанню таких технологій із злочинними намірами.

Література

1. 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. № 3 (2023). Львів: ЛьвДУВС, 2023. С. 148-156.
2. Гайдамашко Олександр. У Європолі попередили про шахрайські схеми з використанням ChatGPT // Новини 24. 30 березня 2023 р. URL: https://24tv.ua/tech/chatgpt-rozshiriv-mozhlivosti-shahrayiv-neochikuvanim-sposobom_n2284722 https://24tv.ua/tech/chatgpt-rozshiriv-mozhlivosti-shahrayiv-neochikuvanim-sposobom_n2284722 (дата звернення: 13.12.2024).
3. Клян Анастасія. Правове регулювання штучного інтелекту в Україні та світі // GOLAW. 03.02.2022. URL: https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/ (дата звернення: 13.12.2024).
4. Глоба Костянтин, Вахліс Інна. Закон України «Про штучний інтелект»: він є? // Юридична газета online. 13.03.2023. URL: https://yur-gazeta.com/publications/practice/ciyne-pravo-telekomunikaciyi/-zakon--ukrayini-pro-shtuchniy-intelekt-vin-e.html (дата звернення: 13.12.2024).
5. Котков Ігор. AI Act: що ЄС думає про штучний інтелект // Legal IT Group. 31.01.2023. URL: https://legalitgroup.com/ai-act-shho-yes-dumaye-pro-shtuchnij-intelekt/ (дата звернення: 13.12.2024).

Здебський Дмитро Володимирович

аспірант 3-го курсу заочної форми навчання докторантури та аспірантури Одеського державного університету внутрішніх справ

ВПРОВАДЖЕННЯ ЕЛЕКТРОННИХ БАЗ ДАНИХ ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Від початку повномасштабного вторгнення російських окупаційних військ поліграф зарекомендував себе як ефективний засіб виявлення колаборантів, представників публічної служби з наявним подвійним громадянством та шпигунів. Проте поліграф так само ефективно застосовується для виявлення осіб причетних до протиправної діяльності, та зокрема й корупції. Досить ефективно поліграф використовують підрозділи сектору безпеки і оборони України, а також приватними й державними банками в кадрових перевірках та службових розслідуваннях. Кількість поліграфологічних досліджень для зазначених потреб та підрозділів зростає у геометричній прогресії, свідченням тому є впровадження окремих поліграфологічних служб як в банківській сфері так і в складових сектору безпеки і оборони України. Будь-яким об’єктом поліграфологічного дослідження є інформація. Відповідно до Закону України «Про інформацію» інформація є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3]. Саме для оцінки достовірності повідомляємої інформації проводиться даний вид дослідження. Отримані дані результатів поліграфологічних досліджень мають цінні відомості які

потребують унормуванню. Відомості отримані в ході поліграфологічного дослідження містять персональні дані учасників поліграфологічного дослідження, а певні її складові відносяться до чутливих, що передбачає більш строгі вимоги до їх обробки.

Будь-яке поліграфологічне дослідження в секторі безпеки і оборони України підлягає документальній звітності. Закон України «Про інформацію» визначає, що документом є матеріальний носій, який містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі [3]. Так за результатами поліграфологічного дослідження поліграфолог складає наступні документи:

- довідку або інший звітний документ, до якого входить відомості про ініціатора, поліграфолога та суб'єкта опитування даного дослідження, що містять персональні дані,
- перелік запитань дослідження,
- методики дослідження, що застосовувались,
- відображення отриманого результату
- висновок.

Крім того, під час поліграфологічного дослідження утворюються додаткові матеріали, а саме: згода на процедуру поліграфологічного дослідження, поліграми (графічне відображення фізіологічних реакцій суб'єкта дослідження), довідки (про стан здоров'я), аудіо/відео матеріали та інші матеріали. Додаткові матеріали можуть мати викриваючи дані як на самого суб'єкта опитування так і на третіх осіб про причетність їх до службових порушень або до протизаконних діянь. Отримана інформація під час поліграфологічного дослідження може відноситись до:

- конфіденційної, в питаннях інформації про фізичну особу;
- інформація з обмеженим доступом, в питаннях аварій, катастроф, інших надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей, факти порушення прав і свобод людини, про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб [3];
- таємна, в питаннях оперативно-розшукової, розвідувальної, контррозвідувальної діяльності, державної та національної безпеки.

Отримана інформація за результатами поліграфологічних досліджень відповідно підлягає захисту. Захист інформації законодавець визначає, як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [3]. Адже дана інформація як мінімум вміщує персональні дані, тобто відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2].

Одним із напрямків роботи підрозділів кримінального аналізу є покращення інформаційно-аналітичної діяльності шляхом розроблення та впровадження сучасних програмних аналітичних інструментів [4, с. 60]. Накопичена інформація за результатами поліграфологічних досліджень може бути використана як джерело формування електронної бази даних для потреб кримінального аналізу. Електронна база даних поліграфологічних досліджень має бути нормативно-врегульована так як має вміщувати персональні дані та чутливу інформацію. Досліджуючи нормативно-правові документи, що регламентують поліграфологічні дослідження в секторі безпеки і оборони України, лише в Порядку проведення психофізіологічного дослідження із застосуванням поліграфа в Управлінні державної охорони України, визначено порядок зберігання

і використання матеріалів, що утворилися в результаті дослідження в електронному вигляді [1]. В решті складових сектору безпеки і оборони України порядок зберігання, використання та обробки матеріалів, які утворилися в результаті поліграфологічного дослідження в електронному вигляді не визначено, що унеможливлює використання їх не лише для формування електронної бази даних але, й взагалі, до використання у електронному документообігу.

В розробці бази даних поліграфологічних досліджень слід врахувати наступні відомості:

- ПІБ, посаду та підрозділ ініціатора, поліграфолога та суб'єкта дослідження;
- Тематику та тип дослідження (державна зрада, подвійне громадянство, корупція та ін.);
- Поліграфологічні методики та підходи, що застосовувались під час дослідження;
- Аудіо/відео-матеріали;
- Поліграми;
- Додаткові матеріали дослідження (згода, установки, аналітичні продукти та інше);
- Додатково отримана інформація під час дослідження;
- Висновок поліграфолога;
- Додаткова інформація (примітки, результати реалізації отриманої інформації і т.д.).

Окремо слід підняти питання про зберігання відеоматеріалів. Так, під час запровадження електронної бази поліграфологічних досліджень одного з державних банків України проблемним питанням було зберігання відеоматеріалів через їх великі об'єми пам'яті на електронних носіях, дану проблематику слід враховувати під час розробки відомчих електронних баз даних поліграфологічного дослідження.

Крім безпосереднього використання бази даних поліграфологічних досліджень для вирішення потреб кримінального аналізу вона може стати в нагоді підрозділам кадрового забезпечення, проведення рецензування або контролю якості роботи поліграфолога, аналітичній діяльності поліграфолога (кількість перевірок за певні періоди, їх результати, реалізація отриманої інформації та ін.), а також в наукових цілях (вибору кращої методики та підходу поліграфологічного дослідження в залежності від запиту, валідизації методик, їх ефективності та ін.). Так, в практиці поліції Великобританії результати поліграфологічних досліджень вносяться до загальної поліцейської бази, що дає змогу знайомитись з результатами уповноваженим особам, а також здійснювати дистанційний контроль якості роботи поліграфолога.

Зазвичай строки зберігання паперових довідок за результатами поліграфологічного дослідження три роки, проте при формуванні електронних баз даних, на нашу думку, інформація про причетність суб'єкта до правопорушення повинна зберігатись залежно від строків давності правопорушення, а для осіб стосовно яких не виявлено причетності до правопорушення на нашу доцільно розробити порядок знеособлення даних після трьох років.

Отже, база даних поліграфологічних досліджень може стати потужним аналітичним продуктом для потреб кримінального аналізу, так як має вміщувати інформацію про причетність до кримінальних правопорушень суб'єктів опитування. Для реалізації впровадження даного аналітичного інструменту слід:

1. Внести зміни до чинних інструкцій, що регулюють застосування поліграфа у відомстві, відносно можливості обробки інформації отриманої за результатами поліграфологічних досліджень в електронному вигляді;
2. Розробити електронні бази даних з врахуванням особливостей електронного документообігу та потреб відомства;
3. Спрогнозувати витрати на впровадження електронних баз даних з врахуванням коштовності електронних носіїв зберігання та обробки інформації.

Запровадження відомчих баз даних поліграфологічних досліджень або їх інтеграція в існуючі бази беззаперечно розширює можливості підрозділів кримінального аналізу, що підвищить якість аналітичних продуктів.

Література

1. Порядок проведення психофізіологічного дослідження із застосуванням поліграфа в Управлінні державної охорони України: затв. Наказом Упр. держ. охорони України від 09 лютого 2021 року № 95. URL: https://zakon.rada.gov.ua/laws/show/z0335-21#Text (20.10.2024).
2. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.10.2024).
3. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.10.2024).
4. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

Івануса Андрій Іванович

доцент кафедри управління інформаційною безпекою Львівський державний університет безпеки життєдіяльності, кандидат технічних наук, доцент

Брич Тарас Богданович

доцент кафедри управління інформаційною безпекою Львівський державний університет безпеки життєдіяльності, кандидат технічних наук, доцент

Ткаченко Артур Мар'янович

викладач кафедри управління інформаційною безпекою Львівський державний університет безпеки життєдіяльності

РОЗРОБЛЕННЯ ПРОГРАМИ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ ДЛЯ WEB-ДОДАТКІВ

Зі зростанням використання додатків також зросла потреба в заходах безпеки для захисту конфіденційних даних. Вразливості WEB-додатків можуть призвести до порушень безпеки, що у свою чергу може призвести до втрати особистої та фінансової інформації користувачів, заподіяння шкоди для репутації організацій і юридичних наслідків. Тому розробка автоматизованого пошуку вразливостей для додатків необхідна з метою виявлення та усунення проблем безпеки до того, як ними зможуть скористатися хакери. Таким чином виникає необхідність проведення дослідження, спрямованого на забезпечення всебічного розуміння методів, робочих інструментів та

методології, які можуть використовуватись для розробки механізму автоматизованого пошуку вразливостей у WEB-додатках.

Метою роботи є розроблення робочого інструменту для автоматизованого пошуку вразливостей у WEB-додатках.

Провівши інформаційний аналіз було встановлено, що найпоширенішими вразливостями WEB-додатків є SQL-ін’єкції, міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF), зламана автентифікація та управління сесіями, небезпечні прямі посилання на об'єкти [1].

Загалом, автоматизований інструмент пошуку вразливостей повинен надавати комплексне і надійне рішення для виявлення і зниження ризиків безпеки у WEB-додатках. Вибір оптимального методу розроблення автоматизованого інструменту пошуку вразливостей для WEB-додатків залежить від конкретних потреб і цілей проєкту. Однак комбінація статичного і динамічного аналізу коду часто ефективна при виявленні вразливостей. Крім того, машинне навчання можна використовувати для підвищення точності виявлення вразливостей [2].

Для розробки інструментів автоматизованого пошуку вразливостей для WEB-додатків потрібна відповідна системна архітектура і компоненти. Нижче наведено рекомендовану системну архітектуру та компоненти для проєктування системи автоматизованого пошуку вразливостей WEB-додатків: зовнішній інтерфейс, бекенд-сервер, сканери вразливостей, база даних, звітність, безпека, інтеграції з іншими інструментами та системами безпеки.

Загалом, системна архітектура і компоненти мають бути розроблені таким чином, щоб забезпечити надійний і всебічний автоматизований засіб пошуку вразливостей для WEB-додатків. Проєктована програма повинна вміти аналізувати пакети інформації та знайшовши в ньому пароль користувача, виводити повідомлення про загрозу і додавати сайт до списку небезпечних сайтів. Також у програмі необхідно передбачити функціональну можливість проєктованої системи виводити звіт її роботи у формі таблиці.

Враховуючи результати інформаційного аналізу найбільш поширених вразливостей WEB-додатків, порівняльного аналізу методів та технологій виявлення вразливостей було розроблено конкретні алгоритми для виявлення певних вразливостей, таких як SQL-ін’єкція та XSS [3, 4] .

Розробивши алгоритми роботи проєктованої системи, можна приступити уже до розроблення сканеру вразливостей WEB-додатків. Для цього можна використати мову програмування Python, середовище програмування Pycharm, WEB-сервер Apache, SQL-сервер MySQL (або щось інше залежно від компетенції розробників). Концептуальна модель роботи автоматизованої системи пошуку вразливостей WEB-додатків представлена на рисунку 5.

Опис схеми процесу перевірки:

- користувач: використовує клієнтську програму, щоб перевірити наявність вразливостей на WEB-сайті, зв’язавши сайт із тестовим сайтом;
- клієнтська програма під’єднується до сервера, завантажує відповідну WEB-сторінку, аналізує, щоб отримати всі пов’язані посилання. Після цього вона виконує відповідну атаку на WEB-сайті й отримує результат. Знову аналізує, чи містить WEB-сайт дефект і повідомляє користувача;

– серверна програма: отримує з’єднання з клієнтом, відповідає певним вимогам. З відповідними налаштуваннями для тестування на сервері, який містить будь-який WEB-сайт, що може містити недоліки. Згідно з аналізом інтерактивної моделі, ми моделюємо продуктивність програми на основі цих взаємодій.

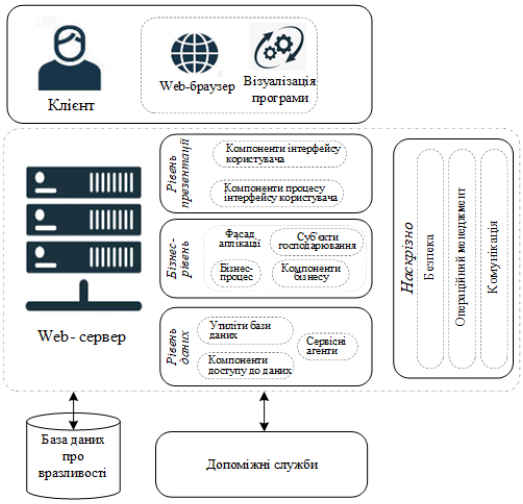

Рисунок 1 – Концептуальна модель автоматизованої програми для перевірки WEB-додатків на вразливість

Механізм сканування встановлює з’єднання із сервером, використовуючи посилання, надане користувачем через параметр. Потім він аналізує вхідні параметри, щоб ідентифікувати відповідний механізм сканування або зловмисника. За відсутності будь-яких параметрів рушій виконує сканування всіх компонентів. На сервері WEB-додатків можуть бути вразливості в мережі, базі даних або інші пов’язані вразливості, які роблять його сприйнятливим до проблем перевірки вхідних даних.

Висновки. Розробка автоматизованого інструменту пошуку вразливостей для WEB-додатків має вирішальне значення для забезпечення безпеки online-систем. Тому розроблено концептуальну модель роботи автоматизованої програми, що забезпечує ефективне та дієве сканування WEB-додатків на наявність вразливостей. Розробка модулів і функціональних можливостей цієї програми створює комплексний інструмент, який охоплює широкий спектр потенційних вразливостей. Запропоновані методи тестування та перевірка функціональності інструменту гарантують, що він працюватиме належним чином і даватиме надійні результати. Загалом розробка автоматизованого інструменту пошуку вразливостей є важливим кроком на шляху підвищення безпеки WEB-додатків.

Література

1. Open Web Application Security Project [Електронний ресурс]. Дата доступу: 10.11.2024. URL: https://owasp.org/
2. Цигой П., Степанчич Ж., Блажіч Б. Й. Широкомасштабний аналіз WEB-вразливості системи безпеки: висновки, проблеми та способи усунення // Gervasi O., et al. Обчислювальна наука та її застосування – ICCSA 2020. ICCSA 2020. Том 12253. Springer, Cham, 2020. DOI: 10.1007/978-3-030-58814-4_64.
3. Івануса А.І, Ткаченко А.М., Петрович А.З. Вдосконалення архітектури засобів автоматизовано-го пошуку вразливостей WEB-додатків // Інформаційна безпека та

інформаційні технології: збірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, С. 71-73.

4. Івануса А.І, Брич Т.Б., Ткач М.Ю. Розробка модулів і функціональності засобу автоматизованого пошуку вразливостей // Інформаційна безпека та інформаційні технології: збірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 203 С. 77-81.

Калашнік Євгеній Олександрович

старший інженер управління інформаційно-аналітичної підтримки ГУНП в Миколаївській області, лейтенант поліції

Рижков Едуард Володимирович

професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

АНАЛІТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ТЕРИТОРІАЛЬНИХ ПІДРОЗДІЛІВ ГОЛОВНИХ УПРАВЛІНЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Стрімкий стан розвитку громадянського суспільства в Україні продовжує сприяти тому, аби інформаційно-аналітичні підрозділи Національної поліції України постійно вдосконалювали підходи, специфіку, методи та засоби забезпечення службової діяльності територіальних підрозділів з метою належного, пропорційного, ефективного та своєчасного виконання функціональних обов’язків, відповідно до чинного законодавства.

Так, станом на сьогоднішній день, беззаперечно основними тенденціями розвитку інформаційно-аналітичного забезпечення у правоохоронній сфері варто визначити: вдосконалення засобів адміністрування та управління відомчими інформаційно-комунікаційними системами; централізацію та інтеграцію даних з доступних та наявних інформаційних, пошукових, аналітичних платформ та реєстрів; впровадження новітніх інформаційно-технічних інструментів для покращення методів взаємодії між поліцейськими; вирішення питань розгалуження комп'ютерних мереж; застосування спеціалізованих засобів захисту інформації; налагодження ефективних механізмів доступу та використання інформації в частині дотримання прав людини.

Оскільки інформаційно-аналітична діяльність стійко пов’язана з розвитком сучасних технологій та безпосередньо специфікою практичної діяльності територіальних органів (в т. ч. їх підрозділів) поліції в регіонах, досить багато аспектів проблематики, пов’язаної з інформаційно-аналітичним забезпеченням останніх потребує свого постійного дослідження та вдосконалення, особливо з огляду на невичерпні можливості спеціалізованого використання для потреб правоохоронної діяльності штучного інтелекту та машинного навчання [1].

Слід зауважити, що авторська думка та інтерес до обраної тематики були сформовані попередніми напрацюваннями науково-методичних матеріалів науковців, а також практичного досвіду виконання службових обов’язків в Управлінні інформаційно-аналітичної підтримки (далі - УІАП) Головного управління Національної поліції (далі - ГУНП) в Миколаївській області.

Згідно зі ст. 25, 26 Закону України «Про Національну поліцію» поліція в межах інформаційно-аналітичної діяльності формує, наповнює, підтримує в актуальному стані та користується реєстрами і базами даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України (далі – ЄІС МВС) [2].

Наповнення ЄІС МВС поліцейськими здійснюється за допомогою інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (далі – система ІПНП) відповідно до Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» затвердженого наказом МВС від 03.08.2017 № 676, зареєстрованим у Міністерстві юстиції України 28 серпня 2017 за № 1059/30927 (далі – Положення) [3].

Відповідно до п. 2 розділу IV Положення адміністратором системи ІПНП визначено уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України.

Зазначимо, що відповідно до пункту 2 Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України (далі – ДІАП), затвердженого наказом Національної поліції України від 31 січня 2020 року № 77 (зі змінами), ДІАП спрямовує та координує діяльність у сферах цифрової інфраструктури та цифрової трансформації процесів службової діяльності, інформаційно-аналітичної діяльності та діяльності, пов’язаної із забезпеченням усіма видами зв’язку структурних підрозділів центрального органу управління, територіальних підрозділів поліції тощо [4].

Таким чином, саме ДІАП з підпорядкованими УІАП ГУНП в регіонах, є відповідальними за організацію (здійснення) розроблення, упровадження, супроводження (адміністрування) інформаційних систем, комп’ютерних технологій, комунікаційних мереж та систем зв’язку для забезпечення діяльності органів (в т. ч. підрозділів) поліції.

Безумовним є те, що, напрямок інформаційно-аналітичної підтримки НПУ на сьогоднішній день охоплює значний пласт забезпечення службової діяльності та сучасних функціональних можливостей поліції. Саме перед фахівцями зазначених підрозділів постають завдання із забезпечення аналітичної обробки інформації, яка постійно накопичується у біля 80 підсистемах ІПНП, що у свою чергу, потребує високого технічного та інформаційно-аналітичного рівня підготовки, практичного досвіду та спеціалізованих навичок використання від працівників поліції. Однак, саме проблема автоматизованої аналітичної обробки службової інформації стає дедалі явною і потребує свого розв’язання.

Раніше ми неодноразово вказували на поточні проблеми у сфері інформаційно-аналітичного забезпечення поліцейської діяльності на різних етапах її розвитку [5]. Пропонували варіанти вирішення проблемних станів та покращення ситуації [6]. І серед іншого перевагу надавали питанням захисту службової інформації, що накопичується і обробляється у відповідних підсистемах [7]. При цьому впевнені, що разом із прогресивним розвитком відомчих технологій процес їх науково-дослідного супроводу повинен проводитись постійно саме для виявлення певних напрямів для подальшого вдосконалення.

Тож, на фоні збільшення міжвідомчих, відомчих систем та підсистем інформаційно-комунікаційної системи ІПНП постає нагальне питання щодо застосування аналітичного програмного забезпечення, здатного підвищити ефективність опрацювання накопиченої інформації, зменшити помилки суб’єктивного характеру, виявляти порушення вводу інформації та вживати додаткові заходи щодо її захисту [8, с. 83].

З причини відсутності централізованого програмного продукту аналітичного спрямування щодо опрацювання розрізненого інформаційного контенту та, наприклад, відеоконтенту з камер усіх рівнів відеоспостереження, представники територіальних підрозділів вимушені пристосовувати, доопрацьовувати та використовувати сторонні програмні продукти без відповідних процедур сертифікації, що безумовно породжує питання безпекового характеру. Такий стан не відповідає нормативам, встановленим законодавством держави, відомчим нормативно-правовим актам і особливостям воєнного стану в країні.

Тому в якості заходів щодо вирішення проблеми пропонуємо:

1. На рівні ДІАП визначити технічні завдання щодо розробки спеціалізованих інформаційно-аналітичних продуктів з метою створення або адаптація наявних інструментів для автоматизованої аналітичної обробки текстової, числової та відеоінформації.
2. Реалізувати інтеграцію нових рішень із підсистемами ІПНП для мінімізації ручної праці та посилення безпеки обробки інформації. Впровадити систему моніторингу якості даних для запобігання помилкам.
3. Проводити процедури авторської реєстрації, вітчизняної сертифікації та відомчої нормативно-правової регуляції всіх програмних рішень (програмних продуктів) перед їх практичним використанням.
4. Вжити заходів щодо підвищення кваліфікації працівників відповідних підрозділів у частині проведення тренінгів із роботи з новими технологіями, включаючи штучний інтелект та машинне навчання для розвитку технічних та аналітичних навичок.
5. Покращувати технічну інфраструктуру у підрозділах Національної поліції. Розширювати обчислювальних можливостей серверів для обробки великих даних. Забезпечувати територіальні підрозділи сучасними інформаційно-аналітичними засобами обробки інформації.
6. Залучати експертів і науковців для постійного вдосконалення інформаційно-аналітичних систем. Проводити регулярний аналіз тенденцій і загроз у сфері інформаційно-аналітичної та інформаційно-технічної підтримки поліції.

Ці заходи дозволять значно підвищити ефективність роботи інформаційно-аналітичних підрозділів Національної поліції України та покращать рівень інформаційної підтримки службової діяльності в умовах воєнного стану.

Література

1. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посібник / А.М. Гребенюк, Е.В. Рижков, Ю.П. Синиціна, С.О. Прокопов, Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2024. – 130 с.
2. Закон України «Про Національну поліцію». 2015. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
3. Наказ МВС України від 03.08.2017 No 686 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». 2017. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.
4. Наказ Національної поліції України 31.01.2020 року No 77 «Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної

поліції України». 2020. URL: – https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Struktura/Polohena11.pdf.
5. Дворецький О.О., Калюга Р.І., Паштета О.М., Рижков Е.В. Оптимізація деяких підсистем ІІПС ОВС та ІТС НПУ та інші питання в діяльності працівників ІАП ГУНП / О.О. Дворецький, Р.І. Калюга, О.М. Паштета, Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції України : матеріали всеукраїнського наук.-практ. семінару, м. Дніпро, 23 листопада 2018 року – Дніпро: ДДУВС, 2017. – С. 18 – 23.
6. Рижков Е.В. Деякі проблемні питання в роботі секторів інформаційної підтримки територіальних органах та підрозділах Національної поліції / Е.В. Рижков // Застосування інформаційних технологій у діяльності НПУ: науково-практичний семінар (21 грудня 2018 року, ХНУВС, м. Харків). – Харків: ХНУВС, 2018. – С. 57-58.
7. Дзех Я.С., Рижков Е.В. Проблемні питання інформаційно-аналітичного забезпечення в системі Національної поліції та проблемні питання щодо захисту інформації під час виконання службових обов'язків / Я.С. Дзех, Е.В. Рижков // Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання: Всеукраїнська науково-практична конференція (21 грудня 2018 р. м. Львів ЛьвівДУВС). – Львів: ЛьвівДУВС, 2019. – С. 83-86.
8. Рижков Е.В. Вдосконалення аналітичної складової Ситуаційних центрів НПУ засобами штучного інтелекту / Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 2 листопада 2023 року). – Дніпро: ДДУВС, 2023. – С. 82-85.

Калин Софія Петрівна

здобувач вищої освіти освітнього ступеня «бакалавр» спеціальності «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Огірко Ольга Ігорівна

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ІНСТРУМЕНТИ OSINT У СУЧАСНІЙ ОСВІТІ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

У сучасних умовах глобалізації та розвитку новітніх інформаційних технологій потрібно знати та розуміти, що таке інформація, як нею керувати та різні її аспекти. Інформація (від лат. informatio – роз'яснення, виклад фактів, подій, представлення, поняття, ознайомлення, просвіта) – це зафіксовані в документній формі або публічно виголошені відомості про події та явища в суспільстві, державі чи довкіллі, які людина сприймає за допомогою власних органів чуття або спеціальних пристроїв [1]. Розвиток інформаційних технологій, які являють собою систему методів, процесів та способів використання обчислювальної техніки й систем зв'язку для створення, збору, передачі, пошуку, оброблення та поширення інформації, дозволив значно змінити повсякденне життя. Завдяки ІТ стали можливими автоматизація процесів, швидкий доступ до даних і нові форми комунікації, що суттєво підвищують ефективність організації діяльності

людей. Важливим напрямком у цьому є застосування OSINT(Open Source Intelligence), який може служити корисним інструментом для досліджень і безпеки.

Технології OSINT дозволяють використовувати відкриті джерела інформації, які доступні без спеціальних дозволів. Це можуть бути медіа, соціальні мережі, державні реєстри, комерційні бази даних, наукові публікації та інші джерела. В умовах швидкого розвитку технологій, таких як Інтернет речей(IoT), штучний інтелект та великі дані, інформація, яка раніше була б недоступною або важко досяжною, сьогодні може бути ефективно зібрана і проаналізована.

Одним з основних застосувань OSINT є моніторинг інформаційних потоків у реальному часі для виявлення потенційних загроз. За допомогою інструментів OSINT можна оперативно оцінювати стан безпеки на різних етапах: від попередження загроз до оцінки наслідків від їх реалізації [2]. У секторі безпеки України: це може включати аналіз публічних повідомлень, моніторинг соціальних мереж на предмет дезінформації або аналіз стану критичної інфаструктури.

Технології OSINT охоплюють велику кількість різноманітних інструментів та методик, що дозволяють отримувати інформацію з різних відкритих джерел.

Основними аспектами застосування *OSINT* є (рис 1):

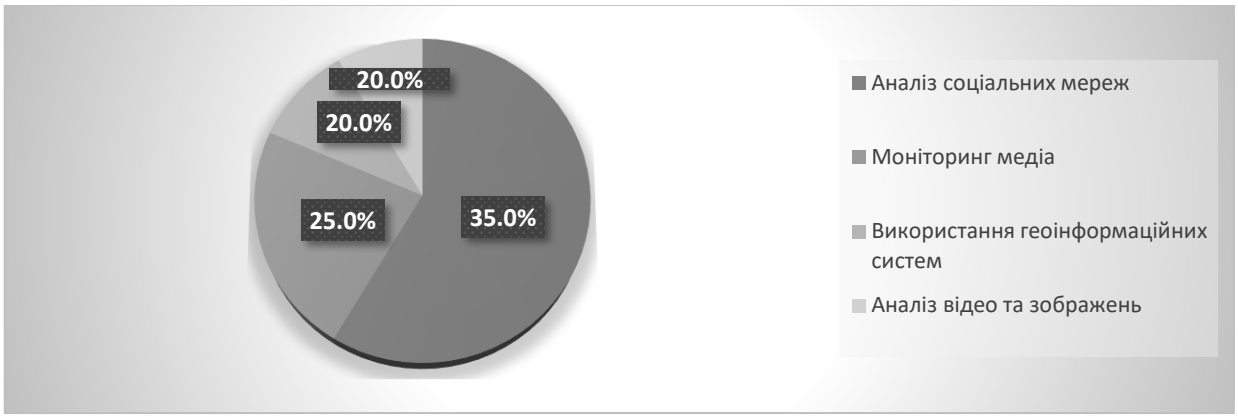

Рис.1 Статистичні дані застосування OSINT

1. Аналіз соціальних мереж: соціальні мережі, такі як Facebook, Twitter(X), Instagram, є одним з найбільших джерел інформації, де можна виявляти різноманітні загрози – від інформаційних атак до актів насильства чи дестабілізації суспільства. Аналіз цих платформ за допомогою автоматизованих систем дозволяє швидко виявляти загрози та реагувати на них.
2. Моніторинг медіа: новинні сайти та інші медіа платформи містять велику кількість корисної інформації для оцінки політичної та соціальної ситуації в країні.
3. Використання геоінфомаційних систем: застосування геопросторових даних, таких як карти, GPS-трекінг, є важливим для оцінки та прогнозування ситуацій на полі бою або для моніторингу інфаструктури.
4. Аналіз відео та зображень: завдяки розвитку технологій обробки зображень можна автоматично аналізувати відео та фотографії для виявлення можливих загроз, таких як зміни на території, загрози в інфаструктурі чи масові протести [1-6].

Інструменти OSINT відіграють важливу роль у підготовці фахівців, здатних ефективно працювати з відкритими даними. Вони допомагають не лише отримувати інформацію з відкритих джерел, а й сприяють розвитку важливих компетентностей: пошуку, аналізу, інтерпретації та використання відкритої інформації у професійній діяльності.

Інтеграція інструментів Maltego, IBM i2, Analyst's Notebook, DataMiner у навчальний процес дозволить здобувачам вищої освіти: застосовувати теоретичні знання на практиці, здобувати реальний досвід роботи з даними, розвивати аналітичне мислення, аналізувати актуальні інформаційні потоки, формувати прогнози щодо можливого розвитку ситуацій.

У результаті навчання здобувачі зможуть опанувати такі практичні навички:

- використання Google Dorking для розширеного пошуку в інтернеті;
- робота з державними реєстрами для отримання відкритих даних;
- виконання деанонімізації осіб;
- проведення зворотного пошуку зображень;
- організація OSINT-розслідувань;
- визначення геолокації за зображеннями;
- пошук особистих даних у Google і соціальних мережах;
- визначення погоди в минулому;
- робота з Google Cache, Google Maps та Street View для встановлення локації;
- використання Webarchive та Wayback Machine;
- проведення фактчекінгу.

Такий комплекс знань і навичок забезпечить високий рівень підготовки майбутніх фахівців до вирішення складних професійних завдань у сфері безпеки та оборони.

Впровадження OSINT в освітній процес має і певні виклики, зокрема це забезпечення інформаційної безпеки. Робота зі значними обсягами відкритих даних під час навчального процесу може створювати ризики витоку конфіденційної інформації або несанкціонованого доступу до навчальних матеріалів, тому виникає необхідність розробити ефективні заходи захисту навчальних баз даних, впровадження сучасних систем кібербезпеки. Ще одним викликом є етичні та правові питання, важливо дотримуватись етики та законодавства при зборі даних, щоб уникнути порушення прав людини чи конфіденційності.

Інтеграція OSINT у навчальний процес, врахувавши наявні виклики, є перспективним і потужним інструментом для підготовки фахівців, здатних вирішувати складні завдання в умовах сучасних інформаційних викликів. Впровадження цих технологій у систему освіти сприятиме формуванню компетентностей, що відповідають актуальним потребам секторів безпеки та оборони.

Література

1. Інформація та інформаційні технології : https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. OSINT Framework : https://osintframework.com/
3. Програми підготовки в галузі OSINT https://www.issp.training
4. Звіти з кібербезпеки та аналітики даних https://www.gartner.com/en

5. Офіційна документація та посібники OSINT https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059_qa1a.pdf
6. Матеріали про геоінформаційні системи https://esri.in.ua
7. Дослідження та звіти у сфері аналізу соціальних мереж і медіа https://www.hootsuite.com

Калугін Володимир Юрійович
професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ

ВІДЕОАНАЛІТИКА У КРИМІНАЛЬНОМУ АНАЛІЗІ

В умовах сучасного світу, де технології стрімко розвиваються, відеоналітика стає важливим інструментом у діяльності підрозділів кримінального аналізу. Використання відеоаналізу дозволяє правоохоронним органам ефективно обробляти та аналізувати великі обсяги відеоданих, що у подальшому сприяє розкриттю, попередженню, профілактиці кримінальних правопорушень, підвищенню безпеки та забезпеченню правопорядку.

Відеоаналітика – це технологія, що дозволяє автоматично аналізувати відеопотоки з метою виявлення та розпізнавання об'єктів, подій і поведінки. Використовуючи алгоритми машинного навчання та штучного інтелекту, відеоналітика може автоматично обробляти відеопотоки з камер спостереження, що дозволяє швидше обробляти великі обсяги відеоданих, що значно зменшує час, необхідний для розслідувань і сприяє виконанню завдань що полегшує роботу аналітиків.

Основним джерелом отримання інформації є системи відеоспостереження, оснащені програмним забезпеченням яке забезпечує можливість проведення подальшого дослідження. Вони дозволяють виявляти підозрілі дії в реальному часі та оперативно реагувати на загрози. Серед компаній, що розробляють такі системи, лідерами є: корпорація NEC (Японія), «FACE ++» Neurotechnology (Литва), і Cognitec Systems GMBH (Німеччина), а також український виробникм активного обладнання та камер відеоспостереження ZetPro, програмно-апаратного комплексу САМАР (vers. VMS). [1]

Можливо акцентувати увагу на основних видах відеоаналітики:

1. Вважається, що найважливішою складовою відеоаналітики є розпізнавання осіб - ідентифікація осіб з бази даних для контролю доступу або пошуку злочинців. є розпізнавання обличчя, яке знаходить застосування в різних сферах, включаючи безпеку, маркетинг, охорону здоров'я та багато інших. Цей напрямок є складним завданням, яке вимагає використання сучасних алгоритмів машинного навчання, комп'ютерного зору та великих обсягів даних.
2. Наступною складовою можливо вважати контроль автомобільного руху, який полягає у розпізнаванні номерних знаків, визначення типу автомобіля та оцінка швидкості руху. Такі системи відеоспостереження використовуються для формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», призначеної для обробки відомостей про транспортні засоби та номерні знаки транспортних засобів, що розшукуються в рамках кримінальних, виконавчих проваджень,

проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду [2].

3. Аналіз поведінки – визначає аномальну поведінку, наприклад тривалого знаходження об’єкта спостереження у певній зоні, що може вказувати на потенційно небезпечні ситуації та дозволяє виявляти аномальні чи підозрілі дії, які можуть свідчити про підготовку чи вчинення кримінального правопорушення. У цьому випадку системи відеоспостереження в реальному часі забезпечують моніторинг ситуації на місцях подій.

Для аналітичної обробки використовується фото- і відеоінформація, отримана з технічних засобів і технічних приладів, які мають функції фото- і відеофіксації (запису), закріплених поліцією на службових транспортних засобах, розміщених по зовнішньому периметру доріг і будівель, а також інформація, отримана з автоматичної фото- і відеотехніки, що знаходиться у приватному володінні.

Спеціалізоване програмне забезпечення створене для формування та ведення ІП «Гарпун», аналітичної обробки й інформування про розшук ТЗ або номерного знаку для запобігання вчиненню правопорушень, аналізу тимчасового набору даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку, одночасного перебування на різних транспортних засобах, використання знищених знаків, а також для автоматизованого інформування про такі факти диспетчерів, оперативних чергових, нарядів поліції органів (підрозділів) поліції та ініціаторів розшуку. [3].

Відеозаписи можуть слугувати важливими доказами в судових справах. Використання відеоаналітики для аналізу цих записів підвищує їхню цінність у правовій системі, однак, слід врахувати, що якість відеоданих може суттєво вплинути на результати аналізу. Погане освітлення, низька роздільна здатність та інші фактори можуть ускладнити розпізнавання об'єктів і осіб.

В ході проведення аналітичного дослідження постають питання які слід врахувати. Це, конфіденційність, етичні питання та право на приватність. Важливо щоб технології забезпечили баланс між безпекою та правами громадян і не порушували права людини, або для масового спостереження без належної підстави. Важливо також дотримуватися принципів прозорості та підзвітності у використанні відеоданих. Порядок отримання інформації, використання технологій доступу, типів наборів даних, обсяг і структура даних, до яких надається доступ з автоматичної фото- і відеотехніки, що знаходиться у приватному володінні, відповідно до потреб Національної поліції України визначаються згідно із законодавством України.

Як висновок, відеоаналітика є потужним інструментом у діяльності підрозділів кримінального аналізу, що дозволяє ефективно обробляти та аналізувати відеодані для розкриття злочинів і підвищення безпеки. Однак її використання супроводжується низкою викликів і етичних питань, які потребують ретельного розгляду. Тільки шляхом розробки чітких норм і стандартів можна досягти справедливості та прозорості у використанні відеоаналітики в кримінальному аналізі.

Література

1. Публікація на телеграм каналі «Printerfort» від 09.05.2022. URL: https://web.telegram.org/k/#@printerfort.
2. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 13.06.2018 № 497 // База

даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.-gov.ua/laws/show/z0787-18 (дата звернення: 10.12.2024).
3. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду: методичні матеріали для працівників підрозділів поліції / [уклад. В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов, В. В. Чумак, В. А. Світличний] ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 44 с.

Ковалів Мирослав Володимирович

завідувач кафедри адміністративно-правових дисциплін Навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

Качмарик Олег Іванович,

здобувач вищої освіти Навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ

РОЛЬ АДМІНІСТРАТИВНОГО ТА ІНФОРМАЦІЙНОГО ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Одним із пріоритетних стратегічних напрямів у Європейському Союзі є розвиток інформаційного суспільства. Цьому питанню Україна у контексті Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, приділяє велику увагу, а також виділяються значні фінансові ресурси. Правові основи формування та розвитку інформаційного суспільства зазначені як самостійний напрям для наукових досліджень у Пріоритетних напрямах фундаментальних та прикладних наукових досліджень в галузі права Національної академії правових наук України на 2021-2025 роки (розділ 1.9).

Роль правового регулювання адміністративного та інформаційного права в інформаційному суспільстві дозволяє підійти до визначення меж цього регулювання. Інформаційне суспільство є об’єктом правового регулювання. Це зумовлено тим, що важливі суспільні відносини, зокрема суспільні відносини в інформаційному суспільстві, підлягають правовому регулюванню.

Виходячи з сутності інформаційного суспільства та основного призначення права випливає, що суспільні відносини в інформаційному суспільстві регулюються всіма галузями права. Кожна галузь права регулює певний спектр суспільних взаємин у інформаційному суспільстві залежно від предмета правового регулювання. У цьому плані правове регулювання суспільних відносин в інформаційному суспільстві нічим не відрізняється від правового регулювання суспільних відносин в індустріальному суспільстві.

Цифровізація впливає на розвиток публічно-правового регулювання, що розширюється у сфері використання цифрової інформації та застосування інформаційних технологій фізичними та юридичними особами, органами публічної влади. Її виникнення зумовило розвиток інформаційної інфраструктури – повсюдне впровадження

цифрових каналів зв'язку, що розширюють можливості та умови здійснення інформаційної діяльності.

Цифровізація призводить до виникнення взаємозв'язків між різними сферами людської діяльності, у тому числі до збільшення цінності інформації в управлінні та появі нових об'єктів у віртуальному середовищі. Адміністративне право України не може не реагувати на зміни у суспільних відносинах, пов'язаних із розвитком інформаційного суспільства [1, с. 1003].

Визначення меж адміністративно-правового регулювання відносин в інформаційному суспільстві буде неможливим без звернення до питання про предмет адміністративного права як галузі.

Для визначення меж адміністративно-правового регулювання інформаційного суспільства, визначення меж предмета адміністративного права у регулюванні доцільно розглянути формат адміністративно-правового регулювання суспільства.

Екстраполяція отриманих висновків на адміністративно-правове регулювання інформаційного суспільства буде доречною, оскільки збільшення ролі інформаційних технологій, інформації, знань та якісні перетворення в суспільстві не повинні вплинути на зміну меж публічно-правового регулювання суспільства.

Якщо розглядати інформаційне суспільство як суспільство нового типу, межі адміністративно-правового регулювання суспільства нового типу залишилися незмінними. Цей висновок можна зробити на підставі аналізу Стратегії реформування державного управління на 2021-2025 роки, Стратегії здійснення цифрового розвитку, цифрових трансформацій та цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації, Національної економічної стратегії на період до 2030 року [2; 3; 4].

Межі інформаційно-правового регулювання відносин у інформаційному суспільстві зумовлюються двоєдиною природою предмета інформаційного права. По-перше, галузь інформаційного права встановлює основи існування та розвитку інформаційного суспільства загалом (в усіх сферах інформаційного суспільства).

По-друге, галузь інформаційного права детально регулює відносини в інформаційному суспільстві, що складаються у сферах, що становлять основні елементи держави: інформаційні технології використовуються у суспільних відносинах, пов'язаних з реалізацією різних форм здійснення влади народом (електронна петиція), організація та механізм діяльності органів державної влади та місцевого самоврядування (електронне урядування).

Виходячи з меж адміністративно-правового регулювання відносин в інформаційному суспільстві, можна зробити висновки щодо джерел правового регулювання відносин в інформаційному суспільстві, відповідно, місці адміністративного права в даному регулюванні. Закріплення основ існування та розвитку інформаційного суспільства здійснюється виключно на рівні Конституції України, але управління належить до прерогатив галузі адміністративного права.

Детальне регулювання відносин в інформаційному суспільстві, які складаються в галузях, що становлять основні елементи держави, здійснюється не так на рівні Конституції України, як на рівні інших джерел права. Детальне регулювання відносин у інформаційному суспільстві за іншими сферах життя здійснюється іншими галузями права.

Заслуговує на окрему увагу питання про місце та роль галузі інформаційного права в системі правового регулювання.

Інформаційна сфера інформаційного суспільства та її правове регулювання займають центральне місце в інформаційному суспільстві, що обумовлюється значенням інформації та інформаційної сфери в суспільстві нового типу, проте інформація та інформаційна сфера не є єдиними об'єктами правового регулювання в інформаційному суспільстві. Існують об'єкти правового регулювання: інформаційна інфраструктура, електронні комунікацій, публічні інформаційні ресурси, забезпечення інформаційної та кібербезпеки, мережа Інтернет [1, с. 1005].

З цієї причини у галузей адміністративного та інформаційного права різна роль регулювання відносин в інформаційному суспільстві, обумовлена різними предметами правового регулювання. Незважаючи на це, не можна не відзначити взаємозв'язок адміністративно-правового та інформаційно-правового регулювання відносин в інформаційному суспільстві, що полягає у взаємодії галузей адміністративного та інформаційного права щодо регулювання відносин в інформаційній сфері інформаційного суспільства.

Література

1. Ковалів М., Єсімов С., Пєтков С., Козяр Р., Хмиз М. Співвідношення адміністративного та інформаційного правового регулювання відносин в інформаційному суспільстві. Traektoriâ Nauki = Path of Science. 2023. Vol. 9. № 9. С. 1001-1007.
2. Деякі питання реформування державного управління України: Розпорядження Кабінету Міністрів України від 21.07.2021 р. № 831-р. URL. https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#Text
3. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровизації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації: Розпорядження. Кабінету Міністрів України від 17.11.2021 р. № 1467-р. URL. https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text
4. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL. https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#n25

Кочман Костянтин Павлович

аспірант кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ

Форос Ганна Володимирівна

завідувачка кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У СЕКТОРІ ОБОРОНИ УКРАЇНИ

Сучасний світ характеризується стрімким розвитком інформаційних технологій, що сприяє зростанню їх значущості в усіх сферах суспільного життя. Разом із цим

посилюється і загроза кібернетичних атак, які становлять серйозний виклик для державних органів, критичної інфраструктури та оборонного сектора. Для України, яка знаходиться в умовах тривалого збройного протистояння, забезпечення кібербезпеки є не лише важливим елементом національної безпеки, але й необхідною умовою збереження суверенітету та стабільності держави.

Протидія кіберзагрозам у секторі оборони вимагає комплексного підходу, що включає розробку сучасних технічних засобів, удосконалення нормативно-правової бази, підвищення рівня професійної підготовки фахівців та ефективної координації між органами державної влади. У цьому контексті інформаційне забезпечення виступає ключовим елементом, що дозволяє оперативно ідентифікувати загрози, оцінювати їх потенційні наслідки та забезпечувати адекватну реакцію на кіберінциденти [3, с. 94].

Розв'язання повномасштабної агресії проти України значно посилило значення кіберпростору як ще одного фронту сучасної війни. Кібербезпека стала критично важливою складовою національної оборони, адже ворог активно використовує інформаційні технології для здійснення атак на державні установи, військову інфраструктуру та системи управління.

У перші дні війни було зафіксовано значний сплеск кібератак, спрямованих на виведення з ладу критичних інформаційних систем. Проте завдяки швидкому реагуванню та підтримці міжнародних партнерів Україна змогла зміцнити захист своїх інформаційних систем. Зокрема:

- розширено інфраструктуру центрів реагування на інциденти кібербезпеки (CERT-UA), які координують виявлення та нейтралізацію атак;
- впроваджено додаткові засоби моніторингу інформаційних систем для виявлення загроз у реальному часі;
- збільшено використання хмарних технологій, що забезпечило резервне копіювання критичних даних та підвищило стійкість систем до атак.

Попри це, залишається проблема недостатньої інтеграції інформаційних систем оборонного сектору в єдину платформу, що ускладнює координацію в умовах масштабних кібератак.

Оборонний сектор України стикається з такими основними кіберзагрозами:

- атаки на системи управління військами: злам каналів зв'язку, спроби викрадення або маніпуляції оперативними даними;
- руйнування критичної інфраструктури: зловмисники атакують енергетичні, логістичні та транспортні системи, які забезпечують функціонування збройних сил;
- розповсюдження шкідливого програмного забезпечення: використання вірусів типу wiper для знищення даних та дестабілізації роботи систем;
- кіберрозвідка та шпигунство: спроби з боку противника отримати доступ до закритої інформації через фішингові атаки, уразливості в системах або використання інсайдерів;
- інформаційно-психологічні операції: дезінформація та маніпуляції в інформаційному просторі, спрямовані на деморалізацію військових і населення [4, с. 25–26].

Основні недоліки в наявному інформаційному забезпеченні кіберзахисту в секторі оборони України значною мірою пов'язані з організаційними, технічними та

кадровими аспектами. Однією з ключових проблем є недостатня координація між підрозділами, що ускладнює обмін інформацією в умовах масштабних атак.

Серйозною перешкодою також є дефіцит висококваліфікованих фахівців у сфері кіберзахисту. Обмежена кадрова спроможність не дозволяє оперативно виявляти та нейтралізувати загрози, що особливо критично в умовах повномасштабної війни. Водночас значна частина обладнання та програмного забезпечення залишається застарілою та не відповідає сучасним стандартам кібербезпеки, що робить систему більш вразливою до атак.

Проблема фінансування є ще одним важливим аспектом. Незважаючи на міжнародну підтримку, значна кількість проєктів у сфері кіберзахисту залишається недофінансованою, що обмежує можливості для модернізації інфраструктури [3, с. 96].

Модернізація технічної інфраструктури є одним із ключових завдань забезпечення ефективного кіберзахисту в оборонному секторі України. Сучасні технологічні платформи здатні забезпечити швидку обробку великих обсягів даних, підвищити стійкість до атак і сприяти інтеграції з міжнародними системами. У цьому контексті особливо перспективним є використання систем штучного інтелекту (ШІ), які можуть автоматично виявляти аномалії в мережах, аналізувати поведінку потенційних зловмисників і прогнозувати можливі сценарії атак. Завдяки ШІ, не лише зменшується час реагування на загрози, але й підвищується точність і ефективність нейтралізації кібератак [2, с. 168].

Ще одним важливим напрямом є застосування блокчейн-технологій для забезпечення цілісності даних і захисту критичних транзакцій. Децентралізована структура блокчейну унеможливлює несанкціоноване втручання або зміну даних, що робить його ідеальним для використання у військових логістичних системах чи під час зберігання конфіденційної інформації. Водночас модернізація мережевого обладнання та програмного забезпечення до стандартів НАТО забезпечить сумісність українських систем із міжнародними платформами, підвищить рівень безпеки і створить умови для більш тісної співпраці з партнерами. Це дозволить створити надійну інфраструктуру, здатну протистояти сучасним кіберзагрозам у контексті повномасштабної війни [4, с. 29].

Ефективна координація оборонного сектору потребує створення інтегрованої платформи для захищеного обміну інформацією в реальному часі, з використанням сучасних криптографічних алгоритмів для захисту даних і механізмів адаптації до нових кіберзагроз. Водночас ключовим аспектом є підготовка висококваліфікованих фахівців через розробку освітніх програм, регулярну сертифікацію та залучення міжнародних експертів для тренінгів, що забезпечить оперативне реагування на сучасні атаки та підвищить стійкість систем [1, с. 113].

Важливо зазначити, що швидке та ефективне реагування на кіберзагрози в сучасних умовах неможливе без впровадження автоматизованих систем. Аналітичні платформи SOC (Security Operations Center) дозволяють централізовано виявляти та класифікувати загрози, аналізувати аномалії в мережевому трафіку та прогнозувати можливі сценарії атак. Використання цих платформ значно скорочує час між виявленням атаки та її нейтралізацією, підвищуючи загальний рівень безпеки систем. Також критично важливим є використання цифрової криміналістики (digital forensics), яка дозволяє ретельно досліджувати інциденти, ідентифікувати джерела атак і відстежувати методи зловмисників, що допомагає уникати повторення подібних загроз у майбутньому.

Окрім виявлення та розслідування, велике значення має відновлення систем після атак. Використання систем резервного копіювання з високим рівнем відмовостійкості забезпечує оперативне повернення до роботи навіть після серйозних кіберінцидентів. Завдяки сучасним технологіям резервування можна мінімізувати втрати даних та скоротити час простою критичної інфраструктури, що є особливо важливим у військових умовах [1, с. 115].

Ефективний кіберзахист також потребує активної співпраці з міжнародними партнерами. Участь України у спільних навчаннях, таких як Locked Shields, організованих НАТО, сприяє підвищенню рівня підготовки українських фахівців та інтеграції у міжнародне кібербезпекове співтовариство. Інтеграція до глобальних систем обміну інформацією про загрози, таких як STIX / TAXII, дозволяє оперативно отримувати дані про новітні загрози та методи атак, що значно підвищує здатність реагувати на сучасні виклики.

Використання досвіду міжнародних партнерів є важливим для вдосконалення національної кіберстратегії. Впровадження передових технологій, отриманих завдяки співпраці, сприяє зміцненню кібербезпеки держави. Крім того, міжнародна взаємодія дозволяє Україні не лише отримувати підтримку, а й ділитися власним досвідом протидії кіберзагрозам в умовах гібридної війни, що підвищує її роль на глобальному рівні [2, с. 174–175].

Отже, умови повномасштабної війни вимагають від України негайного вдосконалення системи інформаційного забезпечення кібербезпеки в оборонному секторі. Модернізація технічної інфраструктури, впровадження інноваційних технологій, підвищення рівня підготовки персоналу та поглиблення міжнародного співробітництва дозволять створити стійку систему протидії кіберзагрозам. Реалізація цих заходів не лише забезпечить ефективну кібероборону, а й зміцнить позиції України у глобальному інформаційному просторі.

Література

1. Гуцалюк М. В. Особливості протидії кіберзлочинності під час воєнного стану. Інформація і право. 2023. № 3. С. 108–117.
2. Гуцалюк М. В. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. Інформація і право. 2024. №2 (49). С. 164–177.
3. Машталір В. та ін. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. Т. 49. №1. С. 93–104. DOI: https: // doi. org / 10.33099 / 2311–7249 / 2024–49–1–93–104.
4. Терновий О., Шкуренко О., Міненко Л. Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. № 1 (46). С. 23–31.

Кукурудза Олег Андрійович
курсант 3-го курсу, ННІПФПКП Львівського державного університету внутрішніх справ
Поляк Святослав Петрович
В.о. завідувача кафедри оперативно-розшукової діяльності, ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНО-АНАЛІТИЧНІ ТЕХНОЛОГІЇ ПРАВООХОРОННИХ ОРГАНІВ, ЯКІ СПІВПРАЦЮЮТЬ З ІНТЕРПОЛОМ ТА ЄВРОПОЛОМ ПІД ЧАС РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

В умовах російського повномасштабного вторгнення одним із ключових завдань в рамках кримінального провадження є чітка організація досудового розслідування в рамках міжнародного співробітництва. Для ефективного розслідування таких злочинів необхідна тісна співпраця між різними національними та міжнародними органами, а також використання передових інформаційно-аналітичних технологій. Важливу роль у цій роботі відіграють міжнародні організації, зокрема Інтерпол і Європол, які забезпечують координацію та обмін інформацією між правоохоронними органами різних країн. Саме тому особливо важливим постає дослідження інформаційно-аналітичних технологій правоохоронних органів, які співпрацюють з Інтерполом та Європолом під час розслідування воєнних злочинів.

Перш за все потрібно зазначити, що Інтерпол (Міжнародна організація кримінальної поліції) – це міжнародна організація, яка забезпечує співпрацю між національними правоохоронними органами для боротьби зі злочинністю. Одним із основних завдань Інтерполу є обмін інформацією про злочинців, розслідування злочинів, а також надання технічної та консультаційної допомоги під час розслідувань. Завдяки своїй глобальній мережі та ефективним каналам комунікації Інтерпол може координувати дії правоохоронних органів у різних країнах, що має важливе значення при розслідуванні воєнних злочинів, які часто виходять за межі однієї держави [1].

Європол (Європейське поліцейське управління), у свою чергу, є агентством ЄС, яке координує діяльність правоохоронних органів країн-членів ЄС у боротьбі з транснаціональними злочинами. Європол збирає, аналізує та обмінюється інформацією про кримінальні загрози та злочинців, а також підтримує оперативне співробітництво між національними поліціями. В умовах воєнних злочинів, які можуть мати вплив на кілька європейських країн, Європол відіграє ключову роль у забезпеченні безпеки та правосуддя.

Сучасні інформаційно-аналітичні технології займають центральне місце у розслідуванні воєнних злочинів. Завдяки технологіям можна швидко збирати, аналізувати та передавати інформацію між різними країнами та організаціями, що значно підвищує ефективність слідчих дій.

На сьогодні одним з основних інструментів для міжнародної співпраці є різні бази даних, що зберігають інформацію про злочинців, місця злочинів, докази та інші критичні відомості. Інтерпол та Європол мають доступ до таких баз даних, які включають інформацію про терористів, воєнних злочинців, викрадені культурні цінності, а також про зброю, боєприпаси і військові засоби. Системи, як I-24/7 Інтерполу, забезпечують національним поліцейським доступ до актуальної інформації, що дозволяє швидко реагувати на загрози та слідкувати за злочинною діяльністю на міжнародному рівні.

Використання методів аналізу великих даних дає змогу правоохоронцям обробляти величезні обсяги інформації про злочини, фінансові потоки, переміщення осіб, а також інші дані, що можуть допомогти у виявленні злочинної діяльності. Це особливо важливо під час розслідування воєнних злочинів, оскільки інформація може бути різноманітною і надходити з багатьох джерел: від свідків, журналістів, правозахисників, громадських організацій, а також з онлайн-платформ [2, с. 55].

Однак, у сучасному світі воєнні злочини часто супроводжуються великим обсягом цифрових доказів, таких як електронні листи, записи на мобільних телефонах, фотографії та відео, що зберігаються в Інтернеті. Криміналісти використовують сучасні технології для збору, збереження та аналізу таких даних. Використання систем штучного інтелекту (ШІ) для аналізу цифрових доказів дозволяє автоматично ідентифікувати ключові елементи, які можуть бути важливими для розслідування.

Крім того, воєнні злочини часто супроводжуються інтенсивним використанням соціальних мереж та Інтернету для пропаганди насильства, координації дій або приховування доказів. Використання технологій для збору та аналізу відкритих джерел інформації дозволяє виявляти зв'язки між підозрюваними, вивчати їх діяльність та виявляти можливі місця скоєння злочинів. При цьому, геоінформаційні системи дають змогу візуалізувати та аналізувати просторові дані, такі як місця скоєння воєнних злочинів, переміщення злочинців або витоки інформації про військові операції. Це особливо корисно для з’ясування обставин злочинів, таких як напади на мирне населення, знищення інфраструктури, насильство над цивільними.

На нашу думку, ключову роль у розслідуванні воєнних злочинів на міжнародному рівні відіграє координація дій між Інтерполом, Європолом і національними правоохоронними органами. Ця співпраця забезпечується через обмін інформацією, спільне використання аналітичних технологій, а також проведення спільних операцій. Інтерпол та Європол надають технічну підтримку, сприяють у розробці стратегій розслідування, а також організовують навчання для правоохоронців щодо розслідування воєнних злочинів. Інтерпол, зі своєю мережею національних підрозділів, має можливість надавати цілеспрямовану допомогу у зборі та обміні інформацією щодо міжнародних - злочинців, пов’язаних з воєнними злочинами. Завдяки своїй глобальній присутності Інтерпол може координувати розслідування, які виходять за межі однієї держави. Європол також відіграє важливу роль у сприянні ефективній співпраці між країнами Європейського Союзу, особливо у випадках, коли воєнні злочини мають європейське або регіональне значення [3].

Але все ж таки, попри значні досягнення, є багато викликів, які стоять перед міжнародними організаціями в процесі розслідування воєнних злочинів. Одним з головних є політичні бар'єри, оскільки деякі держави можуть не бажати співпрацювати через політичні, економічні або військові інтереси. Також виникає проблема захисту даних і забезпечення конфіденційності, особливо коли мова йде про чутливу інформацію, що стосується безпеки.

Таким чином, успішне розслідування воєнних злочинів потребує тісної співпраці між міжнародними та національними органами, таких як Інтерпол і Європол, та використання новітніх інформаційно-аналітичних технологій. Ці технології дозволяють значно підвищити ефективність збору доказів, аналізу даних і виявлення зв'язків між злочинами, що має вирішальне значення для забезпечення правосуддя і відновлення міжнародного правопорядку. Спільні зусилля правоохоронних органів на глобальному рівні допомагають боротьбі з воєнними злочинами та сприяють миру і безпеці на міжнародній арені.

Література

1. Моісеєва А. Що потрібно знати про європол та його співпрацю з Україною?. URL: https://golaw.ua/ua/insights/publication/shho-potribno-znati-pro-yevropol-ta-jogo-spivpraczyu-z-ukrayinoyu/. (дата звернення: 09.12.2024).
2. Величко В. В. Психолого-юридичне забезпечення професійної діяльності працівників Національного центрального бюро Інтерполу в Україні. Теоретичні і прикладні проблеми психології: зб. наук. праць Східноукраїнського національного університету імені Володимира Даля. м. Сєвєродонецьк, 2015. № 2 (37). С.50-56
3. Принципи роботи Інтерполу. «Інтерпол у цифрах та фактах». Випуск 5. 2021. URL: https://vbpartners.ua/uk/principi-robotiinterpolu/. (дата звернення: 09.12.2024).

Кулешник Тарас Яркович

викладач кафедри менеджменту мистецтва Львівської національної академії мистецтв

Кулешник Оксана Ігорівна

старший викладач кафедри менеджменту мистецтва Львівської національної академії мистецтв

ШТУЧНИЙ ІНТЕЛЕКТ І РЕВОЛЮЦІЯ У ЦИФРОВОМУ МАРКЕТИНГУ

Вступ. У світі, який стрімко стає цифровим, маркетинг зазнав радикальних змін завдяки впровадженню нових технологій. Одним із найпотужніших рушіїв цих змін є штучний інтелект (ШІ). Його здатність аналізувати дані, прогнозувати тенденції та створювати персоналізовані рішення робить ШІ невід'ємною частиною сучасного цифрового маркетингу.

Як працює ШІ у цифровому маркетингу? Штучний інтелект у маркетингу використовує алгоритми машинного навчання та обробки природної мови для обробки великих обсягів даних. Це дозволяє маркетологам отримувати глибоке розуміння поведінки споживачів, аналізувати ринки та вдосконалювати стратегії взаємодії з аудиторією. Основними функціями ШІ в маркетингу є:

1. **Аналіз даних**: ШІ може швидко аналізувати великі обсяги інформації, включаючи поведінку користувачів, купівельні звички та дані соціальних мереж.
2. **Автоматизація процесів**: Завдяки чат-ботам, автоматичному таргетингу реклами та email-маркетингу можна зменшити час, що витрачається на рутинні завдання.
3. **Персоналізація**: ШІ забезпечує гіперперсоналізований контент, що відповідає потребам і вподобанням конкретних споживачів.

Вплив ШІ на цифровий маркетинг

1. **Покращена аналітика.** Завдяки аналітичним можливостям ШІ маркетологи отримують доступ до прогнозів, що ґрунтуються на реальних даних. Це дозволяє створювати точні стратегії таргетингу та підвищувати конверсію.
2. **Персоналізований досвід.** ШІ дозволяє компаніям створювати персоналізований досвід для кожного споживача. Наприклад, стрімінгові сервіси, як-от Netflix,

використовують алгоритми ШІ, щоб рекомендувати контент, який відповідає смакам користувачів.

3. **Розумні чат-боти.** Чат-боти з ШІ працюють 24/7 і забезпечують швидку та ефективну взаємодію зі споживачами. Вони можуть відповідати на запити, вирішувати проблеми клієнтів і навіть пропонувати товари чи послуги.
4. **Оптимізація реклами.** ШІ дозволяє автоматично оптимізувати рекламні кампанії, обираючи правильні платформи, аудиторії та час для показу оголошень. Це знижує витрати та підвищує ефективність.
5. **Виробництво контенту.** Системи ШІ, такі як GPT (зокрема, ChatGPT), можуть створювати якісний контент для блогів, соціальних мереж і навіть рекламних оголошень. Це скорочує час і зусилля, необхідні для виробництва контенту.

Виклики використання ШІ в маркетингу

Попри всі переваги, впровадження ШІ в цифровий маркетинг має низку викликів:

1. **Приватність даних**: Використання даних споживачів викликає питання щодо конфіденційності та захисту інформації.
2. **Залежність від технологій**: Надмірна залежність від ШІ може призвести до втрати креативності у розробці маркетингових стратегій.
3. **Вартість**: Інтеграція ШІ потребує значних інвестицій у технології та навчання персоналу.

Майбутнє ШІ у цифровому маркетингу

Майбутнє цифрового маркетингу, безсумнівно, тісно пов’язане з розвитком ШІ. У найближчі роки можна очікувати такі новації:

1. **Інтерактивний контент**: ШІ дозволить створювати більш інтерактивний і захопливий контент, наприклад, віртуальну реальність (VR) і доповнену реальність (AR).
2. **Розумний аналіз настроїв**: ШІ зможе аналізувати емоційний стан споживачів через їхні дописи в соціальних мережах і відповідно адаптувати маркетингові стратегії.
3. **Штучні асистенти**: Голосові помічники, як-от Alexa чи Siri, стануть ще важливішими каналами взаємодії з клієнтами.

Висновок. Штучний інтелект змінює правила гри у цифровому маркетингу, забезпечуючи компаніям нові інструменти для взаємодії з аудиторією. Його впровадження відкриває величезні можливості для аналізу, персоналізації та автоматизації процесів. Проте, щоб максимально скористатися перевагами ШІ, необхідно враховувати етичні аспекти, пов’язані з використанням даних, і продовжувати розвивати людську креативність.

Література

1. Андреас Каплан "Artificial Intelligence in Marketing".
2. AK Gupta, Andrew Stephen "AI for Marketing and Product Innovation: Powerful New Tools for Predicting Trends, Connecting with Customers, and Closing Sales".
3. Омер Артун, Домінік Левін «Прогнозний маркетинг: прості способи, як кожен маркетолог може використовувати аналітику клієнтів і великі дані».

4. Chris DallaVilla «Машинне навчання для маркетингу»
5. Філіп Котлер, Хермаван Картаджая, Іван Сетіаван «Маркетинг 5.0: Технології для людства»

Легуцький Степан Васильович
курсант 2 курсу факультету №2 Львівського державного університету внутрішніх справ
Онипко Микита Віталійович
курсант 2 курсу факультету №2 Львівського державного університету внутрішніх справ
Гурин Марта Миколаївна
здобувач вищої освіти 1 курсу факультету №2 Львівського державного університету внутрішніх справ
Рудий Тарас Володимирович
доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ ДИНАМІЧНИХ МАСИВІВ У КЛАСАХ НА ПРИКЛАДІ РОЗВ'ЯЗАННЯ ЛІНІЙНОЇ СИСТЕМИ АЛГЕБРИЧНИХ РІВНЯНЬ

Головне досягнення C++ полягає у зміні парадигм програмування (*paradigm shift*) з процедурної та модульної на об'єктно-орієнтовану, яка визначає стандарт розроблення програмного забезпечення. Головним доробком об'єктно-орієнтованої парадигми стала ієрархічність програмних структур, яка відтворюється у агрегації об'єктів та успадкуванні класів [1].

На думку авторського колективу, нема потреби деталізувати підходи до розв'язання лінійної системи алгебричних рівнянь (ЛСАР) з огляду на ту обставину, що це відомий матеріал з курсу вищої математики. Очевидно, що не буде зроблено жодних відкриттів і у проєктуванні класів. Проте, у доступній для широкого загалу навчально-методичній літературі [2 - 11] дуже мало уваги відведено використанню динамічних масивів у проєктуванні класів.

Зрозуміло і доступно висвітлено використання масивів при проєктуванні класів у [12], але знову ж таки – фіксованих. Ця обставина спонукала нас провести пропоноване читацькій аудиторії це скромне дослідження, яке у першу чергу орієнтоване на студентську аудиторію. Для окресленої аудиторії, і не тільки, ця тема є актуальною з багатьох пунктів бачення.

Розв'язання поставленої нами задачі буде полягати у використанні технологій об'єктно-орієнтованого програмування (ООП). Зокрема, нами пропонується проєкт шаблонного класу з використанням динамічних масивів.

Отже, розпочнемо з того, що подамо проєкт програмного коду і поділимося деякими своїми міркуваннями.

Використання шаблонного класу є скоріше для "декорування", ніж диктується якоюсь нагальною потребою. Оголошуючи матриці та вектори можна було використати типи `double` або `float` (але не `int`).

```
#include <iostream>
```

```
using namespace std;
template <typename T>
class TDarray
{
private:
T** M; // Матриця коефіцієнтів
T* R; // Вектор вільних членів
T* X; // Вектор невідомих
int n; // Порядок системи
public:
// Конструктор ініціалізування
TDarray(int _n) : n(_n) {
  M = new T * [n];
  for (int i = 0; i < n; i++)
   M[i] = new T[n]();
  R = new T[n]();
  X = new T[n]();
}
void setMatrix(T** inputMatrix) {
  for (int i = 0; i < n; i++)
   for (int j = 0; j < n; j++)
    M[i][j] = inputMatrix[i][j];
}
void setVectorR(T* inputVector) {
  for (int i = 0; i < n; i++)
   R[i] = inputVector[i];
}
void print() {
  cout << "Матриця M:" << endl;
  for (int i = 0; i < n; i++) {
   for (int j = 0; j < n; j++)
    cout << M[i][j] << "\t";
   cout << endl;
  }
  cout << "Вектор R:" << endl;
  for (int i = 0; i < n; i++)
   cout << R[i] << endl;
}
void invertMatrix() {
  double temp;
  T** E = new T * [n];
  for (int i = 0; i < n; i++)
   E[i] = new T[n]();
  for (int i = 0; i < n; i++)
   E[i][i] = 1.0;
  for (int k = 0; k < n; k++) {
   temp = M[k][k];
   for (int j = 0; j < n; j++) {
    M[k][j] /= temp;
    E[k][j] /= temp;
   }
   for (int i = k + 1; i < n; i++) {
```

```
    temp = M[i][k];
    for (int j = 0; j < n; j++) {
     M[i][j] -= M[k][j] * temp;
     E[i][j] -= E[k][j] * temp;
    }
   }
  }
  for (int k = n - 1; k >= 0; k--) {
   for (int i = k - 1; i >= 0; i--) {
    temp = M[i][k];
    for (int j = 0; j < n; j++) {
     M[i][j] -= M[k][j] * temp;
     E[i][j] -= E[k][j] * temp;
    }
   }
  }
  for (int i = 0; i < n; i++)
   for (int j = 0; j < n; j++)
    M[i][j] = E[i][j];
  for (int i = 0; i < n; i++)
   delete[] E[i];
  delete[] E;
}
void solve() {
  for (int i = 0; i < n; i++) {
   X[i] = 0.0;
   for (int j = 0; j < n; j++)
    X[i] += M[i][j] * R[j];
  }
}
void showSolution() {
  cout << "Вектор розв'язків X:" << endl;
  for (int i = 0; i < n; i++) {
   cout << "X[" << i + 1 << "] = " << X[i] << endl;
  }
}
// Деструктор
~TDarray() {
  for (int i = 0; i < n; i++)
   delete[] M[i];
  delete[] M;
  delete[] R;
  delete[] X;
}
};
// Головна програма
int main()
{
setlocale(LC_CTYPE, "ukr");
int n;
cout << "Введіть порядок системи (n): ";
cin >> n;
```

```
double** matrix = new double* [n];
for (int i = 0; i < n; i++)
  matrix[i] = new double[n];
double* vectorR = new double[n];
cout << "Введіть матрицю коефіцієнтів:" << endl;
for (int i = 0; i < n; i++)
  for (int j = 0; j < n; j++) {
  cout << "матриця[" << i + 1 << "][" << j + 1 << "] = ";
  cin >> matrix[i][j];
  }
cout << "Введіть вектор вільних членів (R):" << endl;
for (int i = 0; i < n; i++) {
  cout << "R[" << i + 1 << "] = ";
  cin >> vectorR[i];
}
TDarray<double> fun(n);
fun.setMatrix(matrix);
fun.setVectorR(vectorR);
cout << "Початкове значення:" << endl;
fun.print();
fun.invertMatrix();
cout << "Обернена матриця:" << endl;
fun.print();
fun.solve();
fun.showSolution();
for (int i = 0; i < n; i++)
delete[] matrix[i];
delete[] matrix;
delete[] vectorR;
return 0;
}
```

Масиви формуються конструктором ініціалізування `TDarray(int _n)`. На відміну від фіксованого масиву, де його розмір повинен бути відомий під час компілювання, динамічне відведення пам'яті під масив у C++ дозволяє нам встановлювати довжину масиву під час виконання програмного коду. Тобто розмір об'єкту `fun` класу `TDarray` буде визначатися у процесі виконання програмного коду на інформаційному рівні, що усуне потребу змінювати програмний код у процесі виконання чергового числового експерименту.

Тим не менше, C++ не має вмонтованого механізму зміни розміру динамічного масиву після відведення пам'яті під нього. Це стосується і масивів у класах.

Звернемо вашу увагу на ще один аспект. Для формування двовимірного динамічного масиву використано вказівник другого порядку. Чому використовується вказівник другого порядку? Це вказівник на вказівник. Проєкт програмного коду буквально нам говорить, щоб добратися до довільного значення, яке зберігається у масиві, нам потрібно перейти за адресою, отримати там ще одну адресу і тоді ми отримаємо значення [13 - 14].

Інтерфейс класу формується розробленими нами методами, які зв'язуються з властивостями. Розроблені такі методи:

– `setMatrix` – передавання матриці коефіцієнтів у клас;
– `setVectorR` – передавання вектора вільних членів у клас;
– `print` – виведення матриці та вектора у консольний додаток;
– `invertMatrix` – обчислення оберненої матриці;
– `solve` – обчислення коренів ЛСАР;
– `showSolution` – виведення у консольний додаток вектора розв'язків.

Створений інтерфейс класу дає змогу захистити його властивості від випадкового модифікування або зовнішнього втручання.

За стандартами програмування за динамічною пам'яттю потрібно стежити і вчасно вивільняти, тому нами створено деструктор `~TDarray()`.

Скорше було сказано, що розмір динамічного масиву змінюється під час проведення поточного числового експерименту, але ніде цього явно вказано не було. Зміни розмірності масивів виробляються за наступним алгоритмом:

– настановою `int n;` оголошуємо порядок ЛСАР;
– настановами

```
cout << "Enter the order of the system (n): ";
```

та

```
cin >> n;
```

виводимо потрібне повідомлення у консольний додаток та вводимо значення порядку ЛСАР;

– оголошуємо двовимірний та одновимірний масиви порядку `n` настановами

```
double** matrix = new double* [n];
double* vectorR = new double[n];
```

і, відповідно, їхні розмірності будуть змінюватися за зміни прядку ЛСАР при проведенні поточного числового експерименту.

За стандартами програмування, за динамічною пам'яттю потрібно стежити і вчасно вивільняти, тому нами створено деструктор `~TDarray()`.

Як висновок зауважимо, що масиви є однією з найбільш корисних і широко використовуваних структур даних у програмуванні. Вони дають змогу зберігати великі обсяги даних та швидко обробляти їх, а за використання у класах змінювати розмірність динамічних масивів при проведенні числових експериментів.

Література

1. Бублик В.В. Об'єктно-орієнтоване програмування: Підручник / В.В. Бублик. – К.: ІТ книга, 2015. – 624 с.
2. Об'єктно-орієнтоване програмування: методичні вказівки до виконання лабораторних робіт для студентів за спеціальностями 123 "Комп'ютерна інженерія", 122 "Комп'ютерні науки", 125 "Кібербезпека"/ М-во освіти і науки України, Центральноукр. нац. техн. ун-т; [уклад. П. С. Усік] – Кропивницький: ЦНТУ, 2023. – 105 с

3. Зеленський О.С., Лисенко В.С. Основи програмування на С++: навчальний посібник. – Кривий Ріг: Державний університет економіки і технологій, 2023.-269 с.
4. http://repository.kpi.kharkov.ua/handle/KhPI-Press/52280.
5. Основи об’єктно-орієнтованого програмування : навч. посібник / Гришанович Т. О., Глинчук Л. Я.; ВНУ імені Лесі Українки. Електронні текстові данні (1 файл: 998 КБ). Луцьк : ВНУ імені Лесі Українки, 2022. – 120 с.
6. Міловідов Ю.О. «Об’єктно-орієнтоване програмування» Навчальний посібник друге видання – Видавничий центр НУБіП України, 2022. – 323 с.
7. Безменов М. І. Основи візуального програмування мовою C# : навч. посібник / М. І. Безменов, О. М. Безменова, Д. В. Калінін ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : ФОП Панов А. М., 2023. – 648 с.
8. Коноваленко І.В. Програмування мовою C# 7.0 : навчальний посібник / Коноваленко І.В., Марущак П.О., Савків В.Б. – Тернопіль : Тернопільський національний технічний унверситет імені Івана Пулюя 2017 – 300 с.
9. Жуковський С.С., Вакалюк Т.А. Об‘єктно-орінтоване програмування мовою С++. Навчальнометодичний посібник для студентів напряму 6.040302 Інформатика*. – Житомир: Вид-во ЖДУ, 2016. – 100 с.
10. Щербаков О. В. Основи об'єктно-орієнтованого програмування [Електронний ресурс] : навчальний посібник / О. В. Щербаков, Ю. Е. Парфьонов, В. М. Федорченко. – Харків : ХНЕУ ім. С. Кузнеця, 2019. – 237 с.
11. Основи програмування на С/С++. Методичні вказівки до самостійної роботи з дисципліни «Програмування» для студентів напрямів підготовки 123 – “Комп’ютерна інженерія”. /Укл.: Риндич Є.В., Солдатов А.Ю. – Чернігів: ЧНТУ, 2018. – 53 с.
12. Грицюк Ю.І., Гриник Р.О. Технології програмування: лабораторний практикум. – У 3-ох ч. – Ч. 2. Об'єктно-орієнтоване програмування. – Львів : Вид-во Львівського ДУ БЖД, 2014. – 196 с.
13. https://hi-news.pp.ua/kompyuteri/10725-scho-take-dinamchn-masivi-c.html
14. https://foxminded.ua/masyv-u-prohramuvanni/

Магеровська Тетяна Валеріївна

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

Мельник Ярослав Русланович

курсант Факультету № 2, гр. ІТ-11б Львівського державного університету внутрішніх справ

ЗАСТОСУВАННЯ VR І AR ТЕХНОЛОГІЙ В ОСВІТІ І ТРЕНІНГАХ: СТВОРЕННЯ ІММЕРСИВНИХ НАВЧАЛЬНИХ СЕРЕДОВИЩ ДЛЯ ПРАКТИЧНОГО НАВЧАННЯ У СПЕЦІАЛІЗОВАНИХ ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Анотація. Дана стаття присвячена дослідженню потенціалу застосування технологій віртуальної (VR) та доповненої реальності (AR) в освітньому процесі та тренінгах у спеціалізованих закладах вищої освіти системи Міністерства внутрішніх

справ України. Особлива увага приділяється опису інструментів і платформ для створення іммерсивних навчальних середовищ, які сприяють розвитку практичних навичок та підвищенню мотивації здобувачів вищої освіти до навчання, а також практичній підготовці курсантів і студентів до виконання професійних завдань у реальних умовах.

У дослідженні розглянуто можливості використання VR і AR для моделювання різноманітних сценаріїв, пов'язаних із забезпеченням громадської безпеки, криміналістикою, тактичною підготовкою та реагуванням на надзвичайні ситуації. Підкреслено переваги цих технологій у порівнянні з традиційними методами навчання, для забезпечення безпечного середовища при відпрацюванні складних ситуацій, розвитку практичних навичок і формування стійкості до стресових умов.

Стаття також аналізує виклики, пов'язані з впровадженням VR/AR у навчальний процес закладів МВС, включаючи технічні та фінансові обмеження, а також необхідність адаптації навчальних програм. Окреслено методичні підходи до створення інтерактивних навчальних середовищ, що враховують специфіку підготовки фахівців у спеціалізованих закладах.

У статті представлено рекомендації щодо інтеграції цих технологій у систему освіти МВС та окреслено перспективи їх подальшого розвитку.

Ключові слова: віртуальна реальність, доповнена реальність, освіта, навчання, інновації.

У сучасному світі технології віртуальної (VR) та доповненої (AR) реальності стають все більш значущими, зокрема у сфері освіти, де вони забезпечують унікальні можливості для навчання та тренувань. У спеціалізованих закладах вищої освіти системи МВС ці технології можуть набути особливої важливості, сприяючи ефективному практичному навчанню майбутніх фахівців. Технологія VR дозволить створити реалістичні симуляції для моделювання складних оперативних ситуацій у безпечному середовищі, тоді як AR інтегрує в реальний світ візуальні та звукові елементи, що допоможуть відпрацювати навички реагування у реальному часі. Використання VR та AR може допомогти здобувачам вищої освіти глибше зрозуміти навчальний матеріал, розвинути професійні компетентності та підготуватися до роботи в умовах підвищеної складності.

Переваги VR і AR технологій в освіті численні, особливо у контексті практичного навчання в спеціалізованих закладах вищої освіти системи МВС. По-перше, ці технології сприяють підвищенню зацікавленості та мотивації курсантів і студентів завдяки можливості занурення у захопливе інтерактивне навчальне середовище. Це є надзвичайно важливим для сучасного покоління, яке звикло до інтерактивних форматів спілкування та розваг. По-друге, VR і AR дозволяють глибше зрозуміти складні концепції та явища, забезпечуючи можливість для візуалізації і набуття практичного досвіду в умовах, максимально наближених до реальних. Такі методи навчання є особливо цінними для опанування навичок, необхідних у професійній діяльності співробітників правоохоронних органів, та сприяють ефективнішому засвоєнню і запам'ятовуванню навчального матеріалу.

Створення іммерсивних освітніх середовищ вимагає освоєння різних інструментів та платформ для розробки віртуальної та доповненої реальності (VR та AR). Серед таких інструментів можна виділити популярні ігрові движки, такі як Unity та Unreal

Engine, які надають великі можливості для створення інтерактивних сценаріїв та візуальних ефектів.

Окрім того, існують спеціалізовані онлайн-платформи, такі як CoSpaces Edu, що пропонують прості та доступні інструменти для створення освітніх програм у VR та AR. Ці платформи часто включають готові шаблони, бібліотеки моделей та інструменти для додавання інтерактивних елементів без необхідності глибоких знань у галузі програмування.

На практиці, створення освітніх додатків з використанням VR та AR може включати розробку віртуальних лабораторій для відпрацювання навичок у сфері правозастосування, інтерактивних занять з використанням доповненої реальності для моделювання реальних ситуацій, а також тренінгів та симуляцій, спрямованих на підготовку до виконання професійних обов'язків.

Перспективи розвитку та майбутнє застосування віртуальної та доповненої реальності (VR та AR) в освіті залежать від поточних тенденцій та інновацій у цій галузі. Аналіз існуючих трендів дозволяє припустити, як ці технології використовуватимуться у майбутньому.

На сьогоднішній день спостерігається постійне зростання інтересу до VR та AR в освіті. Щороку з'являються нові освітні програми, платформи та інструменти, що розширюють можливості використання цих технологій у навчальному процесі. Розвиток хмарних технологій і сучасних мережевих рішень значно розширює доступ до віртуальних і доповнених навчальних ресурсів, що відкриває нові можливості для підготовки висококваліфікованих фахівців у галузі правопорядку та безпеки.

Один з перспективних шляхів розвитку використання VR та AR в освіті полягає в індивідуалізації навчання. Ці технології дають змогу створювати адаптивні навчальні середовища, які враховують унікальні потреби, здібності та особливості кожного здобувача вищої освіти. Використання доповненої реальності для налаштування процесу навчання відповідно до індивідуальних уподобань та стилю навчання, є ключовим аспектом цього підходу, що сприяє підвищенню ефективності підготовки майбутніх фахівців.

Іншим важливим напрямом розвитку є інтеграція VR та AR у формальну освіту. Можливість використання цих технологій у навчальних закладах та в рамках стандартних освітніх програм може значно посилити їх вплив на навчання. Також очікується збільшення кількості досліджень, присвячених ефективності застосування VR та AR в освіті, що допоможе краще зрозуміти, яким чином ці технології впливають на навчальний процес та результати навчання.

Впровадження VR/AR у навчальний процес закладів МВС відкриває значні перспективи, однак цей процес також супроводжується низкою викликів.

Технічні виклики VR/AR включають необхідність у високопродуктивному обладнанні та інфраструктурі, що часто відсутні у навчальних закладах і потребують значних ресурсів для впровадження. Таке обладнання вимагає регулярного технічного обслуговування, оновлення програмного забезпечення та ремонту, що потребує кваліфікованих спеціалістів. Крім того, швидкий розвиток технологій призводить до застарівання обладнання та програм, змушуючи інвестувати в їх модернізацію.

Фінансові виклики пов'язані із високою вартістю впровадження, яка включає закупівлю обладнання, розробку програмного забезпечення, адаптацію приміщень і

навчання персоналу, що може перевищувати бюджетні можливості закладів освіти. Окрім того, необхідні додаткові витрати на підтримку працездатності технологій і оновлення ліцензій програмного забезпечення.

Використання VR/AR у навчальному процесі пов'язане і з кількома методичними викликами: необхідністю адаптації традиційних навчальних програм шляхом інтеграції сучасних технологій, що потребує співпрацю науково-педагогічного складу та технічних спеціалістів; підготовкою викладачів, які мають опанувати нові навички роботи з VR/AR через спеціальні тренінги; а також створенням якісного навчального контенту, розробка якого вимагає значних ресурсів часу і фінансів.

Також використання VR/AR у навчальному процесі супроводжується низкою організаційних викликів, серед яких скептичне сприйняття нових технологій через страх змін або недостатню обізнаність про їх переваги, значний час, необхідний для їх інтеграції та адаптації до навчального процесу, а також проблеми доступності для окремих осіб із медичними протипоказаннями, такими як кінетоз чи порушення зору.

Для подолання цмх викликів важливо залучати фінансову підтримку через державні кошти, гранти чи партнерські програми для придбання обладнання та створення контенту. Початково можна запускати пілотні проєкти, зокрема експериментальні курси, щоб оцінити ефективність технологій. Також необхідна міждисциплінарна співпраця спеціалістів із технологій, освіти та психології для розробки збалансованих навчальних програм. Важливим є навчання персоналу через тренінги та семінари, а також адаптація навчальних планів для того, щоб VR/AR доповнювали, а не замінювали традиційні методи навчання.

Отже, застосування технологій віртуальної та доповненої реальності в освіті та тренінгах відкриває значні можливості для покращення практичного навчання у спеціалізованих закладах вищої освіти системи МВС. Попри наявні успіхи у впровадженні VR і AR у навчальний процес, залишаються широкі перспективи для подальших досліджень та створення нових методів і засобів. Розвиток цих технологій може сприяти більш інтенсивному використанню у підготовці майбутніх фахівців, що здатне кардинально змінити підхід до навчання і професійного тренування у сфері правоохоронної діяльності.

Література

1. Immersive Learning with VR and AR Technologies // [Електронний ресурс] URL: https://youtu.be/iqjcNRJf-Nc?si=ioAyvYZYFu1TrfV0
2. How VR And AR Are Revolutionizing eLearning For Learners Of All Ages // [Електронний ресурс] URL: https://elearningindustry.com/how-vr-and-ar-are-revolutionizing-elearning-for-learners-of-all-ages
3. Abdullah M. Al-Ansi, Mohammed Jaboob, Askar Garad, Ahmed Al-Ansi. Analyzing augmented reality (AR) and virtual reality (VR) recent development in education / Social Sciences & Humanities Open, Volume 8, Issue 1, 2023

МАНЖАЙ Олександр Володимирович,
завідувач кафедри протидії кіберзлочинності ННІ № 4 Харківського національного університету внутрішніх справ, кандидат юридичних наук, професор.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДОЛОГІЇ SOCTA 2021 ТА SOCTA 2025

European Union Serious and Organised Crime Threat Assessment (EU SOCTA) – це документ, в якому визначено поточний стан та тенденції розвитку організованої злочинності в ЄС. Він складається з використанням відповідної методології.

На теперішній час застосовується методологія SOCTA 2021 року [1], водночас з березня 2025 року почне діяти SOCTA 2025 [2], яка стане вже четвертою ітерацією цього важливого документу. Як і у SOCTA 2021 концептуальна модель SOCTA 2025 побудована на основі чотирьох окремих аспектів:

- фокус;
- інструменти (індикатори/показники);
- аналіз та визначення пріоритетів;
- результат.

Фокус

SOCTA 2025 охоплює такі основні напрямки:

- злочинні суб’єкти;
- сфери серйозної та організованої злочинності;
- інфраструктуру злочинності;
- географічні аспекти;
- рушійні сили для серйозної та організованої злочинності;
- вплив серйозних злочинів та організованої злочинності.

На відміну від SOCTA 2021 у SOCTA 2025 відійшли від застосування терміну організовані злочинні угруповання (organised crime group), ввівши більш широке поняття **злочинні мережі (criminal networks).**

Поняття «злочинна мережа» є ширшим терміном, ніж організоване злочинне угруповання, та відображає природу сучасного злочинного середовища, яке є більш складним і включає в себе також злочинні об’єднання, які вертикально та ієрархічно менш інтегровані. Злочинні мережі включають групи та окремих осіб, які взаємодіють з організованими злочинними угрупованнями.

Злочинні суб’єкти охоплюють:

- злочинні мережі;
- організовані злочинні угруповання
- ролі у кримінальній діяльності.

Сфери серйозної та організованої злочинності як і у попередній методології SOCTA 2021 характеризуються попитом та пропозицією на нелегальні товари та/або послуги. Водночас у SOCTA 2025 було прибрано згадування про те, що SOCTA охоплює всі сфери злочинної діяльності в рамках мандату Європолу, та пов’язані

кримінальні злочини, як зазначено в Регламенті ЄС щодо Європолу. Таким чином, сфери серйозної та організованої злочинності стали трактуватися більш широко.

Інфраструктура злочинності – це засоби, що сприяють вчиненню злочинів; елементи, що використовуються як частина кримінальної діяльності або способу дій, які роблять злочин можливим або полегшують його вчинення, а також заходи, що вживаються для уникнення переслідування. Так само як і у SOCTA 2021 стосовно інфраструктури злочинності зазначається, що це можуть бути дії, які самі по собі є кримінальними і дії, які самі по собі є законними, але використовуються для вчинення злочинів.

Географічні аспекти характеризуються тим, що під час аналізу головна увага приділяється ключовим місцям у межах та за межами ЄС, які пов'язані з серйозною та організованою злочинністю. У межах цього напрямку у SOCTA 2025 було представлено окремий перелік індикаторів, які потребують вимірювання.

Рушійні сили для серйозної та організованої злочинності характеризуються змінами в макросередовищі, які можуть призвести до появи вразливих місць та можливостей для організованої злочинності. У SOCTA 2025 зазначається, що розуміння змін у макросередовищі і того, як вони впливають на організовану злочинність, є важливим не тільки для оцінки поточних загроз, але й для майбутньої загрози.

Вивчення **впливу серйозних злочинів та організованої злочинності** допомагає оцінити відповідні ризики, виходячи з характеру впливу, його обсягу, частоти та серйозності.

Інструменти (індикатори) SOCTA

Згідно з положеннями SOCTA 2025 індикатори використовуються як інструменти для збору, аналізу та визначення пріоритетності інформації. Для того, щоб оцінити загрози серйозної та організованої злочинності використовуються набори індикаторі, які визначаються раніше зазначеними напрямами SOCTA. Як і у SOCTA 2021 індикатори поділяються на два види: описові (**D**/escripive/) та загроз (**T**/hreat/).

Описові індикатори (**D**) використовуються для аналізу та опису загрози. У SOCTA 2021 зазначалося, що описові індикатори використовуються виключно для аналізу поточних загроз. Індикатори загрози (**T**) використовуються для оцінки поточної загрози на основі шкали загрози (висока, середня, низька, нульова, не застосовується / high, medium, low, nil, not applicable).

Порівняно з SOCTA 2021 у SOCTA 2025 було змінено вагу окремих індикаторів.

Методи накопичення даних

У SOCTA 2025 виділено три рівні накопичення даних:

- Дані, які перебувають в Європолі.
- Зовнішні дані від країн-членів ЄС, третіх країн та інших відповідних партнерів (згідно з положеннями SOCTA 2025 вони мають узгоджуватися із накопиченням даних і результатами картографування злочинних мереж в ЄС).
- Інформація з відкритих джерел, що використовується як додаткове джерело даних.

Аналіз та визначення пріоритетів

Метою аналізу є розробка найбільш точних та обґрунтованих висновків на основі отриманої інформації, з метою виявлення ключових загроз та надання обґрунтованих рекомендацій щодо визначення пріоритетів. Ключові загрози – це загрози, які мають найвищий рейтинг на основі узгодженого механізму визначення пріоритетів.

Визначення пріоритетів відбувається у три етапи:

1) оцінюється поточна загроза (на основі індикаторів загроз **T**, злочинних суб'єктів, інфраструктури злочинності, географічного виміру);

2) оцінюється вплив серйозної та організованої злочинності;

3) оцінюється майбутня загроза (майбутній розвиток на основі очікуваних змін у навколишньому середовищі).

Оцінки за цими трьома критеріями в сукупності дають загальний бал для кожної сфери організованої злочинної діяльності. Сфери з найвищими сумарними балами визначаються як ключові загрози. Індикатори загроз зважуються відповідно до заздалегідь узгоджених вагових коефіцієнтів.

Важливо розрізняти шкалу і вагу індикаторів загроз. Вага індикатора загрози – це присвоєне значення на основі узгодженої порівняльної значущості індикатора. Ваги індикаторів вказані у додатку А.

Характеристики найбільш загрозливих злочинних суб'єктів, інфраструктури злочинності та географічного виміру мають бути більш глибоко проаналізовані на основі описових індикаторів **D** та індикаторів загроз **T**.

Результати

На підставі SOCTA визначаються пріоритети протидії серйозній та організованій злочинності в ЄС на найближчі чотири роки. Рекомендації щодо визначення пріоритетів мають бути обґрунтованими з описом відповідних причин. Зазначаються також прогалини у розвідувальних відомостях. Під час опису пріоритетів особлива увага приділяється злочинним суб'єктам, інфраструктурі злочинності та географічному виміру. Фокусування не тільки на злочинних суб'єктах та географічному вимірі, але й на інфраструктурі злочинності є новелою SOCTA 2025 у порівнянні з SOCTA 2021.

Методологія SOCTA 2025 ґрунтується на попередніх методологіях, проте має характерні відмінні риси, які мають бути враховані під час складання національних моделей SOCTA.

Висновки. Під час складання національної моделі SOCTA рекомендується врахувати:

1. Зміну термінологічного апарату, зокрема в частині застосування більш широкого терміну «злочинні мережі» замість «організованих злочинних угруповань».
2. Необхідність оцінювання поточних загроз на основі усіх індикаторів загроз Т. Крім того, потрібно врахувати, що описові індикатори можуть застосовуватись не тільки для аналізу поточних загроз.
3. Зміну окремих індикаторів та їх ваги для оцінки загроз. Серед іншого в SOCTA Україна були додані нові, але залишені старі індикатори, які були виключені з SOCTA 2025. Так само ваги окремих індикаторів в SOCTA Україна не відповідають оновленій вазі індикаторів у SOCTA 2025.

4. В оригінальній методології SOCTA 2025 відсутні індикатори, які позначаються як D/T, які виділені в SOCTA Україна.
5. Можливість зміни поправочних коефіцієнтів для відповідних індикаторів в SOCTA Україна шляхом заміни значень показників оціночної шкали на стаціонарні величини замість інтервальних по аналогією з методологією SLEIPNIR. Це дозволить уникнути неоднозначних оцінок з боку виконавців та дозволить застосувати більш спрощений універсальний підхід до розрахунку показників.
6. Можливість кольорових позначень індикаторів відповідної ваги для візуалізації отриманих результатів, а також програмування відповідних автоматизованих рішень.
7. Можливість розрахунку інтегрального показника оцінки під час формування SOCTA Україна.

Література

1. EU Serious and Organised Crime Threat Assessment (SOCTA) 2021. European Union Agency for Law Enforcement Cooperation, 2021. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (дата звернення: 29.08.2024).
2. European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2025 – Revised methodology, 14642/23 REV 2, 21 November 2023. URL: https://data.consilium.europa.eu/doc/document/ST-14642-2023-REV-2/en/pdf (дата звернення: 10.11.2024).

Манівська Соломія-Іванна Миколаївна

Старший інспектор відділу аналітичної роботи управління кримінального аналізу ГУНП у Львівській області

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ КРИМІНАЛЬНОГО АНАЛІЗУ ПІД ЧАС ОПЕРАТИВНОГО ПРОВАДЖЕННЯ ТА ДОСУДОВОГО РОЗСЛІДУВАННЯ

Значна увага до кримінального аналізу є ключовою у сучасній правоохоронній діяльності, так як, він визначає стратегію та тактику боротьби з злочинністю. Слід зауважити, що кримінальний аналіз – це специфічний вид інформаційно-аналітичної діяльності, спрямований на встановлення та передбачення взаємозв'язків між даними про злочинну діяльність та іншими даними, потенційно з ними пов'язаними, їх оцінювання, інтерпретація та прогнозування розвитку досліджуваних подій з метою їх використання під час досудового розслідування та здійснення оперативно-розшукової діяльності, а також для розроблення тактичних і стратегічних заходів із протидії злочинності [1, с. 16-17].

У процесі кримінального аналізу здійснюється систематичне вивчення даних про злочин, зокрема інформація про злочинців, їхні методи та знаряддя злочину, а також контекст вчинення злочину, включаючи час і місце. Цей аналіз має не лише описовий, а й аналітичний характер, спрямований на виявлення закономірностей і трендів у злочинності [2].

Результатом кримінального аналізу є розробка гіпотез та висновків щодо минулих, теперішніх і майбутніх протиправних дій, структури та сфери діяльності злочинних груп. Ця інформація надає підстави для проведення оперативно-розшукових заходів та слідчих дій. Сучасні технології, зокрема програмні засоби аналізу даних, роблять процес кримінального аналізу більш ефективним і швидким. Зокрема, інструменти, такі як IBM i2 та Power BI, надають можливості для візуалізації даних, що сприяє зростанню продуктивності та зменшенню часу, необхідного для обробки інформації [3].

Широкий спектр питань, пов'язаних із правовими аспектами використання методів кримінального аналізу під час оперативного провадження та досудового розслідування, досліджували знані вчені, зокрема: О. Ю. Бусол, О. М. Джужа, О. М. Заєць, О. В. Калиновський, С. М. Князєв, О. Є. Користін, О. В. Корнейко, М. В. Кузнєцов, В. А. Некрасов, Д. Й. Никифорчук, О. Ю. Орлов, О. В. Тихонова, О. М. Цільмак, С. С. Чернявський, В. І. Школьніков та ін.

Загальна мета кримінального аналізу полягає у напрацюванні нових напрямів в оперативно-розшуковій діяльності та досудовому розслідуванні кримінальних проваджень; для отримання детального аналітичного продукту щодо об'єктів кримінального аналізу; якісного планування окремих оперативно-розшукових заходів та слідчих (гласних та негласних) дій; аналітичного супроводження оперативно-розшукової діяльності та досудового розслідування; аналізу стану та ефективності досудового розслідування, оперативно-розшукової та превентивної діяльності у протидії злочинності; оброблення великого обсягу інформації, що унеможливлює відстеження та пов'язування фактів без застосування спеціальних аналітичних методів; аналізу складної і розгалуженої структури зв'язків об'єктів оперативно-розшукової справи або кримінального провадження; виявлення ризиків, тенденцій майбутнього розвитку злочинності та, у подальшому, її запобігання; вирішення більш масштабних довгострокових проблем і цілей, для виявлення крупних фігур злочинного світу або синдикатів, прогнозування зростання видів злочинної діяльності і встановлення пріоритетів діяльності правоохоронних органів; аналізу інформації, спрямованої на виявлення тенденцій, закономірностей, прогнозування розвитку за великий період часу.

Сучасні інформаційні технології вражають своїми можливостями та дозволяють, як поліпшити життя звичайних пересічних громадян, так і сприяти ефективній роботі працівників Національної поліції. Адже за допомогою сучасних технологій обробки інформації та новітніх технік можливо виконати поставлені завдання з легкістю та швидкістю.

Слід зауважити, що в умовах сьогодення підрозділи кримінального аналізу щодня на професійному рівні користуються системами відеоспостереження та аналізують сотні терабайт відеоматеріалів, що є невід'ємною складовою роботи аналітика.

Кримінальні аналітики розкрили весь накопичений потенціал підрозділів кримінального аналізу у секторі відеоаналітики саме з повномасштабним вторгненням – а це аналіз великих масивів відео, геопросторовий аналіз, аналіз маршрутів руху, у тому числі військової техніки ворога, розпізнання воєнних злочинців, мародерів, незаконного обігу зброї, викрадення людей, диверсантів, покращення відеоматеріалів, пошук та встановлення дітей, яких незаконно депортували з України на територію країни агресора, спростування дезінформації, що набувала суспільного резонансу та сіяла деморалізацію і паніку (ІПСО).

Кримінальний аналіз дозволяє швидко виявляти кримінальні правопорушення та події, які можуть набрати суспільний резонанс, розглядати їх особливості та розробляти

способи боротьби з ними. Ефективне розслідування злочинів також стає можливим завдяки аналізу наявної інформації про злочин, їх обставини та осіб, причетних до них. Кисельов А.О. який акцентує на тому, що знання з аналітики дозволяють підрозділам Національної поліції ефективніше протидіяти кримінальним правопорушенням. Досконало володіти інтернет-ресурсами та базами даних неможливо без спеціальних знань, умінь та навичок. Все це вимагає від поліцейського постійної самоосвіти, підвищення кваліфікації та відвідування відповідних занять, тренінгів тощо, а також врахування поліцейськими тактичних особливостей під час оперативно-розшукової протидії кримінальним правопорушенням [4, с. 67, с. 149-152; 5, с. 12-14], в тому числі в умовах воєнного стану.

Основними завданнями, які можна та доцільно вирішувати за допомогою новітніх технологій, зокрема, відео технологій, є: розпізнавання, адже найчастіше розпізнаються обличчя людей і номери автомобілів або вагонів; завдання, пов'язані з аналізом поведінки людини, автомобіля або іншого рухомого об'єкту; реалізація охоронних функцій на різноманітних об’єктах. В умовах сьогодення розвиток систем відеоспостереження в Україні не просто інструмент для оперативного реагування на правопорушення, а стратегічне питання національної безпеки України.

Аналіз сучасних тенденцій у розслідуванні кримінальних правопорушень свідчить, що успіх їх розкриття більш як на 90 % залежить від наявності відеоматеріалів, де зафіксована кримінальна подія. При цьому в 97 випадках зі 100 завжди є відеоконтент із повною або частковою фіксацією злочину. Джерела такого контенту оточують нас всюди: це і системи відеоспостереження і відеоконтролю, розташовані на об’єктах інфраструктури населених пунктів, і відеореєстратори, розміщені в транспортних засобах, і навіть любительські відео, зроблені випадковими свідками події.

За результатами проведених аналітичних заходів вся інформація узагальнюється у відповідному форматі для подальшої її реалізації замовниками або особами, які отримають аналітичний продукт. Уся отримана та опрацьована в результаті аналітичних досліджень інформація повинна бути викладена у зрозумілій для замовника формі. Цією формою може бути відеоряд, схема, аналітичний звіт або будь-який інший аналітичний документ[6].

Отже, використання можливостей кримінального аналізу під час оперативного провадження і досудового розслідування має вирішальне значення для ефективності діяльності правоохоронних органів. Враховуючи нові форми та характер злочинності, аналіз дозволяє оперативно виявляти нові схеми злочинів, ефективно розслідувати злочини та прогнозувати можливі злочинні дії. Кримінальний аналіз залишається важливим інструментом для забезпечення безпеки та боротьби зі злочинністю в надзвичайних умовах. Використання різноманітних методів аналізу, таких як аналіз кримінальної статистики, картографічний аналіз та аналіз зв'язків, дозволяє оперативно реагувати на злочинність та запобігати можливим загрозам у період воєнних дій.

Література

1. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.
2. ЗУ «Про оперативно-розшукову діяльність» поточна редакція — від 09.08.2024, (Відомості Верховної Ради України (ВВР), 2023, № 47-50, ст.120). URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 12.12.2024).

3. Кримінальний процесуальний кодекс України чинний, поточна редакція — від 21.11.2024, (Відомості Верховної Ради України (ВВР), 2024, № 30, ст. 217). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 12.12.2024).
4. Кузнєцов М. В., Василинчук В. І. Правові аспекти використання методів кримінального аналізу оперативними підрозділами Національної поліції Укра їни під час тимчасового доступу до інформації про зв"язок. Використання досягнень сучасної науки й техніки в розкритті злочинів: матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лют. 2021 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ: Нац. акад. внутр. справ, 2021. С. 21–26. URL: http://elar.naiau.kiev.ua/jspui/bitstream/123456789/18320/1/%d0%92%d0%b8%d0%ba%d0%be%d1%80%d0%b8%d1%81%d1%82%d0%b0%d0%bd%d0%bd%d1%8f%20%d0%b4%d0%be%d1%81%d1%8f%d0%b3%d0%bd%d0%b5%d0%bd%d1%8c%20%2025.02.2021.pdf.
5. Саковський А.А. Оперативно-розшукове документування як пошуково-пізнавальний процес і складник оперативно-розшукової діяльності. Підприємництво господарство і право. 2020. No 7. С. 371–377.
6. Методичні рекомендації щодо організації та проведення кримінального аналізу підрозділами Національної поліції 132 України, затверджені Головою Національної поліції України Клименком Ігорем 11 травня 2021 року (вих. ДДЗ від 26 травня 2021 року № 6516/01/33-2021).

Маржан Єлизавета Володимирівна

курсант 3-го курсу факультету № 3 Донецького державного університету внутрішніх справ, рядова поліції

Пекарський Сергій Петрович

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПРАВОВИЙ АСПЕКТ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗШУКУ ОСІБ, ЗНИКЛИХ БЕЗВІСТИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Закон України «Про правовий статус осіб, зниклих безвісти за особливих обставин» від 12 липня 2018 року № 2505-VIII під особою, яка зникла безвісти за особливих обставин визначає особу, зниклу безвісти у зв’язку із збройним конфліктом, воєнними діями, тимчасовою окупацією частини території України, надзвичайними ситуаціями природного чи техногенного характеру [1, ст. 1]. Дефініцією є те, що особа, яка зникла безвісти під час дії правового режиму воєнного стану також відноситься до категорії осіб, зниклих безвісти за особливих обставин. Зазначаємо те, що ннформаційно-аналітичне забезпечення розшуку осіб, зниклих безвісти в умовах дії правового режиму воєнного стану має праву регламентацію. Так, на підставах визначених Законом України «Про правовий статус осіб, зниклих безвісти за особливих обставин» діє Єдиний реєстр осіб, зниклих безвісти за особливих обставин. Реєстр створений для накопичення та централізації відомостей та даних про таких осіб, а також для обліку інформації, необхідної для їх ефективного розшуку [1, ст. 12].

Держателем Реєстру є МВС України. Відповідно до вимог Положення про Єдиний реєстр осіб, зниклих безвісти за особливих обставин, яке затверджено наказом МВС України від 29 серпня 2022 року № 535 Реєстр є функціональною підсистемою єдиної інформаційної системи Міністерства внутрішніх справ України [2]. Держатель має право доступу до відомостей, внесених до Реєстру, у повному обсязі [1, ст. 12]. Держатель у межах визначених повноважень, має право отримувати інформацію (включаючи персональні дані) від інших органів державної влади, у тому числі шляхом інформаційної взаємодії між Реєстром та іншими державними інформаційними ресурсами в електронній формі інформаційно-комунікаційними засобами з використанням засобів технічного та криптографічного захисту інформації відповідно до вимог законодавства з питань захисту інформації [1, ст. 12]. Структура Реєстру складається із взаємопов'язаних розділів, які містять відомості: про осіб, зниклих безвісти за особливих обставин та про невпізнані тіла (останки) померлих (загиблих) осіб та пов'язані з ними речі, документи [2].

Отже, до Реєстру вносяться відомості про особу, зниклу безвісти за особливих обставин: прізвище, власне ім'я, по батькові (за наявності) (українською мовою та латинськими літерами відповідно до правил транслітерації), фото; інформація про дату та місце народження; інформація про сімейний стан; інформація про задекларване (зареєстроване) місце проживання (перебування) особи; інформація про фактичне місце проживання; у разі якщо така особа уповноважена на виконання функцій держави, інформація про роботодавця, у якого вона виконувала роботу (проходила службу); реквізити документів, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи (назва, номер, серія (за наявності) документа, дата видачі, уповноважений суб'єкт, що його видав); унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності); дата, місце (у тому числі з прив'язкою до населеного пункту, координати зникнення), обставини та час зникнення особи; прикмети особи; інформація про наявність кримінального провадження, розпочатого за фактом зникнення такої особи, або в якому потерпілий є особою, зниклою безвісти за особливих обставин; найменування органу, який здійснює досудове розслідування в кримінальному провадженні за фактом зникнення безвісти особи, або в іншому кримінальному провадженні, в якому потерпілий є особою, зниклою безвісти за особливих обставин; найменування територіального органу (підрозділу) Національної поліції України, який здійснює розшук особи, зниклої безвісти (у якого в провадженні перебуває оперативно-розшукова або розшукова справа), найменування іншого органу, який здійснює оперативно-розшукову діяльність; інформація про наявність рішення суду про визнання особи безвісно відсутньою або оголошення її померлою (зазначається найменування суду, який прийняв відповідне рішення, дата ухвалення рішення суду, номер справи, номер провадження, а також інформація про те, чи набрало вказане судове рішення законної сили); дата та місце встановлення місцезнаходження особи, зниклої безвісти; інша інформація, що може сприяти розшуку особи, зниклої безвісти за особливих обставин [2].

Окрім того, наказом МВС від 28.06.2023 № 534 затверджена Інструкція з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», яка визначає порядок формування і ведення бази даних «Розшук» (БД «Розшук») інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» [3]. При цьому БД «Розшук» – це автоматизований банк відомостей, у якому обробляється інформація щодо різних категорій осіб, які розшукуються, зокрема і щодо осіб, зниклих безвісти. Суб'єктами наповнення БД «Розшук», зазначеною Інструкцією, визначені працівники оперативних підрозділів, які здійснюють оперативно-розшукову діяльність [3].

Наказом МВС від 05.07.2023 № 553 затверджено Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» [4]. Дане положення визначає мету, структуру та функції інформаційної підсистеми «Електронна розшукова справа» (ІП «ЕРС») інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», а також порядок її використання органами (підрозділами) поліції в розшуковій роботі [4]. Відповідно ІП «ЕРС» становить собою сукупність програмних засобів, які призначені для формування та ведення інформаційних ресурсів ІП «ЕРС» в електронному вигляді. Констатуємо, що однією метою ведення ІП «ЕРС» є інформаційно-пошукове та інформаційно-аналітичне забезпечення розшукової роботи органів (підрозділів) поліції, зокрема і щодо розшуку осіб, зниклих безвісти [4]. Зазначеним наказом встановлено те, що ОРС «Розшук» складається з двох частин: перша – в електронному вигляді в ІП «ЕРС», у якій накопичуються та систематизуються документи, що не містять інформації з обмеженим доступом; друга – у паперовому вигляді відповідно до встановленого законодавством України порядку ведення діловодства та поводження з документами, які містять інформацію з обмеженим доступом [4].

Окрім вищенаведеного, міжнародне співробітництво з використанням інформаційної системи Інтерполу при розшуці особи, зниклої безвісти регламентовано Інструкцією про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол, яка затверджена наказом МВС, ОГП, НАБУ, СБУ, ДБР, МФУ, МЮУ від 17.08.2020 № 613/380/93/228/414/510/2801/5 [5]. Використання інформаційної системи Інтерполу правоохоронними органами України здійснюється відповідно до встановленого порядку у формі надсилання запиту (звернення) до уповноваженого підрозділу або у формі прямого доступу [5].

У запитах (зверненнях), що надсилаються уповноваженому підрозділу, зазначаються: номер кримінального провадження та оперативно-розшукової (розшукової) справи (за наявності); детальний опис обставин злочину або підстав проведення оперативно-розшукових заходів чи здійснення ідентифікації особи; обґрунтування потреби звернення до компетентних органів іноземних держав; заходи, що мають бути здійснені компетентними органами іноземних держав та перелік відомостей, які необхідно отримати з-за кордону; перелік держав-членів Інтерполу, на території яких необхідно провести відповідні заходи [5]. І тому, уповноважений підрозділ з України запитує публікацію Генеральним секретаріатом Інтерполу Жовтого оповіщення з метою встановлення місцезнаходження особи зниклої безвісти або для ідентифікації особи, яка не може повідомити відомості про себе.

Публікація Жовтого оповіщення запитується за сукупності таких умов: розшук особи зниклої безвісти або заходи з ідентифікації особи, що здійснює правоохоронний орган України в установленому законодавством порядку; місцезнаходження особи зниклої безвісти або дані особи, яка підлягає ідентифікації, що правоохоронним органам України невідомі [5].

Отже, з метою ефективного розшуку особи, зниклої безвісти в умовах правового режиму воєнного стану підрозділи кримінальної поліції використовують інструментарій інформаційно-аналітичного забезпечення. Дана діяльність регламентується низкою нормативно-правових актів, які визначають особливості накопичення інформації, ведення баз даних та інформаційну міжнародну взаємодію.

Література

1. Про правовий статус осіб, зниклих безвісти за особливих обставин: Закон України від 12 липня 2018 року № 2505-VIII. Дата оновлення: 18.10.2024. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text.
2. Положення про Єдиний реєстр осіб, зниклих безвісти за особливих обставин: затв. наказом МВС України від 29 серпня 2022 року № 535.
3. Інструкція з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»: затв. наказом МВС від 28.06.2023 № 534.
4. Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України: затв. наказом МВС від 05.07.2023 № 553.
5. Інструкція про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол: затв. наказом МВС, ОГП, НАБУ, СБУ, ДБР, МФУ, МФУ від 17.08.2020 № 613/380/93/228/-414/510/2801/5.

Мовчан Анатолій Васильович

професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

ХАРАКТЕРИСТИКА СУЧАСНОЇ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ У КІБЕРПРОСТОРІ

За результатами Оцінки загроз організованої злочинності в Інтернеті (IOCTA) Європолу, пріоритетами боротьби з кіберзлочинністю, які визначені Циклом політики ЄС – EMPACT, наразі є: кіберзалежна злочинність; сексуальна експлуатація дітей в Інтернеті; шахрайство з оплатою. Крім того, IOCTA-2024 розглядає додаткову сферу злочинності, ринки онлайн-криміналу, як на поверхні, так і в Darknet, а також зближення кіберзлочинності та тероризму. Водночас фінансові злочини, головним чином шахрайство з інвестиціями та відмивання грошей, залишаються сферою, в якій найчастіше стикаються з криптовалютами [1].

Європейський центр боротьби з кіберзлочинністю також створює спільну робочу групу по боротьбі з кіберзлочинністю (J-CAT), завданням якої є керівництво скоординованими діями учасників проти ключових загроз кіберзлочинності. Ці інституційні механізми призвели до певних успіхів на операційному рівні, зокрема: координація спільної операції щодо протидії ботнету Ramnit, який заразив мільйони комп'ютерів по всьому світу; координація разом з Євроюстом операції проти широкомасштабних атак зловмисного програмного забезпечення, які виникли в Україні та які розслідувалися низкою відомств; операція, спрямована проти великого форуму кіберзлочинців, які займаються торгівлею хакерським досвідом, зловмисним програмним забезпеченням і ботнетами, експлойтами Zero Day, доступом до скомпрометованих серверів і пошуком партнерів для спам-кампаній й атак зловмисного програмного забезпечення.

Зокрема, у січні 2024 року оперативні працівники Департаменту кіберполіції та слідчі Головного слідчого управління Нацполіції під процесуальним керівництвом Офісу

Генерального прокурора спільно з колегами з Європолу затримали хакера, якого вважають автором складної схеми криптовикрадення, що використовує скомпрометовані комп'ютери для майнінгу криптовалюти. 29-річний хакер із Миколаєва проводив зараження серверів хмарного постачальника для криптоджекінгу з 2021 року, здійснивши злом 1500 облікових записів, щоб отримати паролі, перш ніж заразити серверне обладнання компанії з криптоджекінгом. Для цього підозрюваний створив понад мільйон віртуальних комп'ютерів для запуску шкідливого програмного забезпечення. У результаті цієї схеми отримано понад 1,8 млн євро видобутого Ethereum, Monero та TON. Українські слідчі також вивчають потенційну причетність підозрюваного до проросійських хакерських груп [2].

У нинішніх умовах структура кіберзлочинців залишається різноманітною, включаючи як поодиноких хакерів, так і злочинні мережі, які пропонують широкий спектр досвіду та можливостей. Деякі кіберзлочинці спрямовують свої атаки на ЄС в межах ЄС, тоді як інші прагнуть працювати з-за кордону для приховування своїх незаконних операцій і коштів у третіх країнах. Постійне видалення форумів і маркетплейсів кіберзлочинців скоротило життєвий цикл злочинних сайтів, оскільки адміністратори сайтів намагаються не привертати уваги правоохоронних органів. Ця невизначеність у поєднанні зі зростанням випадків шахрайства з виходом з ринку призвела до подальшої фрагментації кримінальних ринків [3, с. 26-30].

Натомість, як свідчать результати опитування SOCTA, у нинішніх умовах окремі складові торгівлі людьми перемістились в онлайн середовище, від вербування жертв до реклами незаконних послуг. Злочинні угруповання використовують намагання нелегальних мігрантів потрапити в країни Європи, вимагають високу оплату за контрабанду в ЄС або всередині ЄС, а також за допомогу в отриманні легального статусу для проживання [3, с. 18].

Водночас важливою складовою переважної більшості злочинних операцій є відмивання грошей, зокрема 68% ОЗУ використовують основні методи відмивання грошей, наприклад, інвестування в нерухомість або цінні товари. У багатьох випадках злочинці використовують доступ до паралельної банківської системи, яка дозволяє їм переказувати гроші партнерам по всьому світу. Вирішальне значення мають брокери або посередники підключення злочинних мереж, груп та окремих злочинців, які сприяють злочинному бізнесу, зв'язуючи виробників з оптовими дистриб'юторами, дистриб'юторів з постачальниками транспорту, а також полегшують доступ до інформаторів, вбивць, підробників документів та інших спеціалістів з кримінальної справи [3, с. 26-30].

Натомість спецслужби країни-агресора намагаються використати кіберзлочинність проти нашої країни. Зокрема, вінницькі кіберполіцейські та слідчі спільно з кіберфахівцями обласного Управління СБУ викрили двох мешканців обласного центру, які організували діяльність ботоферми шляхом несанкціонованого втручання в роботу автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку. Щоденно ділки забезпечували реєстрацію сотень фейкових акаунтів у відомих соціальних мережах, у тому числі заборонених на території України. За оперативною інформацією, фігуранти за допомогою платіжних сервісів рф могли продавати новостворені облікові записи агентам країни-агресора, які у подальшому використовували їх для проведення ІПСО та поширення закликів до українців ухилятися від мобілізації. Правоохоронці провели

обшуки у приміщеннях вінничан та вилучили комп'ютерну техніку і серверне обладнання, зокрема десятки модемів та 19 шлюзів, спеціалізоване програмне забезпечення і майже 20 тисяч сім-карток українських мобільних операторів [4].

В Україні судитимуть учасника міжнародного хакерського угруповання, причетного до нанесення понад 3 млрд грн збитків країнам Європи та Північної Америки. Зловмисники атакували промислові підприємства у Франції, Німеччині, США, Норвегії, Нідерландах і Канаді, використовуючи власноруч розроблені віруси-шифрувальники. Таким чином хакери отримували доступ до серверів через зламані акаунти співробітників, викрадали інформацію і зашифровували комп'ютери, після чого вимагали викуп у криптовалюті. Особу й місце перебування одного з найактивніших членів ОЗУ – 49-річного киянина – встановили українські кіберполіцейські. До багаторівневої міжнародної спецоперації долучилися Європол, Євроюст і правоохоронні органи з кількох провідних країн світу. Разом із ними українські поліцейські провели понад 80 обшуків і припинили діяльність угруповання. Під час обшуків вилучили комп'ютерну техніку з доказами скоєних злочинів, банківські та сім-картки та майже 4 млн грн. Також у співпраці з іноземними колегами українські поліцейські виявили криптоактиви на суму понад 24 млн грн, 9 елітних автомобілів та 24 земельних ділянки загальною площею майже 12 га. Доведено, що за допомогою програми-вимагача зловмисники заблокували понад 4000 інформаційних систем норвезького підприємства і зашифрували наявну там інформацію, після чого вимагали 2500 біткоїнів (еквівалент 348 млн грн) за її дешифрування. Сума завданої підприємству майнової шкоди шляхом тимчасового зупинення його діяльності внаслідок кібератаки складала 8,9 млн євро. У вересні 2024 року слідчі Нацполіції завершили досудове розслідування відносно українського фігуранта і скерували обвинувальний акт до суду [5].

Зважаючи на особливу небезпеку подібного виду злочинів для всієї світової спільноти, у вересні 2024 року в місті Гаага кіберполіцейські та слідчі Нацполіції поділилися з іноземними колегами з провідних країн світу успішним досвідом знешкодження міжнародних угруповань хакерів-вимагачів. Окрім цього, правоохоронці різних країн ознайомилися з передовими методами виявлення, дослідження та знешкодження шкідливого програмного забезпечення. Проведена зустріч стала ще одним важливим кроком для протидії глобальним кіберзагрозам та захисту об'єктів критичної інфраструктури країн-учасниць.

Література

1. Internet Organised Crime Threat Assessment IOCTA 2024.pdf URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
2. Завдав провідній світовій компанії сотні мільйонів збитків: кіберполіція та слідчі Нацполу викрили хакера URL: https://www.npu.gov.ua/news/zavdav-providnii-svitovii-kompanii-sotni-milioniv-zbytkiv-kiberpolitsiia-ta-slidchi-natspolu-vykryly-khakera?fbclid=IwY2xjawHJT2FleHRuA2FlbQIxMAABHU6YgarhPiekST5eJI5Zo1xKDyWjQoPv1fYxghH9P60E1pJGBssh7F-uaQ_aem_FjTnuupWN8X-1pAdveKPSQ
3. EUROPOL. EU Serious and Organised Crime Threat Assessment 2021. A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime URL: https://www.europol.europa.eu/
4. Створювали сотні фейкових акаунтів щодня: поліція Вінниччини припинила діяльність ботоферми з ворожою пропагандою URL: https://cyberpolice.gov.ua/

news/stvoryuvaly-sotni-fejkovyx-akauntiv-shhodnya-policziya-vinnychchyny-prypynyla-diyalnist-botofermy-z-vorozhoyu-propagandoyu-6879/
5. Понад 3 мільярди гривень збитків країнам Європи й Північної Америки: в Україні судитимуть учасника міжнародного хакерського угруповання URL: https://cyberpolice.gov.ua/news/ponad--milyardy-gryven-zbytkiv-krayinam-yevropy-j-pivnichnoyi-ameryky-v-ukrayini-sudytymut-uchasnyka-mizhnarodnogo-xakerskogo-ugrupovannya-3103/

Моргунова Тетяна Іванівна
доцент кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, кандидат технічних наук, доцент

ХМАРНІ ТЕХНОЛОГІЇ В СИСТЕМІ ПІДГОТОВКИ ПРАВООХОРОНЦІВ: ЕФЕКТИВНІСТЬ ТА ВИКЛИКИ ВПРОВАДЖЕННЯ

Сучасні технологічні перетворення охоплюють усі аспекти життя, включаючи сферу освіти. Заклади вищої освіти, які здійснюють підготовку фахівців для системи внутрішніх справ, мають йти в ногу з часом і впроваджувати новітні інструменти для забезпечення високої якості навчального процесу. Хмарні технології стали важливим компонентом цифрової трансформації, забезпечуючи доступ до актуальних знань, інтерактивних платформ і автоматизованих систем навчання. У даній роботі висвітлюються переваги хмарних технологій для системи підготовки правоохоронців, розкриваються основні аспекти їх ефективності, а також визначаються ключові виклики, що постають на шляху їх впровадження.

Однією з найбільших переваг хмарних технологій у контексті підготовки правоохоронців є забезпечення доступності навчальних ресурсів [1]. Хмарні платформи дозволяють здобувачам вищої освіти отримувати доступ до матеріалів незалежно від місця знаходження та часу. Це особливо важливо для працівників правоохоронних органів, які часто працюють у змінних умовах і потребують швидкого оновлення знань. Наприклад, хмарні сервіси можуть забезпечувати доступ до актуальних законодавчих актів, методичних рекомендацій чи навіть оперативних тренувальних сценаріїв у реальному часі.

Крім того, хмарні платформи сприяють інтерактивності навчання. Завдяки таким технологіям створюються реалістичні симуляції, які дозволяють здобувачам вищої освіти тренуватися у вирішенні складних ситуацій, що максимально наближені до реальних умов роботи. Наприклад, це можуть бути симуляції управління натовпом, реагування на надзвичайні ситуації або координація дій під час затримання правопорушників. Такий підхід сприяє розвитку критичного мислення, аналітичних здібностей та командної роботи.

Економічна ефективність хмарних технологій також є їхньою значною перевагою. Використання хмарних сервісів знижує витрати на інфраструктуру та технічне обслуговування. У той час як традиційні серверні рішення потребують значних фінансових ресурсів, хмарні платформи пропонують модель оплати за використання (pay-as-you-go), що дозволяє оптимізувати витрати. Крім того, їхня масштабованість дає можливість швидко адаптувати платформу до потреб окремих груп зацікавлених осіб або цілого закладу.

Важливим аспектом в системі підготовки фахівців є автоматизація процесів оцінювання. Хмарні технології дозволяють проводити тести, аналізувати їх результати в реальному часі та формувати індивідуальні рекомендації для здобувачів вищої освіти. Це знижує навантаження на викладачів, дозволяючи їм більше часу приділяти розробці навчальних матеріалів і вдосконаленню методик викладання. Наприклад, автоматизовані тести можуть не лише оцінювати знання, але й аналізувати слабкі місця в підготовці кожного здобувача вищої освіти.

Однак усі ці переваги можуть бути реалізовані лише за умови подолання викликів, які супроводжують процес впровадження хмарних технологій.

Першим і найважливішим викликом є забезпечення безпеки даних. Система внутрішніх справ оперує великою кількістю конфіденційної інформації, витік якої може мати серйозні наслідки як для освітнього процесу, так і для національної безпеки. Використання хмарних платформ вимагає впровадження складних механізмів захисту, таких як багаторівневе шифрування, контроль доступу та моніторинг активності користувачів. Важливо також обирати провайдерів хмарних послуг, які відповідають національним стандартам безпеки.

Другим суттєвим викликом є інфраструктурна готовність закладів вищої освіти. У багатьох регіонах України спостерігається недостатній рівень розвитку мережевої інфраструктури, що обмежує можливості використання хмарних рішень. Наприклад, відсутність швидкісного Інтернету або сучасного обладнання може ускладнити доступ до навчальних матеріалів чи функціонування інтерактивних тренажерів. Це вимагає інвестицій у модернізацію освітньої інфраструктури та розширення технічної підтримки.

Не менш важливим є людський фактор. Викладачі та здобувачі вищої освіти часто стикаються з труднощами у використанні нових технологій через брак досвіду або небажання змінювати звичні підходи до навчання. Це створює потребу в організації тренінгів та інформаційних кампаній, які допоможуть подолати психологічний бар’єр і підготувати персонал до ефективної роботи з хмарними платформами.

Юридичні аспекти також відіграють значну роль в системі підготовки правоохоронців. Використання закордонних хмарних платформ часто регулюється міжнародними нормами та національним законодавством [2]. Наприклад, питання збереження даних за межами країни може створювати ризики для їхньої конфіденційності. Тому необхідно розробляти власні національні рішення, які відповідатимуть вимогам безпеки та правовим нормам.

Слід відмітити, що попри виклики, хмарні технології є потужним інструментом для модернізації освітнього процесу в закладах освіти [3], зокрема, закладах системи внутрішніх справ. Для успішного впровадження цих технологій необхідно враховувати особливості правоохоронної діяльності та дотримуватися комплексного підходу.

1. Розробити національну хмарну платформу, яка відповідатиме вимогам безпеки та буде спеціально адаптована для закладів освіти системи внутрішніх справ.
2. Інвестувати у розвиток інфраструктури**,** зокрема забезпечення швидкісного Інтернету та сучасного обладнання в навчальних закладах.
3. Забезпечити підвищення цифрової грамотності викладачів і здобувачів освіти через спеціалізовані тренінги, семінари та навчальні курси.
4. Інтегрувати хмарні технології поетапно, починаючи з пілотних проєктів, що дозволить врахувати потенційні ризики та коригувати підхід на основі отриманого досвіду.

5. Регулярно проводити аудит безпеки, щоб запобігти витоку даних і підвищити довіру до використання хмарних рішень.

На завершення відзначимо, що впровадження хмарних технологій у систему підготовки правоохоронців сприятиме підвищенню доступності, інтерактивності та ефективності навчання. Водночас, вирішення існуючих викликів дозволить створити сучасне освітнє середовище, яке відповідатиме вимогам часу та сприятиме формуванню висококваліфікованих кадрів для системи внутрішніх справ.

Література

1. Зінченко А.О. Використання хмарних технологій для навчання правоохоронців. Цифрова трансформація освіти. 2020. № 2. С. 15-23.
2. Кулинич О.І. Юридичні аспекти використання хмарних технологій у системі підготовки правоохоронців. Вісник права та безпеки. 2022. № 2. С. 120-128.
3. Сітченко В.М., Пилипенко Ю.А. Хмарні платформи для моделювання навчальних процесів у закладах вищої освіти. Технології в освіті. 2021. № 5. С. 59-67.

Мукан Іван Васильович

В.о. доцента кафедри права, Львівський національний університет природокористування, доктор філософії

Котовська Ольга Петрівна

доцент кафедри адміністративного та фінансового менеджменту, Національного університету «Львівська політехніка», кандидат філософських наук, доцент

СПІВПРАЦЯ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ З ГРОМАДСЬКИМИ (НЕУРЯДОВИМИ) ОРГАНІЗАЦІЯМИ В ПИТАННЯХ КРИМІНАЛЬНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ

Активний розвиток кібертехнологій та ІТ-бізнесу в останні роки активно спонукає для вчинення злочинів онлайн та у сфері інформаційних технологій. У всьому світі злочини у кіберпросторі щороку завдають збитків на десятки мільярдів доларів США як державам, так і приватним компаніям. Важливим аспектом оперативного та ефективного реагування на кіберзагрози є співпраця органів сектору безпеки з приватними компаніями та неурядовими (громадськими) організаціями у сфері кримінально-правової охорони кіберпростору. Така взаємодія сприятиме усуненню прогалин у методах протидії кіберзлочинам.

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. У Кримінальному кодексі України відсутнє визначення поняття «кримінальне правопорушення з використанням кіберпростору», тоді як це формулювання використовується у Законі України «Про основні засади забезпечення кібербезпеки України».

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті

функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [6].

Органи сектору безпеки відіграють головну роль у кримінально-правовому захисті кіберпростору, зокрема у забезпеченні протидії злочинам, захисті об'єктів критичної інфраструктури.

До органів сектору безпеки належать Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Антитерористичний центр при Службі безпеки України, Служба судової охорони, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України [5].

У 2001 році 35 держав (країни Ради Європи, а також Австралія, Домініканська Республіка, Японія, Панама, США) прийняли Конвенція про кіберзлочинність, яку Україна ратифікувала 07 вересня 2005 року. Конвенція про кіберзлочинність стала основою для гармонізації національного законодавства у сфері кіберпростору, яка продовжується і зараз. Конвенція спрямована на доповнення існуючих конвенцій Ради Європи щодо співробітництва у кримінальній сфері, а також аналогічних угод між державами-членами Ради Європи та іншими країнами. Її мета - підвищити ефективність кримінальних розслідувань і судових переслідувань, пов'язаних із правопорушеннями, що стосуються комп'ютерних систем та даних. Окрім того, Конвенція створює правові умови для збору доказів у кримінальних справах, зокрема в електронній формі, що сприяє вдосконаленню міжнародного співробітництва у протидії кіберзлочинності [2].

Правові та організаційні основи забезпечення захисту інтересів у кіберпросторі в Україні визначено у Законі України «Про основні засади забезпечення кібербезпеки України». У статті 10, п. 5 зазначеного Закону визначено можливість залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до розробки ключових галузевих проєктів і нормативних документів у сфері кібербезпеки [6]. У статті 6, п. 3 цього ж Закону передбачено, що громадські організації, разом із науковими установами, незалежними аудиторами та експертами з кібербезпеки, беруть участь у розробленні нормативно-правових актів, які регламентують проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури відповідно до міжнародних стандартів, а також стандартів Європейського Союзу та НАТО [6].

У цьому контексті доцільно уточнити особливості національного та міжнародного законодавства, які регулюють участь громадських (неурядових) організацій у забезпеченні безпеки кіберпростору. Закон України «Про громадські об'єднання» визначає дві форми громадських об'єднань (громадська організація або громадська спілка) правові засади діяльності, їхню незалежність від державних органів та право на участь у процесах, що мають суспільне значення [4]. Зазначеним Законом у статті 2. п.4. перечалено поняття «неурядові організації» у контексті діяльності інших держав та міжнародних неурядових організацій: «Неурядові організації інших держав, міжнародні неурядові організації (далі – іноземні неурядові організації) діють на території України відповідно до цього та інших законів України, міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України» [4]. Фактично згідно національного законодавства та міжнародних нормативно-правових актів, зокрема Ради

Європи, поняття «громадська організація» та «неурядова організація» використовуються як синоніми, хоча неурядові організації є дещо ширшим поняттям.

Термін «неурядова організація» (non-governmental organization) бере свій початок із часу створення Організації Об'єднаних Націй у 1945 році. У розділі 10, статті 71 Статуту ООН вперше визначено консультативну роль неурядових організацій [7]. Згодом роль неурядових організацій у більшості країн із розвиненою демократією значно розширилась. Поряд із державним (урядом) та приватним сектором (бізнесом) вони сформували так званий «третій сектор», для якого характерні такі ознаки як: захист та представлення важливих для суспільства питань, некомерційність діяльності, незалежність і організаційний плюралізм [1]. Неурядові організації мають чітко визначені цілі, напрями діяльності (соціальні, економічні, політичні та екологічні) та функції, які можуть змінюватися залежно від потреб суспільства. Головні функції неурядових організацій: 1. надання підтримки як матеріальної, так і нематеріальної; 2. співпраця з урядом (органами державної влади) для вирішення суспільно важливих питань, участь у формуванні публічної політики; 3. захист і просування прав певних соціальних груп; 4. навчання їх (новим навичкам); 5. інформування щодо важливих питань; 6. мобілізація масової підтримки та залучення громадськості до розв'язання актуальних проблем [1].

На сьогоднішній день в Україні, як і в світі в цілому, рівень кібербезпеки явно недостатній. Міжнародна співпраця сприяє вирішенню цієї проблеми, однак основні зміни повинні бути здійснені в середині країни, щоб згодом передати світу наш успішний досвід боротьби з кіберзлочинністю і регулювання кіберпростору. Для цього держава і суспільство повинно об’єднати свої зусилля та зробити все можливе для подолання проблеми кіберзлочинності. Закон України «Про громадські об’єднання» набув чинності у 2013 році, але розвиток громадянського суспільства в Україні, зокрема громадських організацій, значно активізувався після 2014 року. Зважаючи на важливу роль як українських, так і міжнародних неурядових організацій у протидії агресії рф та подоланні її наслідків, доцільно переглянути окремі положення цього Закону [8], зокрема щодо координації діяльності у сфері кібербезпеки. На нашу думку залучення до вирішення цієї проблеми громадських (неурядових) організацій, які спеціалізуються у сфері кібербезпеки та інформаційних технологій дасть змогу пришвидшити виявлення та підняти рівень боротьби з правопорушеннями у кіберпросторі на якісно вищий рівень.

Література

1. Вахович І., Смолич Д. Неурядові організації: сутність поняття, ознаки, цілі та функції. Економіка та суспільство. 2022. Вип. 46. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2045/1974
2. Конвенція про кіберзлочинність, Рада Європи, Конвенція, Міжнародний документ, від 23.11.2001, URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
3. Кримінальний кодекс України, Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III, URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
4. Про громадські об'єднання, Закон України від 22.03.2012 № 4572-VI URL: https://zakon.rada.gov.ua/laws/show/4572-17#Text
5. Про національну безпеку України, Закон України від 21.06.2018 № 2469-VII URL: https://zakon.rada.gov.ua/laws/show/2469-19#n318
6. Про основні засади забезпечення кібербезпеки України, Закон України від 05.10.2017, № 2163-VIII, URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Статут Організації Об’єднаних Націй. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf
8. Яцина М. О. «Неурядові організації» vs. «громадські організації»: до питання співвідношення. Актуальні проблеми правознавства. 2022. Тернопіль. № 4. – С. 117-123. DOI:10.35774/app2022.04.117

Мусійовська Мар’яна Михайлівна
доцент кафедри інформаційних систем та технологій Львівського державного університету внутрішніх справ, кандидат технічних наук

ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Для формування професійних і загальнокультурних компетенцій майбутніх бакалаврів і магістрів потрібні нові умови навчання. Сфера вищої освіти дещо відстає від загальної діджиталізації, і необхідно докласти більше зусиль, щоб скористатися інструментами та сильними сторонами нових інформаційних технологій, одночасно вирішуючи проблеми щодо можливих зловживань, таких як кібервторгнення та проблеми конфіденційності[4].

Завдання розвитку законодавства у сфері освіти окреслюються Національною доктриною розвитку освіти, яка визначає систему концептуальних ідей та поглядів на стратегію і основні напрямки розвитку освіти до 2025 р. [2, 3].

Згідно зі Стратегією розвитку вищої освіти в Україні на 2021-2031 роки, в основу концептуальної моделі вищої освіти України має бути покладений кібернетичний принцип необхідного розмаїття [1].

Істотний вплив на впровадження нових інформаційних технологій здійснюють сучасні інформаційні технологічні тенденції, основні з яких такі:

- віртуалізація та «хмарні» технології;
- розширення використання сервісорієнтованих архітектур;
- впровадження мобільних пристроїв та рішень на корпоративному рівні для доступу до ресурсів та виконання корпоративних до атків;
- посилення диференціації користувацьких переваг;
- візуалізація, вебінари та відеоконференцзв'язок [6].

Одним із важливих шляхів забезпечення ефективного функціонування освітньої системи при впровадженні інформаційних технологій у навчальний процес у закладах вищої освіти є створення та використання електронних навчально-методичних комплексів. Усі документи у складі цього інформаційного комп'ютерного продукту – мультимедійні, у них завжди присутні елементи інтерактивності, вони можуть бути оформлені в вигляді набору веб-сторінок. Електронні навчальні комплекси можуть бути використані на лекційних заняттях (проказ відеозаписів, інтерактивних моделей та анімації), під час проведення лабораторних робіт, атестації та самостійної роботи здобувачів вищої освіти. Таким чином, електронний навчально-методичний комплекс це програмний мультимедіапродукт навчального призначення, що забезпечує безперервність та повноту дидактичного циклу процесу навчання та містить організаційні систематизовані

теоретичні, практичні, контролюючі матеріали побудовані на принципах системного підходу, інтерактивності інформаційної відкритості [4].

Щоб підвищити ефективність роботи закладу вищої освіти, потрібно комплексно впливати на систему в цілому стратегію, мережеву інфраструктуру, організаційну структуру, систему управління, систему мотивації до праці, корпоративну культуру. Для вирішення завдання інформатизації закладу вищої освіти необхідно створити його єдину електронну систему, яка б дозволила управляти знаннями, що забезпечило б розвиток інновацій, збільшення продуктивності праці шляхом скорочення часу пошуку потрібного рішення в управлінні та обсягу виконаних робіт, підвищення компетентності персоналу. В результаті користувачі отримають доступ до високоякісної інформації, а самі рішення в галузі інформаційних технологій будуть так задіяні в основні ділові процеси закладу вищої освіти, що персонал і здобувачі вищої освіти вже не зможуть обходитися без сервісів, що надаються інформаційним середовищем. При цьому підвищується ефективність виконання персоналом його посадових обов'язків, підвищується якість навчання здобувачів вищої освіти, що робить інвестиції в інформаційні технології економічно виправданими [4].

Можна виділити такі основні завдання, виконання яких спрямовані на формування єдиної інформаційної системи закладу вищої освіти:

- формування організаційної структури інформатизації;
- створення інформаційної інфраструктури закладу вищої освіти та автоматизація її управління;
- інформатизація процесів управління закладом вищої освіти, зокрема фінансами;
- інформатизація навчального процесу,
- інформатизація наукових досліджень та проектів;
- підвищення рівня компетентності персоналу у сфері інформаційних технологій [5].

При створенні інформаційної системи закладу вищої освіти слід забезпечувати розумний обсяг інновацій як у навчальній, так і в управлінській діяльності. Створення та організація єдиної інформаційної системи закладу вищої освіти – складне організаційне та технологічне завдання, що обумовлює доцільність поетапної розробки системи: розв'язання задачі отримання на кожному етапі закінченого продукту, який послідовно модифікуватиметься та нарощуватиметься від етапу до етапу. Тільки на такій основі може бути забезпечене стійке функціонування інформаційної системи вищої освіти.

Інформатизація вищої освіти в Україні є одним із пріоритетних напрямків реформування вищої школи. На шляху інформатизації навчального процесу важливим є створення, впровадження та розвиток комп'ютерно орієнтованого освітнього середовища на основі інформаційних технологій, систем, мереж та ресурсів.

Це – комплекс перетворень, пов'язаних із насиченням освітньої системи інформаційною продукцією, інформаційними засобами, що грунтуються на мікропроцесорній техніці, та інформаційними технологіями при всебічному використанні можливостей системного підходу як методологічної бази.

Ресурс системного підходу, інтегрованого застосуванням інформаційних технологій у процесі професійної підготовки, позволяє організаторам та учасникам навчального процесу чітко усвідомлювати взаємозв'язок усіх компонентів освітньої системи та більш ефективно реалізовувати основні її функції: організацію, керівництво, контроль.

Література

1. Міністерство освіти і науки України Стратегія розвитку Вищої освіти в Україні на 2021-2031 роки [Електронний ресурс]. Режим доступу: https://mon.gov.ua/storage/app/media/rizne/2020/09/25/rozvitku-vishchoi-osviti-v- ukraini-02-10-2020.pdf
2. Президент України Указ № 347/2002. Про Національну доктрину розвитку освіти [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/-347/2002#Text
3. Президент України Указ № 344/2013. Про Національ стратегію розвитку освіти в Україні на період до 2021 року [Електронний ресурс]. Режим доступу: https://mon.gov.ua/storage/app/media/news/2022/04/15/VO.plan.2022-2032/Stratehiya.rozv.VO-23.02.22.pdf
4. Мусійовська М.М. Організація навчального процесу у закладах вищої освіти із застосуванням інформаційних технологій: збірник наукових статей за матеріалами доповідей Науково-практичної конференції 22 грудня 2023 року / Львів: ЛьвДУВС, 2023. – С. 120-122.
5. Польгун К. В. Організаційні засади створення електронного освітнього середовища закладу вищої освіти на базі платформи MOODLE. Фізико- математична освіта. 2020. Ч. 1. № 3(25). С. 68-73 [Електронний ресурс]. Режим доступу: https://fmo-journal.fizmatsspu.sumy.ua/journals/2020-325-1/20203-25-Polhun FMO.pdf
6. Cloud Computing: Concepts, Technology & Architecture. by Thomas Erl, Ricardo Puttini, Zaigham Mahmood. [Електронний ресурс]. Режим доступу: https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/0133387526.pdf

Новосьолова Єлизавета Юріївна

курсант 3-го курсу, ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

В.о. завідувача кафедри оперативно-розшукової діяльності, ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ ДЕПАРТАМЕНТУ ВНУТРІШНЬОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Підрозділи Департаменту внутрішньої безпеки Національної поліції України (далі – ДВБ НПУ) є одними з ключових суб’єктів документування злочинів, вчинених поліцейськими. Існує досить багато способів забезпечення ефективного здійснення підрозділами ДВБ НПУ оперативно-розшукової діяльності, спрямованої на виконання покладених законом на цей орган завдань, тож вважаємо, що правильна організація збору, систематизації та обробки оперативно значущої інформації відіграє важливу роль у цьому процесі. Погоджуємось із думкою про те, що результативність діяльності

правоохоронних органів у боротьбі зі злочинністю безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності [2, с.23].

Хоча законодавство конкретно не роз'яснює які саме дії можуть вчиняти працівники ДВБ у межах вирішення питань щодо інформаційно-аналітичного забезпечення, деякі положення Наказу Національної поліції України від 09.11.2015 №83 визначають окремі повноваження на користування інформаційними ресурсами Національної поліції та Міністерства внутрішніх справ. Так, працівникам оперативних підрозділів Департаменту внутрішньої безпеки надається право відповідно до вимог законодавства України створювати, накопичувати та використовувати окремі оперативно-розшукові, оперативно-профілактичні та оперативно-довідкові бази даних, обліки, в тому числі картотеки, справи контрольно-наглядового провадження та автоматизовані інформаційні системи за напрямами роботи ДВБ [1].

Окрім зазначеного вище, на нашу думку, ДВБ, будучи складовою частиною апарату Національної поліції України, може користуватись повноваженнями, покладеними на поліцію, у сфері інформаційно-аналітичного забезпечення. Такі повноваження визначаються статтею 25 Закону України «Про Національну поліцію» і передбачають можливість працівників формувати реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користуватись цими та іншими реєстрами, базами (банками) даних; здійснювати інформаційно-пошукову та інформаційно-аналітичну роботу; здійснювати інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями; створювати власні реєстри та бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону, та інформаційно-аналітичні системи (у тому числі міжвідомчі), необхідні для виконання покладених на неї повноважень [5].

До таких обліків, зокрема, відносимо автоматизовану інформаційну систему оперативного призначення, в якій організовано обробку інформації з грифом секретності «таємно» (далі – АІС ОП)., окремо впроваджену з метою забезпечення оперативно-розшукової діяльності оперативних підрозділів кримінальної поліції, на виконання вимог Закону України «Про оперативно-розшукову діяльність», Наказу МВС України від 05.05.2016 р. № 07 [6, с.72]. АІС ОП є сукупністю програмно-технічних та технічних засобів електронних комунікацій і призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності та діяльності з проведення кримінального аналізу Національної поліції України, крім інформації, яка обробляється в інформаційно-пошуковій системі «Філін» Національної поліції України [4].

Важливим аспектом діяльності ДВБ є те, що цей орган може не лише користуватись облікованою інформацією, а й виступати її розпорядником. Так, ДВБ здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, що належать до його компетенції [1]. Оскільки основним завданням цього органу є забезпечення внутрішньої безпеки в Національній поліції України, вважаємо, що до інформації, що передається уповноваженим особам належать дані про попередження та виявлення кримінальних, корупційних та пов'язаних з корупцією правопорушень серед поліцейських, державних служ-

бовців та інших працівників поліції. Для забезпечення оперативного обміну повідомленнями та інформацією оперативно-розшукового характеру між підрозділами, що здійснюють оперативно-розшукову діяльність, створюються галузеві інформаційні мережі, які є складовою частиною інформаційної мережі правоохоронних органів. В правоохоронних відомствах створюються спеціальні галузеві служби, що займаються інформаційним забезпеченням, в МВС України це, Департамент інформаційно-аналітичної підтримки Національної поліції України [3, с.140].

У висновку можемо зазначити, що основні можливості і повноваження ДВБ у сфері здійснення інформаційно-аналітичної роботи не передбачаються прямо у нормативному акті, який регулює його діяльність, а певною мірою випливають із документів, які становлять правову основу діяльності Національної поліції в цілому. Ефективність підрозділів ДВБ значною мірою залежить від правильної організації інформаційно-аналітичної діяльності, що може включати доступ до баз даних, формування власних реєстрів, обробку оперативно значущої інформації, а також використання автоматизованих систем, таких як АІС ОП. Водночас ДВБ виступає розпорядником інформації, забезпечуючи керівництво поліції й інші державні органи даними про попереджені та виявлені злочини, корупційні правопорушення і порушення дисципліни серед працівників поліції.

Література

1. Наказ Національної поліції України від 09.11.2015 №83 «Про затвердження Положення про Департамент внутрішньої безпеки Національної поліції України»
2. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навчальний посібник. Львів: ЛьвДУВС, 2017. – 244 с.
3. Поляк, С. П., & Батрух, В. Ю. (2022). Інформаційне забезпечення діяльності оперативних підрозділів МВС України. Редакційна колегія, 140.
4. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС : Наказ М-ва внутр. справ України від 20.10.2017 № 870 : станом на 15 лют. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z1433-17#Text
5. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII : станом на 16 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
6. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

Огірко Ольга Ігорівна

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університет внутрішніх справ кандидат технічних наук, доцент

ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ТА ДОПОВНЕНОЇ РЕАЛЬНОСТІ В ПІДГОТОВЦІ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ: ЗАРУБІЖНИЙ ДОСВІД

Віртуальні технології (VR) та технології доповненої реальності (AR), які здатні проектувати цифрову інформацію (зображення, відео, текст, графіку) поза екранами

пристроїв та об’єднувати віртуальні об’єкти з реальним середовищем є одними з перспективних освітніх інформаційних технології в сучасному суспільстві.

Віртуальна реальність – це штучно створений світ, який завдяки спеціальним технічним засобам дозволяє кожному здобувачу вищої освіти повністю зануритися у вигадане середовище. Унікальність VR полягає у впливі на більшість органів чуття людини, включаючи зір, слух, дотик і навіть нюх [1].

Доповнена реальність – це технологія, що інтегрує в реальний світ додаткові елементи комп’ютерної графіки, створюючи розширене уявлення про навколишнє середовище та дозволяючи користувачеві залишатися в контакті з реальністю [1-2].

Прикладом впровадження технологій віртуальної та доповненої реальності в освітній процес є створення віртуальних лабораторій. Це інтерактивні навчальні середовища, які дають здобувачам освіти можливість проводити лабораторні досліди та вивчати наукові концепції онлайн, без необхідності відвідування фізичної лабораторії. Зокрема, у листопаді 2022 року Міністерство освіти і науки України уклало угоду з Labster, світовим лідером з розроблення віртуальних навчальних симуляторів, на платформі якої успішно навчається більше 5 млн. студентів та учнів 3000 навчальних закладів в 70 країнах світу.

Технології VR та AR дозволяють наочно проводити лекції, тренінги й демонстрації, а також візуалізувати об’єкти та процеси, які неможливо відтворити у реальності. До основних переваг впровадження віртуальної та доповненої реальності в процес навчання фахівців сектору безпеки та оборони доцільно віднести [1-4]:

- покращенню розуміння складної інформації через інтерактивні візуалізації;
- формуванню нових практичних навичок;
- деталізацію природних процесів, явищ чи об’єктів через візуалізацію навчальних матеріалів;
- створення безпечного середовища для практичних і лабораторних робіт;
- можливість багаторазового повторення експериментів для вдосконалення навичок;
- адаптацію навчання до індивідуальних потреб, включно зі студентами з особливими освітніми потребами;
- інтеграцію технології BYOD (Bring Your Own Device) для персоналізації навчання;
- застосування теоретичних знань на практиці для розвитку ключових компетентностей;
- створення “wow-ефекту”, який сприяє активізації уваги та інтересу до навчання.

Використання технологій віртуальної та доповненої реальностей у підготовці фахівців сектору безпеки є важливим кроком до модернізації та підвищення ефективності навчання. Найкращі практики впровадження VR та AR представлені у таких країнах: Сполучені Штати Америки, Ізраїль, Велика Британія, Німеччина та Китай [5-6]. Досвід, набутий цими країнами, може стати в нагоді для Україні у покращенні рівня розвитку інформаційних технологій, враховуючи динамічні темпи, якими вони змінюються (табл. 1).

Таблиця 1

Країна	**Використання VR та AR в секторі безпеки та оборони**
США	тренування військових з допомогою технологій VIRTSIM дозволяє в умовах бойових операцій моделювати сценарії на полі бою з використанням датчиків руху та VR-гарнітур; поліцейські використовують VR для моделювання ситуацій, пов'я-заних із переговорами, управлінням натовпом та реагуванням на збройні напади
Ізраїль	тренувань солдатів у ситуаціях міської війни та терористичних загроз, зокрема: система SkyHawk: VR-тренажер, що дозволяє пілотам і опера-торам дронів виконувати місії в реалістичних умовах; для навчання польових медиків, відпрацювання навичок надання першої допомоги в бойових умовах
Велика Британія	для підготовки до операцій у міських умовах та вдосконалення командної взаємодії: система Bohemia Interactive Simulations (BIS) - реалістичні військові тренажери, що використовують віртуальні ландшафти для відпрацювання стратегій та тактик; поліцейські застосовують VR для симуляції кризових ситуацій, напри-клад, захоплення заручників або масових заворушень
Німеччина	для навчання технічному обслуговуванню військової техніки VR-тренажери для танкових екіпажів створюють реалістичні бойо-ві сценарії для навчання водіїв та стрільців у танках; AR-технології застосовують в підготовці фахівців з кібербезпеки для виявлення й протидії кібератакам
Китай	у підготовку військових льотчиків, операторів дронів та морських сил військові симулятори: Тренажери для військово-морського флоту, які дозволяють навчатися у реалістичних умовах без необхідності використовувати реальні кораблі; AR використовується для навчання інженерів з обслуговування військь-кової техніки, спрощуючи доступ до інформації про обладнання
Канада	для тренувань солдатів, зокрема у холодному кліматі та арктичних умовах використання AR у підготовці рятувальних підрозділів для пошуку та евакуації постраждалих у надзвичайних ситуаціях
Австралія	для відпрацювання спільних операцій з іншими країнами, зокрема у міжнародних миротворчих місіях платформа Immersive Tactical Trainer: забезпечує навчання в умо-вах бойових дій, включаючи управління складними операціями

Зарубіжний досвід демонструє ефективність впровадження VR/AR-технологій у підготовку фахівців сектору безпеки та оборони. Країни світу використовують ці інно-ва-ційні інструменти для підвищення рівня підготовки персоналу, оптимізації навчального процесу та відпрацьовування навиків реагування без ризику для життя. Такі тренування забезпечують занурення в умовний сценарій, дозволяючи аналізувати поведінку, прийняття рішень і командну роботу в умовах стресу. Україна може використовувати ці практики для вдосконалення власної системи навчання.

Література

1. Войцеховська О. О. Технології доповненої та віртуальної реальності в освіті. Матеріали LII науково-технічної конференції підрозділів ВНТУ, Вінниця, 20-23 червня 2023 р. 2023. URL: https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2023/paper/view/17990.
2. Волинець В. Використання технологій віртуальної реальності в освіті. Непе-рерв-на професійна освіта: теорія і практика, №2, 2021. С. 40–47. URL: https://doi.org/-10.28925/1609-8595.2021.2.5.
3. Огірко О. І. Використання вітруальних технології та технології доповненої реальності в освітньому процесі. Інформаційні технології в освіті та практиці: матеріали Всеукраїнської науковопрактичної конференції (Львів, 18 грудня 2020). Львів: ЛьвДУВС, 2020. С. 36-38.
4. Віртуальна та доповнена реальність: як нові технології надихають вчитися URL: https://osvitoria.media/opinions/virtualna-ta-dopovnena-realnist-yakoyu-mozhe-buty-suchasna-osvita/
5. Unimersiv: VR Training // Virtual Reality Education URL: https://unimersiv.com/
6. Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 – 2030, Available at: https://www.grandviewresearch.com/industry-analysis/education-technology-market

ОСАДЧА Варвара,

здобувач вищої освіти 2 курсу спеціальності 126 «Інформаційні системи та технології»

ГАЛАЙКО Наталія,

старший викладач кафедри інформаційних систем та технологій Львівського державного університету внутрішніх справ

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АНАЛІЗІ ВЕЛИКИХ ДАНИХ

Штучний інтелект (ШІ) як наукова галузь існує з середини XX століття. Протягом останніх десятиліть, в процесі розвитку цієї галузі, яка фокусується на створенні автоматизованих інтелектуальних систем, були розроблені концептуальні моделі, методи та підходи. Багато ідей штучного інтелекту вже інтегровані у спеціалізовані технології, що стали невід'ємною частиною повсякденного життя. ШІ змінив сучасні підходи до аналізу даних і прийняття рішень, і нині застосовується в численних сферах, таких як медицина, промисловість, наука, фінанси, освіта та інші.

Т. Яровой відзначає, що використання ШІ може суттєво полегшити життя та роботу людей. Автоматизація рутинних і повторюваних завдань за допомогою ШІ може вивільнити людей від монотонної роботи і дозволити їм більше уваги приділяти складнішим і творчим завданням [1, с. 39].

Штучний інтелект має численні переваги та недоліки, які визначають його роль у сучасному світі. До переваг належать уникнення помилок, що особливо важливо у високоточних галузях, таких як медицина, де роботизовані системи забезпечують високу точність. ШІ знижує ризики для людини, виконуючи небезпечні завдання, працює безперервно без втрати продуктивності та широко використовується у вигляді цифрових помічників, таких як чат-боти й голосові асистенти. Він є ключовим драйвером інновацій у технологіях, наприклад, в автономному транспорті, та забезпечує об'єктивність у прийнятті рішень, виключаючи вплив емоцій. Також ШІ ефективно виконує рутинні завдання та відіграє вирішальну роль у медицині, покращуючи діагностику й терапевтичні методи.

Серед недоліків виділяються високі витрати на розробку та впровадження систем, обмеження в креативності, ризик зростання безробіття через автоматизацію, залежність від технологій, що може впливати на когнітивні здібності людини, відсутність емоцій, яка ускладнює міжособистісну взаємодію, та потреба в людському втручанні для удосконалення або коригування роботи системи [1].

Впровадження штучного інтелекту (ШІ) у аналіз великих даних відкриває нові можливості для ефективної обробки та інтерпретації величезних обсягів інформації, що раніше було складно зробити за допомогою традиційних методів. ШІ дозволяє значно покращити процеси збору, обробки та аналізу даних, що робить їх більш точними та корисними для прийняття рішень у реальному часі.

Слід підкреслити, що великі дані виступають своєрідним «паливом» для ШІ, тоді як ШІ надає їм потужні аналітичні інструменти. Взаємодія між великими даними та штучним інтелектом (ШІ) базується на п'яти ключових елементах (таблиця 1).

Ці елементи демонструють, як великі дані та ШІ взаємодіють, створюючи потужний інструмент для вирішення складних завдань у різних сферах.

Таким чином, поєднання великих даних і ШІ створює потужну платформу для інновацій та розвитку в різних сферах, включаючи бізнес, охорону здоров'я, науку та освіту. Здатність ШІ аналізувати дані з неймовірною швидкістю та точністю відкриває нові горизонти в наукових дослідженнях. У поєднанні зі суперкомп'ютерами він дозволяє вирішувати завдання, які раніше здавалися нерозв'язними.

Таблиця 1. Великі дані та штучним інтелектом [2]

Елемент взаємодії	**Опис**
Збирання даних	Великі дані характеризуються обсягом, цінністю, ре-зультативністю, правдивістю, точністю, візуалі-за-ці-єю, різноманітністю, швидкістю тощо. Алгоритми ШІ відіграють важливу роль у збиранні, обробці та ана-лізі цих даних, що забезпечує їхню корисність і релевантність для вирішення поставлених завдань.
Обробка даних	Алгоритми ШІ призначені для виявлення законо-мірностей і взаємозв'язків у великих наборах даних. Це дає

	змогу організаціям отримувати інсайти й прий-ма-ти обґрунтовані рішення на основі зібраної інфор-мації.
Машинне навчання:	Алгоритми машинного навчання, що є підмножиною ШІ, використовують великі обсяги даних для нав-чання, з метою прогнозування та прийняття рішень. Великі дані забезпечують необхідний матеріал для виявлення зако-номірностей, побудови моделей і формування точних прогнозів.
Обробка природної мови (NLP)	NLP працює з людською мовою. Великі дані допо-ма-га-ють навчати моделі, здатні розуміти та обробляти при-родну мову. Це використовується в чат-ботах, голосових помічниках (Siri, Google Assistant, Microsoft Cortana, Alexa) та інших інструментах.
Аналіз зображень і відео	ШІ також широко застосовується для аналізу візуаль-ної інформації, зокрема у великих обсягах зображень і відео, таких як контент у соціальних мережах. Алго-ритми вико-ристовують великі дані для навчання роз-піз-на-вання облич, класифікації об’єктів і виконання інших завдань, пов’язаних із візуальною аналітикою.

Література

1. Яровой Т. С. Можливості та ризики використання штучного інтелекту в публічному управлінні. Economic Synergy, (2), 2023. 36–47. https://doi.org/10.53920/ES-2023-2-3.
2. Горобець О. О. Взаємозалежність штучного інтелекту та великих даних: перспективи використання в економіці. Бізнес-аналітика в управлінні зовнішньоекономічною діяльністю: Матеріали X міжнародної науково-практичної конференції, 2023. С. 166-168.

Пастух Дмитро Сергійович

Студент 3 курсу Інституту права та безпеки Одеського державного університету внутрішніх справ

Матвєєвський Олег Володимирович

Старший викладач кафедри кримінально-правових дисциплін інституту права та безпеки Одеського державного університету внутрішніх справ

РОЗВИТОК КІБЕРЗАГРОЗ У КОНТЕКСТІ ГЛОБАЛІЗАЦІЇ ТА ВІЙСЬКОВОЇ АГРЕСІЇ РФ: УРОКИ ДЛЯ УКРАЇНИ ТА СВІТУ

Світ сьогодні опиняється під загрозою рекордних масштабів кібернападів, які постійно трансформуються і стають дедалі більш складними та важко прогнозованими. Кіберзлочинці використовують все новітніші та технічно досконаліші методи для досяг-нення своїх цілей, що ставить перед організаціями величезний виклик. Це вимагає не лише постійного оновлення захисних механізмів, але й глибокої адаптації до швидко змінюваного кіберсередовища. У сучасних умовах забезпечення високого рівня кібер-

безпеки стало не просто вимогою, а стратегічною необхідністю для підтримки безперебійної роботи та захисту конфіденційної інформації на всіх етапах діяльності організацій.

Втім, зростання кіберзагроз разом із нестачею досвідчених фахівців у сфері кібербезпеки, ставлять перед корпораціями, державними установами величезні виклики на глобальному рівні. Швидке зростання кіберзлочинності призводить не лише до значних фінансових втрат, але й до серйозних порушень в операційній діяльності компаній, зниження їх репутації та втрати довіри з боку клієнтів і партнерів. Крім того, такі атаки можуть викликати регуляторні санкції та штрафи, що ще більше ускладнює ситуацію для організацій, що не готові ефективно протистояти новітнім кіберзагрозам [2].

Фішинг, що став головною кіберзагрозою на початку масштабного вторгнення Росії в Україну у 2022 році, залишає за собою лідерство серед кіберзагроз у США, Канаді, Південній кореї та країнах Європейського Союзу і станом на середину 2024 року. Відомі компанії з кібербезпеки, зокрема PICUS Lab, ESET ChecPoint, відзначають, що ця загроза зберігає свою актуальність завдяки постійній еволюції методів і зміні тактик, які застосовують злочинні групи [4].

Один із різновидів фармінгу – це Advanced Persistent Threat (APT), або розширена постійна загроза. Це форма прихованої кібератаки, за якої зловмисник отримує несанкціонований доступ до цільової комп'ютерної мережі і зберігає його протягом тривалого періоду часу, залишаючись непоміченим. Основна мета APT полягає у викраденні або вилученні конфіденційних даних, а не у створенні перешкод у роботі мережі, відмові в обслуговуванні чи зараженні систем шкідливим програмним забезпеченням [2].

Дослідження кібератак виявили, що за цими атаками стоять численні хакерські угруповання, серед яких Gallium, Gamaredon, Webworm, MirrorFace, Kimsuky, ScarCruft, Sednit (Fancy Bear), FrostyNeighbor, MuddyWater, Mustang Panda, Lazarus, Citrine Sleet. Встановлено, що ці групи діють у інтересах розвідок та урядів Росії, Китаю, Північної Кореї та Іраку, що підтверджує глобальний характер та серйозні масштаби сучасних кіберзагроз. Ці угруповання використовують складні методи для здійснення атак, включаючи фішинг, зловмисне програмне забезпечення, експлойти в уразливостях систем та інші тактики, щоб отримати доступ до конфіденційної інформації, зламати мережі та інфраструктуру, а також здійснити шпигунство чи саботаж. Аналіз діяльності цих хакерських груп дозволяє зрозуміти, яким чином держави-агресори застосовують кіберпростір як інструмент для здійснення геополітичного впливу та реалізації стратегічного тиску.

У лютому 2024 року було виявлено високу активність хакерських угруповаанй, які орієнтуються на створенні психологічного впливу та дезінформації серед українців, особливо тих, хто проживає за кордоном. Зловмисники використовують електронну пошту як основний інструмент для поширення своїх повідомлень, спрямованих на маніпуляцію свідомістю. У вересні 2024 року були зафіксовані нові спроби атаки: були виявлені електронні листи, надіслані з адреси DCHC@headlineinteresting[.]pro, ймовірно, націленого на осіб, які проживають у Сумській області України. Лист містив дезінформаційне повідомлення українською мовою, що є частиною більш широкої кампанії з впливу на громадську думку серед населення [3]. Тіло електронного листа містить таке повідомлення українською мовою:

«Шановні жителі Сумської області!

Через російські авіаудари в регіоні почалися серйозні перебої з електроенергією та водопостачанням. Води і електрики не передбачається в найближчі три тижні.

Просимо вас в найближчі 48 годин придбати все необхідне для життя в екстрених умовах. У вкладенні – рекомендації, які допоможуть вам пережити цей складний період. Обов'язково перепишіть їх на папір.»

Також у 2024 р було вперше зафіксовано як хакерська група MirrorFace, яка раніше зосереджувалась на цільових атаках, розширила свою діяльність на європейські дипломатичні установи. Цей крок робить ЄС ще одним центром притягання для кіберзагроз з боку Китаю, Північної Кореї та Росії, які традиційно цікавляться державними структурами та оборонним сектором. Водночас, в Україні ситуація залишається напруженою, оскільки російські хакерські угруповання зокрема Gamaredon який покращив свій інструмент вилучення даних для настільної програми Signal – PteroSig. Це коригування було зроблено через останні зміни в Signal Desktop. Тепер PteroSig може аналізувати та розшифровувати використаний ключ, захищений DPAPI[1] (використовується в операційній системі Windows для симетричного шифрування асиметричних приватних ключів) програмою Signal, дозволяючи PteroSig знову розшифровувати та вилучати дані з Signal, завдаючи постійних ударів на державні установи, критичну інфраструктуру та оборонний сектор. Під час подібних атак зловмисники використовували як приманку майбутню Всесвітню виставку, яка відбудеться в 2025 році в Осаці, Японія. Під час цієї атаки MirrorFace надіслав жертві фішинговий електронний лист із посиланням на ZIP-архів під назвою The EXPO Exhibition in Japan in 2025.zip, розміщений на OneDrive та містить один **файл LNK під назвою Виставка** EXPO в Японії в 2025 році.docx. lnk, що маскується під документ Word. Після відкриття LNK, файл відображає документ Word-приманку, що зрештою призводить до розгортання версії 5.5.5 бекдору ANEL. Одним із. найвідоміших прикладів є NotPetya – Вірус Петя [3].

Аналізуючи вищезазначені дії хакерів, більшість з яких діють під контролем російських спецслужб, можна виокремити два основні пріоритети: перший – це психологічний вплив на населення, другий – це проведення APT та DDoS-атак, спрямованих на паралізацію державного, банківського та енергетичного секторів. Щодо другого пріоритету, то він є відносно зрозумілим: це стандартні атаки, які не вимагають суттєвих змін у тактиці. Однак, перший пріоритет є набагато складнішим і більш цікавим. Тут можна простежити елементи концепції канадського культуролога Маршала Маклуена, який досліджував, як медіа та технології впливають на формування громадської думки. Згідно з його теорією, медіа не лише передають інформацію, але й визначають, як суспільство сприймає реальність, що є важливим інструментом у веденні психологічної війни[5]. Тому Росія активно використовує медіа-простір для впливу на свідомість громадян, створюючи потрібні наративи і маніпулюючи інформацією з метою підриву морального духу та зміни ставлення до ключових подій. Тоді як в Україні інформаційна війна більше фокусується на захисті національних цінностей і боротьбі з дезінформацією, у той час як в Росії медіа використовуються для пропаганди та посилення політичного контролю.

Кіберзагрози є важливою складовою сучасних глобальних викликів, і їхній характер вимагає комплексних зусиль у боротьбі з ними. Зважаючи на технологічну

[1] DPAPI[1] - використовується в операційній системі Windows для симетричного шифрування асиметричних приватних ключів.

еволюцію атак і їхній стратегічний вплив на суспільство, критично важливо впроваджувати ефективні заходи безпеки, мінімальні з яких це – постійне оновлення захисних механізмів, навчання персоналу, розширення міжнародної співпраці, запровадження розширеного моніторингу мережі та аналітики поведінки користувачів UEBA – (це передова технологія, призначена для виявлення, прогнозування та запобігання потенційним ризикам у режимі реального часу, покращуючи рівень безпеки будь-якої організації. На відміну від традиційних інструментів безпеки, які зосереджені на попередньо визначених сигнатурах загроз, UEBA постійно навчається та адаптується, забезпечуючи проактивний захист від внутрішніх загроз, зловживання привілеями та вдосконалених постійних загроз (APT), створення резервних і відновлювальних планів, психологічний захист та боротьба з дезінформацією, посилення захисту IoT (internet of Things – комплекс фізичних мережевих пристроїв, що взаємодіють між собою за допомогою мережі зв'язку)

Література

1. Ахтирська Н., Гуцалюк М. Правові засоби боротьби з кіберзагрозами під час воєнного стану в світлі використання механізмів Другого додаткового протоколу до Конвенції про кіберзлочинність: матеріали Міжнародної науково-практичної конференції Актуальні питання розвитку юридичної науки та практики, м. Київ, 12 трав. 2022 р. / за заг. ред. д.ю.н., акад. НАПрН України О.П. Орлюк, к.ю.н., доц. Г.З. Остапенко, к.ю.н. А.В. Айдинян. Київ, 2022. С. 283-286.
2. Електронний ресурс, компанії в сфері кібербезпеки Onapsis https://onapsis.com/category/resources/case-studies/
3. ESET Threat Report H1 2024, https://www.eset.com/int/business/resource-center/reports/eset-threat-report-h1-2024/
4. NATO: Military cyber defenders need to be present on networks during peacetime. URL: https://therecord.media/nato-peacetime-cyberdefense-david-van-weel-cycon
5. Szapranski R. A Theory of Information Warfare; Preparing for 2020. Montgomery, Maxwell Air Force Base: Air University, 1995. URL: https://apps.dtic.mil/sti/citations/ADA328193

Пекарська Євгенія Олегівна

студентка 2-го курсу факультету № 4 Донецького державного університету внутрішніх справ

Бондаренко Ольга Олегівна

доцент кафедри цивільного, трудового права та права соціального забезпечення факультету № 4 Донецького державного університету внутрішніх справ,

кандидат юридичних наук, доцент

ПАРТНЕРСЬКІ ЗАСАДИ ДІЯЛЬНОСТІ ПРИВАТНИХ ДЕТЕКТИВІВ ТА ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

Розвиток сучасного державного демократичного механізму визначається з урахуванням загроз, які виникли після початку повномасштабної агресії росії проти нашої держави. Пріоритет надається силам безпеки і оборони України, які відстоюють

територіальну цілісність та незалежність України. Однак, не дивлячись на наявні небезпеки, в нашій країні поєднується розвиток інституцій, які регламентуються нормами як публічного так і приватного права.

На тепер в суспільстві розвиваються цивільні правові відносини, які пов'язані з різними видами договорів. Як приклад – надання приватних детективних послуг. Зазначаємо дефініцію про те, що в законодавстві Україні відсутня пряма заборона на здійснення детективної діяльності, але й немає її законодавчого регулювання. Чинним законодавством України договірні зобов'язання регулюються нормами Цивільного кодексу України від 16 січня 2003 року № 435-IV [1]. У главі 63 ЦК України зазначено те, що за договором про надання послуг одна сторона (виконавець) зобов'язується за завданням другої сторони (замовника) надати послугу, яка споживається в процесі вчинення певної дії або здійснення певної діяльності, а замовник зобов'язується оплатити виконавцеві зазначену послугу, якщо інше не встановлено договором [1, гл. 63]. Положення глави 63 ЦК України можуть застосовуватися до всіх договорів про надання послуг, якщо це не суперечить суті зобов'язання [1]. Це підтверджується і положеннями статті 3 ЦК України, яка визначає загальні засади цивільного законодавства. Однією із засад цивільного законодавства є свобода підприємницької діяльності, яка не заборонена законом.

Реалізація договору про надання детективних послуг в різних країнах має як правову регламентацію так і практичну реалізацію. Кращі практики детективної діяльності мають такі держави як США, Італія, Португалія, Японія, Канада та інші, в яких приватна детективна діяльність тривалий час функціонує та врегульована на рівні законодавства. При цьому розвиток сучасних інформаційних технологій та кіберпростору надає можливість приватним детективам ефективніше забезпечувати отримання необхідної замовнику інформації. Під кіберпростором український законодавець визначає середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [2].

На нашу думку приватні детективи можуть стати партнерами для державних правоохоронних органів при зборі через інформаційні ресурси доказів вчинення представниками країни агресора різних злочинів. Не дивлячись на відмінності у механізмах забезпечення прав людини, суспільних відносинах, які регулюються нормами публічного та приватного права поєднання державної правоохоронної функції з приватною детективною діяльністю, на нашу думку, ефективним буде саме при інформаційно-аналітичній взаємодії. Отже, договір надання детективних послуг спрямований на забезпечення майнових й особистісних немайнових відносин (цивільних правовідносин). Приватні детективні послуги, які здійснюються на підставі договору про надання приватних детективних послуг, укладеного між замовником та суб'єктом приватної детективної діяльності надаються шляхом пошуку, отримання, аналізу та фіксації інформації про осіб, об'єкти і події, встановлення місцезнаходження осіб та об'єктів із застосуванням засобів та методів, що не заборонені чинним законодавством України.

Своєю чергою оперативно-розшукова діяльність уповноважених суб'єктів виконує завдання щодо пошуку і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій

з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [3].

Як приклад, інформацією, що може сприяти розшуку особи, зниклої безвісти за особливих обставин визнаються будь-які відомості та/або дані про особу, зниклу безвісти, що можуть сприяти визначенню її місцеперебування, ідентифікації невпізнаних останків, визначенню місця поховання або місцезнаходження останків померлої особи [4]. Іншим напрямком спільної діяльності представників приватних детективів та правоохоронних органів може стати пошук інформації про місцезнаходження майна, яким незаконно заволоділи представники військових формувань країни-агресора. Або пошук інформації через можливості кіберпростору про майно, яке могло б забезпечити відшкодування нашим громадянам завданої агресором майнової шкоди. Відповідно безпосередній пошук інформації в соціальних мережах, приватних електронних інформаційних ресурсах в мережі Інтернет, зокрема: блог-платформах, відеохостингах, інших веб-ресурсах може сприяти ідентифікації потерпілих, свідків, злочинців, майна, різних подій тощо.

Відповідно, зазначаємо те, що розвиток інформаційно-комунікативних технологій засвідчує про те, що і приватна детективна діяльність і державна оперативно-розшукова діяльність використовує мережу Інтернет. Кіберпростір та пошук інформації з відкритих джерел є тому підтвердженням.

Отже, розвиток партнерських засад діяльності приватних детективів та правоохоронних органів у сфері інформаційного забезпечення це напрям, який може сприяти в подальшому, після деокупації тимчасово окупованих територій, відновленні дотримання прав громадян. На нашу думку запропонований механізм партнерських засад потребує правового регулювання з метою чіткого визначення компетенції суб’єктів взаємодії. При правовому регулюванні окремо необхідно звернути увагу на захист персональних даних та недопущення розголошення інформації, яка відноситься до державної таємниці чи службової інформації.

Література

1. Цивільний кодекс України від 16 січня 2003 року № 435-IV. Дата оновлення: 3 вересня 2024. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Дата оновлення: 28 червня 2024 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
3. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. Дата оновлення: 09.08.2024. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
4. Про правовий статус осіб, зниклих безвісти за особливих обставин: Закон України від 12 липня 2018 року № 2505-VIII. Дата оновлення: 18.10.2024. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text.

Пелехач Володимир Тарасович
курсант 3-го курсу, ННІПФПКП Львівського державного університету внутрішніх справ
Жуковський Ігор Вячеславович
викладач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КОРУПЦІЙНИМ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ У ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

В цій роботі ми розглянемо інформаційно-аналітичне забезпечення як діяльність зі збору, обробки, аналізу й надання інформації, що використовується у різних сферах, зокрема в органах сектору безпеки й оборони. Воно спрямоване на систематизацію даних, формування інформаційних ресурсів, прогнозування ситуацій та розробку рекомендацій для ефективної діяльності. Поєднуючи інформаційно-аналітичне забезпечення з протидією корупції в рамках діяльності органів сектору безпеки і оборони України, ми рухаємось в ногу з часом, використовуючи сучасні інформаційно-аналітичних технології, що дозволяє не лише виявляти й попереджати корупційні злочини правоохоронними органами, але й забезпечувати комплексну оцінку ризиків, закривати прогалини у внутрішніх процедурах і сприяти впровадженню кращих управлінських практик.

Сектор безпеки і оборони – система органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об’єднання, які добровільно беруть участь у забезпеченні національної безпеки України [1]. Інформаційно-аналітична система в секторі безпеки і оборони повинна бути на високому, пріоритетному рівні, так як має підвищений ступінь корупційних ризиків. Здебільшого питання протидії корупції покладено на Національне агенство з питань запобігання корупції (НАЗК), Національне антикорупційне бюро України (НАБУ), Національну поліцію України (НПУ) та спеціалізовану антикорупційну прокуратуру (САП), а також громадські організації, міжнародні компанії, органи місцевої влади, що допомагають правоохоронним органам України отримувати статистичну інформацію, забезпечують культурні заходи та розголошення інформації серед населення. Однією з таких організацій є Transparency International Ukraine, яка щорічно проводить підсумки щодо корупційної ситуації в Україні. На звіти Transparency International Ukraine активно посилається НАЗК, публікуючи їх на офіційному сайті [2]. Ми можемо бачити позитивну тенденцію змін, поступово долаючи корупційні проблеми.

На сьогодні в Україні інформаційно-аналітична діяльність здебільшого спрямована на розробку нових та вдосконалення вже існуючих баз даних. Це поширюється як на всіх громадян, так і на державні органи[3]. Прикладом забезпечення державою інформаційно-аналітичного забезпечення протидії корупційним кримінальним правопорушенням є наказ «Про затвердження порядку обліку корупційних діянь та інших правопорушень пов'язаних з корупцією»[4].

Важливим інструментом для боротьби з корупцією в Україні є Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення, основні цілі якого є виявлення та моніторинг осіб, які порушили антикорупційне законодавство; запобігання повторним правопорушенням; покращення прозорості та підзвітності; інструмент для органів контролю та правоохоронних органів. Затверджений такий реєстр Рішенням НАЗК № 166 від 09.02.2018[5]. Згідно з даних НАЗК в реєстрі внесено 50706 записів, з яких 17028 за кримінальними правопорушеннями[6].

Інформаційно-аналітичне забезпечення протидії корупційним кримінальним правопорушенням є одним з ключових елементів у діяльності органів сектору безпеки і оборони України. Воно забезпечує своєчасне та ефективне виявлення, аналіз та нейтралізацію корупційних загроз, що мають серйозний вплив на національну безпеку країни. Залучення сучасних інформаційних технологій та створення інтегрованих аналітичних платформ дозволяють оптимізувати процеси моніторингу, виявлення та запобігання корупційним правопорушенням, підвищити прозорість та ефективність діяльності органів безпеки, а також зміцненню довіри громадян до державних структур.

Література

1. п. 16 ч. 1 ст. 1 Закону України «Про національну безпеку України»
2. Офіційний веб-сайт Національного агенства з питань запобігання корупції [Електронний ресурс]. – Режим доступу: https://nazk.gov.ua/uk/indeks-spryynyattya-koruptsii-2023-ukraina-pokraschyla-sviy-pokaznyk-na-3-baly/
3. Коваленко А.В. Інформаційно-аналітичне забезпечення діяльності Національної поліції: теоретичний та практичний підхід. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2018. Спеціальний випуск № 3. С.250-254.
4. Наказ №58/560/795/679/99 від 29.10.2008
5. Офіційний веб-сайт Верховної Ради України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0345-18#Text
6. Офіційний веб-сайт Національного агенства з питань запобігання корупції [Електронний ресурс]. – Режим доступу: https://corruptinfo.nazk.gov.ua/

Петров Юрій Анатолійович

курсант 3-го курсу, ННІПФПКП Львівського державного університету внутрішніх справ

Жуковський Ігор Вячеславович

викладач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ЩОДО ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

З початку повномасштабного вторгнення на території України було вчинено близько 9000 воєнних злочинів суб'єктами яких є російські військові, в основному ці злочини вчинялись стосовно цивільних громадян, наглядний приклад місто Буча, яка здобула свою відомість саме тим, що на території даного міста під час окупації було вчинено злочини стосовно цивільного населення.

Відповідно до статей 25, 26 Закону України «Про Національну поліцію» поліція в межах інформаційно-аналітичної діяльності формує, наповнює, підтримує в актуальному стані та користується реєстрами і базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України (далі – ЄІС МВС) [1],[2].

З метою внесення осіб які причетні до вчинення злочину пов'язані з воєнними злочинами в системі ІПНП було створено ІП-«воєнний злочинець» [4]. Діяльність Департаменту інформаційно- аналітичного забезпечення регулюють наказом Національної поліції України від 31 січня 2020 року № 77 [3]. Отже цілком можна сказати, що інформаційно-аналітичне забезпечення підрозділів Національної поліції України є відповідним на національному рівні до сьогодення. Але в банки даних інформації про осіб які причетні до вчинення воєнних злочинів, а саме в ІП «воєнний злочинець» вноситься відомості тільки про осіб які вчинили категорію даних злочинів тільки на території України, але як ми знаєм, що достатня кількість країни підтримують росію у війні з Україною, тому те, що в ІП «воєнний злочинець» вносяться відомості тільки про осіб які вчиняли злочини на території України, є неповною і навіть не достатньою, щоб розкривати і розслідувати такі злочини. Але в цілому функціонування такого інформаційного порталу, на даний час є необхідним, якщо розглянути кількість злочинів, які розкрили, та виявили осіб які причетні до вчинення воєнних злочинів наприклад, після деокупації міста Бучі було виявлено понад 91 особу яка причетна до вчинення воєнних злочинів, також для подальшого полегшення виявлення осіб, які причетні до вчинення таких злочинів, було внесенні відомості саме в ІП «воєнний злочинець», після чого ідентифікувати та попередити вчинення саме таких злочинів тими і самими особами стає набагато більше шансів ніж до того як виявляли ці злочини.

Отже, як висновок ми можемо сказати, що забезпечення Національної поліції, а точніше підрозділів кримінальної поліції, саме в межах інформаційно- аналітичного забезпечення є певною мірою достатньою і ефективною, в сфері розкриття і виявлення осіб які причетні до воєнних злочинів.

Література

1. Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII із змінами і доп. // Відомості Верховної Ради. 2015. № 40-41. – Ст. 379. – Режим доступу:https://zakon.rada.gov.ua/laws/show/580-19.#Text
2. Григорович О.Б. «Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції та слідчих органів під час документування»
3. Наказ Національної поліції України від 31.01.2020 року року № 77 «Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України». 2020. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Struktura/Polohena11.pdf.
4. Наказ МВС України від 03.08.2017 № 686 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України».2017. URL:https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

Полотай Орест Іванович
доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук, доцент

ДОСВІД ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО НАВЧАННЯ У ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Львівський державний університет безпеки життєдіяльності (ЛДУ БЖД) – провідний український заклад вищої освіти в сфері безпеки людини. Належить він до Державної служби України з надзвичайних ситуацій. Всі учасники навчального процесу поділяються на дві групи: студенти та курсанти.

На жаль, так склалося, що останні пару років процес навчання підпадає під вплив непередбачуваних форс-мажорних обставин. Пандемія COVID-19, війна в країні, проблеми з електропостачанням активізували пошук нових методів та засобів навчання. Виходячи з цього, виникає потреба у змішаній формі навчання, яка би містила в собі елементи дистанційного навчання.

Отже, доцільним є опис досвід використання віртуального навчального середовища ЛДУ БЖД, яке використовується як допоміжний засіб організації змішаного навчання, та включає як традиційну так і дистанційну форми навчання.

Віртуальне навчальне середовище ЛДУ БЖД, має назву Віртуальний університет ЛДУ БЖД (ВУ ЛДУ БЖД) та працює на базі оболонки Moodle [4]. Під час своєї історії, ВУ ЛДУ БЖД мав різний веб-інтерфейс, в залежності від того, яка версія системи Moodle використовувалася на той момент. На даний час, віртуальне середовище працює на останній версії системи Moodle і має наступний вигляд (рис. 1).

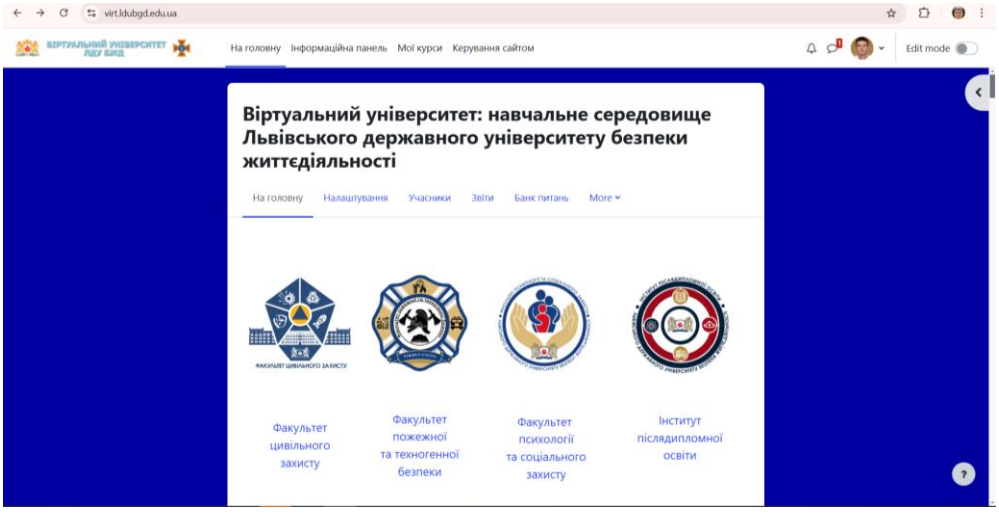

Рис. 1. Головна сторінка навчального середовища ЛДУ БЖД

З метою допомоги у роботі із ВУ ЛДУ БЖД адміністратором середовища, та автором даних тез були опубліковані методичні матеріали, щодо розроблення електронних курсів у віртуальному навчальному середовищі [6] і періодично розміщуються короткі відеоматеріали на головній сторінці навчального середовища [1].

На даний момент часу всі електронні курси ВУ ЛДУ БЖД повинні відповідати заздалегідь узгодженій структурі.

Структура електронного курсу включає такі елементи [5]:

Інструктивний блок:

- Назва електронного курсу;
- Анотація курсу;
- Робоча навчальна програма (силабус);
- Е-посібники та додаткові електронні ресурси;
- Рекомендована література.

Теоретична частина:

- електронний конспект лекцій;
- мультимедійні презентації лекцій;
- за потреби аудіо-, відео-, анімаційні навчальні ресурси;

Практична частина:

- завдання на практичні, лабораторні, самостійні та розрахунково-графічні роботи (в залежності від специфіки курсу), перелік індивідуальних варіантів завдань;
- методичні вказівки для виконання практичних, лабораторних, самостійних чи розрахунково-графічних робіт (в залежності від специфіки курсу);

Контрольна частина:

- виконання практичних, лабораторних, самостійних чи розрахунково-графічних робіт (в залежності від специфіки курсу);
- тестування.

Підсумковий контроль:

- тестування;
- перелік питань на екзамен чи диференційований залік.

В кінці кожного електронного курсу міститься два опитування для здобувачів освіти для оцінювання ними самого електронного курсу.

Останні пару років ВУ ЛДУ БЖД використовується не тільки для допомоги у навчанні здобувачам освіти, але й для здійснення на його базі проходження курсів підвищення кваліфікації працівниками структурних підрозділів ДСНС України за різноманітними освітніми програмами.

Перед початком роботи з ВУ ЛДУ БЖД було організовано процес створення електронних курсів. Для цього було проведено навчання відповідальних працівників кафедри, деканату та за бажанням викладачів на семінарах тренінгах. Було проведено два семінари тренінги, щодо роботи викладачів з технологіями дистанційного навчання.

Але оскільки в університеті з часом оновлюється склад науково-педагогічних працівників, і багато з них або раніше не працювали з системою Moodle, або слабо орієнтуються в новій версії системи, то виникає потреба у повторному проведені навчання по роботі з системою Moodle, який найкраще проводити у змішаному форматі: такі теми, які викликають найбільше труднощів у викладачів, розглянути очно, більше прості теми – в онлайн режимі.

Для цього пропонується оновити раніше розроблені два допоміжні електронні курси, один з яких був зразком для створення нових курсів, інший для онлайн навчання майбутніх викладачів-тьюторів створювати власні електронні курси (рис. 2).

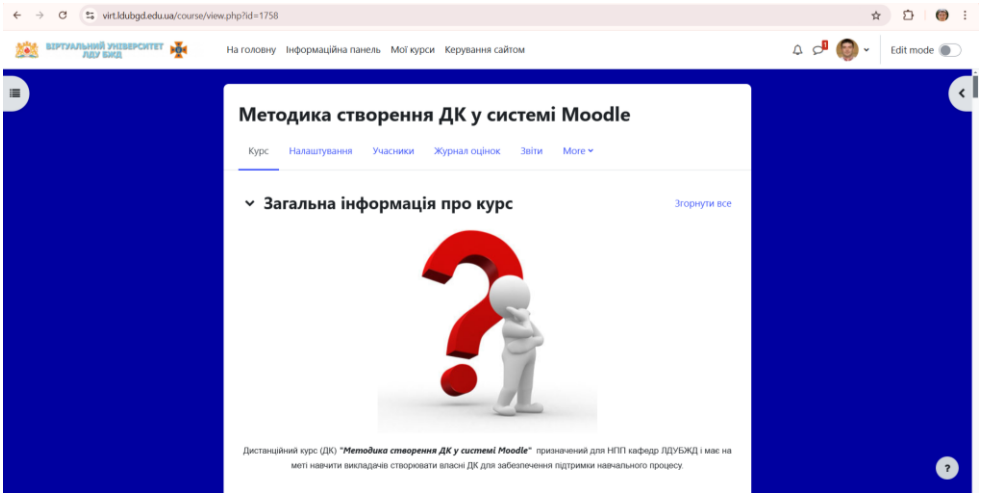

Рис. 2. Електронний курс «Методика створення ДК у системі Moodle»

У рамках цього курсу, всі учасники мають змогу ознайомитися із основними тонкощами та труднощами, з якими вони можуть зіштовхнутися під час розроблення власних електронних курсів, за допомогою викладача-тьютора розібратися зі всіма проблемними питаннями, та використовуючи еталонний електронний курс, який так і називається «Зразок електронного курсу» розробити власні, готові до роботи, електронні курси.

Щодо політики безпеки навчального середовища, то доступ до ВУ ЛДУ БЖД – персоніфікований. Логін та пароль доступу здобувачі освіти отримують у адміністратора сайту на початку навчання. Викладачі, які раніше не були зареєстровані в системі, повинні звернутися (очно або за допомогою електронної пошти) до адміністратора, та зареєструватись на сайті. Обов'язковою умовою реєстрації учасника на сайті є наявність облікового запису внутрішньої електронної пошти ЛДУ БЖД.

На сьогоднішній день, у ВУ ЛДУ БЖД всіх користувачів було розбито на групи: кафедри, технічний персонал та здобувачів (включаючи працівників ДСНС України, які проходять курси підвищення кваліфікації).

Розподіл здобувачів ВУ ЛДУ БЖД по групам дає змогу автоматично зараховувати їх на конкретний курс з вказанням терміну перебування їх в курсі.

В результаті впровадження в освітній процес ЛДУ БЖД віртуального середовища, здобувачі вищої освіти мають змогу самостійно опрацювати теоретичний матеріал та візуально ознайомитись з особливостями та тонкощами таких процесів як пожежогасіння та ін.

Ефективність використання ВУ ЛДУБЖД підтверджена роботою в ньому користувачів під час карантинного періоду, активність яких за цей період зросла в 4 рази [3].

Отже, можна зробити висновок, що ВУ ЛДУБЖД, виступає потужним інструментом для ефективного забезпечення освітнього процесу в сучасних непростих умовах.

Література

1. Віртуальний університет Львівського державного університету безпеки життєдіяльності. URL: https://virt.ldubgd.edu.ua
2. Козяр М.М. Віртуальний університет: перспективи переходу на новий тип освіти / Козяр М.М. // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: ме-тодологія, теорія, досвід, проблеми: зб. наук. праць. − Київ-Вінниця: ТОВ фірма "Планер", 2010. – Вип. 23. − С. 40-46.
3. Меньшикова О.В., Полотай О.І. Використання технологій дистанційного навчання в умовах Covid-19 в ЛДУБЖД. Зб. тез доп. VI Міжнар. наук.-практ. конф. “Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи”. (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 196-203
4. Офіційний сайт розробників системи Moodle. URL: https://moodle.org
5. Полотай О.І. Особливості запровадження змішаного навчання в закладах вищої освіти з особливими умовами навчання. Матеріали міжнар. наук.-практ. конф. “Змішане навчання – інновація XXI сторіччя”. (м. Харків, 29-30 листопада 2018 р.). Харків : НТУ «ХПІ», 2018. С. 79-85
6. Полотай О.І., Кухарська Н.П. Розроблення електронних курсів у віртуальному навчальному середовищі. Львів : СПОЛОМ, 2021. 172 с.

Поляк Святослав Петрович

В.о. завідувача кафедри оперативно-розшукової діяльності

ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ У КРИМІНАЛЬНІЙ РОЗВІДЦІ

В процесі життєдіяльності кожна жива істота намагається вивчити та з’ясувати якомога більше процесів, що відбуваються довкола. Ці процеси протікають як з її участю так і без неї. Однак, з моменту відколи людина як вищий клас цивілізації – біомережа, створила комп’ютерні технології та математичні моделі, які самостійно навчаються на основі отриманих даних – нейромережу, механізм пошуку інформації та її ідентифікація для проактивного пізнання зазнав прогресу, що подекуди не піддається людському усвідомленню.

Натхненні біонейромережею штучні нейромережі стали невід’ємним інструментом правоохоронної діяльності у всьому цивілізованому світі, а особливо в найактивнішому її напрямі – кримінальній розвідці.

Носії сучасних наукових догмат вважають, що кримінальна розвідка виступає однією з функцій оперативно – розшукової діяльності та реалізується шляхом використання системи розвідувальних, пошукових, інформаційно-аналітичних заходів, у т.ч. із застосуванням оперативних та оперативно-технічних засобів, спрямованих на своєчасне запобігання, виявлення і нейтралізацію реальних і потенційних кримінальних загроз суспільній безпеці, захист особи, держави та суспільства від злочинності [1, с. 4].

Виходячи з «природніх» функціональних обов’язків наявних правоохорнних органів в Україні, окремі науковці логічно визначають, що суб’єктами кримінальної розвідки (підрозділами, що здійснюють кримінальну розвідку) є визначені законодавством

України та відомчими нормативними актами оперативні підрозділи системи МВС України, СБ України, Державної прикордонної служби [2, с. 25].

Однак маємо зауважити, що на даний момент поняття самої кримінальної розвідки не визначено на законодавчому рівні, і взагалі, вважається необхідним розробити та прийняти Закон України «Про кримінальну розвідку» як окремий напрям правоохоронної діяльності. В сьогоденні, яке супроводжується масою викликів і загроз інформаційного та технічного характеру, доцільним було б створення за прикладом окремих країн Європейського Союзу підрозділу кримінальної розвідки в структурі наявних органів, або навіть окремого правоохоронного органу, адже коло її функціоналу виходить далеко за межі кримінального аналізу.

До прикладу у поліції багатьох країн створено профільні підрозділи, а методи кримінальної розвідки (англ. – criminal intelligence) набули настільки суттєвого значення у кримінальному аналізі, що фактично перетворили його в розвідку [3, с. 93].

Історично та доктринально такий вид діяльності як кримінальна розвідка зароджувався і випливав з оперативно-розшукової діяльності, адже остання є фундаментальною наукою та практичною діяльністю, що постійно удосконалювалася та шукала найефективніші шляхи збору й аналізу оперативної інформації кримінального характеру.

Вдало підкреслює Федчак І.А., що чим більше інформації збирається, тим більше це допомагає аналізу та у підсумку – прийняттю вірного рішення. Однак це також збільшує подальше навантаження, що, в свою чергу, змушує збільшувати штат аналітиків і їх продуктивність або втрачати ефективність [4, с. 25].

Все це природньо стимулює трансформацію архаїчних підходів до збору й оцінки інформації в правоохоронній діяльності у новітні процеси детекції необхідних даних з інформаційних масивів (інфомаси) та їх вірної ідентифікації з використанням різноманітних інформаційно-аналітичних технологій поряд із людськими можливостями. Все це зумовлює миттєву глобалізацію й технології штучного інтелекту, що застосовується для оптимізації такої діяльності і надання процесу обробки інформації максимальної точності та оперативності.

Виходячи з наведеного, сучасну кримінальну розвідку за аналізом зарубіжних джерел поділяють на стратегічну й оперативну види розвідки та її окремі галузі: людську розвідку (Human Intelligence – HUMINT), розвідку сигналів (Signals Intelligence – SIGINT), розвідку зображень (Imagery Intelligence – IMINT), розвідку сигнатур (Measurement and Signatures Intelligence – MASINT), розвідку з відкритих джерел (Open-Source Intelligence – OSINT) [5, с. 8-9].

Логічним видається, що для проведення зазначених видів розвідки без використання комп’ютерних технологій та штучного інтелекту не обійтися. Програмне забезпечення нейромереж спроможне за долі хвилин знаходити найбільш тотожні дані за заданими параметрами в надвеликих масивах інформації, для пошуку яких звичайній людині-аналітику довелося б працювати досить довго.

Науковці зазначають, що нейронні мережі – це підмножина Machine Learning, мережі із здатністю самостійного навчання. Вони застосовуються не як технологія чи інструмент або засіб, а як систему яка здатність вчитися і використовувати вивчене. Нейронні мережі – влаштовані за образом і подобою людського мозку. Тобто намагаються відтворити окремі аспекти влаштування нейромереж у мозку людини та використовують BigData, DataScience як матеріал, на якому вони навчаються [6, с. 13].

Отже, використання нейронних мереж у кримінальній розвідці відкриває нові горизонти для аналізу складних і неоднозначних даних. Завдяки здатності нейронних мереж навчатися на великих масивах інформації, вони можуть виявляти приховані закономірності, що важко розпізнати за допомогою традиційних методів. Наприклад, такі алгоритми можуть ефективно аналізувати телефонні дзвінки, електронні листи або транзакції, щоб ідентифікувати можливі зв'язки між підозрюваними, навіть якщо ці зв'язки добре замасковані. Також нейронні мережі здатні прогнозувати ймовірність злочинів, оцінюючи ризики на основі історичних даних та поведінкових моделей.

Важливою перевагою нейронних мереж є їхня здатність працювати з неструктурованими даними, такими як відео, аудіо та текстові документи. Це робить їх незамінними для аналізу доказів із камер спостереження, розпізнавання голосу або відтворення подій на основі фрагментів інформації. Водночас використання таких технологій ставить перед суспільством виклики, пов'язані із захистом персональних даних та етичністю застосування. Нейронні мережі можуть помилково ідентифікувати невинних людей або підвищувати ризик упереджених рішень через помилки у вихідних даних. Тому їх ефективне використання потребує ретельного нагляду, прозорості алгоритмів та залучення фахівців, які можуть мінімізувати можливі ризики.

Література

1. Албул С.В. Кримінальна розвідка як функція оперативно-розшукової діяльності: європейський досвід та українські перспективи (Criminal Intelligence as a Function of Operatively-Search Activity: European Experience and Ukrainian Prospects). European Reforms Bulletin: international scientific peer-reviewed journal: Grand Duchy of Luxembourg. 2015. № 2. P. 2–6.
2. Семенюк, О. (2024). Місце й функції кримінальної розвідки у системі забезпечення національної безпеки україни. Наукові праці міжрегіональної академії управління персоналом. Юридичні науки, (2 (70)), 23-27.
3. Степанюк, Р. Л. (2024). Розвідка у криміналістиці й оперативно-розшуковій діяльності. Вісник Луганського навчально-наукового інституту імені ЕО Дідоренка, 1(2), 191-203.
4. Федчак, І. А. (2020). Виникнення розвідувальної (кримінальної) аналітики. РЕДАКЦІЙНА КОЛЕГІЯ, 23.
5. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підруч-ник. Одеса : Видавництво «Юридика», 2024. 180 с.
6. Федоренко О. А., Стрільців О. М., Тарасенко О. С. Використання технологій штучного інтелекту у правоохоронній діяльності : аналіт. огляд. Київ : Нац. акад. внутр. справ, 2022. 105 с.

Пядишев Володимир Георгійович

професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, доктор юридичних наук, професор

ЗАСТОСУВАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ: ЗАРУБІЖНИЙ ДОСВІД

Правоохоронні органи стикаються зі складним завданням: керувати постійно зростаючою горою цифрових доказів і даних кримінальних розслідувань. Величезний

обсяг цих даних вимагає сучасного рішення. Загрози та інциденти розвиваються швидко, і правоохоронні органи повинні не тільки встигати, але й передбачати нові загрози та протидіяти їм. Платформа, яка використовує потужність генеративного штучного інтелекту може стати ключем до відкриття нової ери ефективності правоохоронних органів. Генеративний штучний інтелект може аналізувати величезну кількість даних від відеоканалів до цифрових доказів, а також визначати тенденції та моделі поведінки набагато швидше, ніж люди [1].

Намагаючись оцінити переваги генеративного штучного інтелекту, слід, по-перше, усвідомити різницю між звичайним штучним інтелектом та генеративним штучним інтелектом.

Якщо **штучний інтелект (ШІ)** – це здатність апаратно-програмного комплексу виконувати завдання, що вимагають участі людського інтелекту, починаючи від розпізнавання – до міркування, навчання або прийняття рішень. У свою чергу **генеративний штучний інтелект (ГШІ)** – це підмножина штучного інтелекту, за допомогою якої на підставі вивчення наявних даних, тобто на підставі завдання та прикладів, продукуються нові дані, зокрема, текст, зображення тощо. ШІ та ГШІ інтелект вже сьогодні мають низку застосувань у діяльності правоохоронних органів [2].. Причому вони мають різні можливості, що можна побачити з таблиці 1.

Таблиця 1. Можливості штучного інтелекту та генеративного штучного інтелекту залежно від завдань

Завдання	**Можливості**	
	Ш І	Г Ш І
Розпізнавання облич	може допомогти ідентифікувати підозрюваних, жертв або зниклих безвісти шляхом порівняння їхніх облич із базами даних зображень, як-от фотографій, водійських прав або профілів у соціальних мережах.	може допомогти створити реалістичні композиції облич на основі описів чи ескізів свідків або покращити зображення чи відео низької якості для покращення ідентифікації
Розпізнавання та переклад мовлення	може допомогти транскрибувати та перекладати мовлення в режимі реального часу, дозволяючи офіцерам спілкуватися з людьми, які говорять різними мовами, або створювати точні та своєчасні звіти на основі записів голосу	може допомогти синтезувати мову та створити реалістичні зразки голосу для різних цілей, таких як голосова біометрія, клонування голосу або голосовий фішинг
Виявлення та розпізнавання об’єктів	може допомогти виявляти та розпізнавати об’єкти на зображеннях або відео, наприклад зброю, транспортні засоби, номерні знаки чи докази. Це може допомогти поліцейським знаходити та відстежувати підозрюваних, транспортні засоби чи цікаві предмети та автоматизувати процес збору доказів і документування	може допомогти створити реалістичні зображення або відео об’єктів на основі описів або маніпулювати чи покращувати існуючі зображення чи відео для покращення виявлення та розпізнавання

Аналіз поведінки та прогнозування	може допомогти аналізувати та прогнозувати поведінку людини на основі різних факторів, таких як вираз обличчя, мова тіла, мовлення та біометричні дані. Це може допомогти офіцерам оцінити рівень ризику ситуації або передбачити дії чи наміри особи	може допомогти створити реалістичні симуляції або сценарії на основі моделей поведінки та генерувати синтетичні дані для навчання та тестування
Підтримка прийняття рішень та оптимізація	може допомогти надавати офіцерам відповідну інформацію, пропозиції та рекомендації на основі різних джерел даних, таких як бази даних, датчики та соціальні мережі. Це може допомогти офіцерам приймати обґрунтовані та своєчасні рішення та оптимізувати свої дії чи стратегії	може допомогти створити альтернативні рішення та результати на основі різних критеріїв або обмежень і оцінити ефективність або вплив різних рішень і дій

У поєднанні з великими мовними моделями (LLM) ГШІ може допомагати швидко і легко знаходити інформаційні елементи, а також вказувати зв'язки між ними. Такий «цифровий помічник» може генерувати короткі резюме, висвітлювати важливі деталі, знаходити прогалини та протиріччя у ході розслідування, а також пропонувати наступні завдання [3].

Перейдем до прикладів конкретного обладнання. Яскравим прикладом технолгії ГШІ є інструмент Co-Analyst від PenLink [4]. Його розроблено для оптимізації розслідувань і підвищення ефективності правоохоронних органів, через надання глибокої інформації та оперативної розвідки. В ньому застосовуються інструменти для геолокації, аналізу історії веб-перегляду, пошуку в корпоративному реєстрі тощо. Інструмент допомагає розпізнавати та інтерпретувати унікальний сленг або кодові слова, які використовуються у в'язничних листах або телефонних дзвінках, надаючи важливу інформацію про приналежність до банди та її діяльність. Досліджуючи, наприклад, прекурсори фентанілу, інструмент може не лише ідентифікувати відомі прекурсори, але й розширити пошук, щоб виявити нові, аналізуючи інформацію з різних джерел у мережі. При розслідуванні торгівлі людьми інструмент може аналізувати зображення та текст з різних джерел, виявляючи зв'язки та спільні риси, що неможливо вручну.

Цікаво розглянути приклади інструментів із застосуванням ГШІ, що використовуються в Індії. Тут застосування ГШІ бачать у таких напрямках [5].

Покращення прогнозування та попередження злочинності. Для цього використовується можливість ГШІ аналізувати величезні обсяги даних із різноманітних джерел, включаючи записи про злочини, соціальні мережі та записи з камер спостереження, а також виявляти аномалії та закономірності в цих даних.

Удосконалення криміналістики та процесу розслідування. ГШІ автоматизує розпізнавання облич, аналіз інших зображень та відео, а також судово-медичний аналіз, реконструюючи місце злочину, підвищуючи ефективність збирання доказів.

Зниження рівня упередженості та підвищення рівня звітності. Упередженість у прийнятті рішень поліцією може негативно вплинути на громаду. ГШІ надає об'єктивну, побудовану на історичних та інших даних інформацію про діяльність правоохоронних органів. Аналіз цієї інформації та виявлення моделі упередженості допоможе правоохоронним органам сприяти чесності в діяльності та підвищити підзвітність.

Турбота про забезпечення конфіденційності та підтримку етичних стандартів. Застосування ГШІ у правоохоронних органах забезпечує численні переваги, але воно також обумовлює важливі міркування стосовно етики та конфіденційності. Важливо переконатися, що при застосуванні ГШІ у правоохоронних органах підтримується повага до прав і свобод людини. Ця турбота проявляться у впровадженні заходів надійного захисту даних, забезпеченні прозорості алгоритмів прийняття рішень та у протидії зловживанням технологіями спостереження на основі ГШІ.

Відповідно у правоохоронних органах Індії застосовується певна кількість інструментів на базі ГШІ [6]. Вони описані у таблиці 2.

Таблиця 2. Інструменти з ГШІ у правоохоронних органах Індії.

Назва	Призначення	Сутність роботи
Palantir Gotham:	допомога в кримінальних розслідуваннях і розвідувальних операціях	інтеграція, аналіз та візуалізація даних
PredPol	ефективніший розподіл ресурсів	інтелектуальний контроль, прогнозування територій із більшою ймовірністю злочинів
Veritone	допомога у розслідуваннях та судових розглядах	автоматизація аналізу аудіо- та відеодоказів
Rekognition	ідентифікації людей на зображеннях і відео	технологія розпізнавання обличчя
Urbint	допомога у забезпеченні громадської безпеки	виявлення потенційних проблем з безпекою в інфраструктурах громад

Багато правоохоронних органів впроваджують ГШІ повільно з різних причин, зокрема, через обмежене розуміння переваг ГШІ, бюджетні обмеження, проблеми етики та конфіденційності, нормативні та правові проблеми, а також проблеми інтеграції технологій. Однак слід пам'ятати, що представники організаційної злочинності ретельно впроваджують нові технології, не шкодуючи коштів. А правоохоронні органи не мають права програвати в гонці технологій.

Література

1. How Generative AI Can Help Law Enforcement Keep Communities Safe. Penlink. May 3, 2024. Site. URL : https://www.penlink.com/blog/blog-how-generative-ai-can-help-law-enforcement/ (дата звернення: 14.11.2024).
2. Lukens, Ph. The future of policing: How AI is transforming police operations and digital evidence management. Police1. September 02, 2024. Site. URL : https://www.police1.com/police-products/intelligence-led-policing/the-future-of-policing-how-ai-is-transforming-police-operations-and-digital-evidence-management#:~:text=AI%20is%20a%20rapidly%20evolving,improving%20data%20security%20and%20privacy. (дата звернення: 14.11.2024).
3. Joyner-Roberson, E. 3 ways generative AI can assist in criminal investigations. CFE May 21, 2024. Site. URL : https://blogs.sas.com/content/sascom/2024/05/21/3-ways-that-generative-ai-can-be-effective-in-criminal-investigations/ (дата звернення: 14.11.2024).

4. The Role of Generative AI in Law Enforcement: Insights from PenLink's Co-Analyst Tool. Penlink. Site. URL : https://www.penlink.com/blog/role-of-generative-ai-in-law-enforcement/ (дата звернення: 14.11.2024).
5. Kamath, N. Unlocking the Future: The Application of Generative AI in Law Enforcement in India. Linkedin. 7 March 2024. Site. URL : https://www.linkedin.com/pulse/unlocking-future-application-generative-ai-law-india-nithin-kamath-esryc (дата звернення: 14.11.2024).
6. Mohindroo, S.K. Harnessing Generative AI in Law Enforcement: A Vision for Smarter, Safer Communities. Linkedin.08 November 2023. Site. URL : https://www.linkedin.com/pulse/harnessing-generative-ai-law-enforcement-vision-safer-mohindroo--xwsxf (дата звернення: 14.11.2024).

Синиціна Юлія Петрівна

доцент кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ ДЛЯ ДЕРЖАВНИХ І КОМЕРЦІЙНИХ УСТАНОВ

Стрімкий розвиток інформаційно-аналітичної діяльності (ІАД) у державному та комерційному секторах України є однією з ключових тенденцій сучасності. Цей процес зумовлений низкою об'єктивних чинників: демократизацією суспільства, розвитком ринкових відносин, легітимністю управлінських процесів, а також активізацією підприємницької діяльності. З іншого боку, зростає значення інтелектуального аналізу під час ухвалення управлінських рішень, що обумовлено зростаючим потоком інформації, необхідної для ефективного управління.

Розвиток ІАД у державних і комерційних установах сприяє постійному вдосконаленню механізмів інформаційної безпеки, яка, своєю чергою, тісно пов'язана з питаннями економічної безпеки. Сучасні виклики інформаційної безпеки вимагають інтеграції новітніх інформаційних технологій, зокрема тих, що базуються на штучному інтелекті. Інструменти штучного інтелекту дозволяють виявляти та прогнозувати інформаційні та економічні загрози, забезпечуючи тим самим надійний захист.

Сучасні розробки у сфері штучного інтелекту (AI), даталогії (Data Science) та машинного навчання (Machine Learning) відкривають нові можливості: розпізнавання зображень і мови, ідентифікація особистості, прогнозування поведінки, автокерування транспортними засобами тощо. Водночас цифровізація стала невід'ємною складовою нашого життя, а індекс цифрової готовності (NRI), запроваджений у 2001 році, відображає рівень розвитку інформаційно-комунікаційних технологій країни, слугуючи показником її інвестиційної привабливості.

Актуальність теми інтеграції штучного інтелекту (ШІ) в системи інформаційної безпеки визначається стрімким зростанням кіберзагроз, які стають все складнішими та більш руйнівними. У державних і комерційних установах значні обсяги критичної інформації щодня піддаються ризику компрометації, що вимагає ефективних інструментів для її захисту. ШІ здатний забезпечити проактивний моніторинг загроз, автоматизоване

виявлення аномалій та адаптивне реагування, що значно підвищує ефективність традиційних систем безпеки.

Проте впровадження ШІ супроводжується численними викликами, зокрема, пов’язаними з етичними аспектами, конфіденційністю даних, ризиками неправильних рішень, а також значними ресурсами для навчання алгоритмів. Особливо це актуально в умовах України, де кіберзахист є ключовим елементом національної безпеки. Тема є критично важливою для розробки стратегій захисту інформаційних систем, адаптованих до сучасних умов глобалізованого цифрового середовища.

Значний внесок у дослідження правових аспектів застосування штучного інтелекту зробили О.А. Баранов, В.М. Брижко, К.С. Мельник, В.Г. Пилипчук та інші науковці. Питанням ролі та місця штучного інтелекту в кримінально-правових відносинах присвячені роботи В.А. Мисливого, М.В. Карчевського та Н.А. Савінової. Однак кожен новий крок у наукових дослідженнях відкриває ще ширші перспективи для подальшого вивчення та пізнання реальності.

У роботах [1, 2] розглянуто використання нейронних мереж у складі інтелектуальної системи підтримки прийняття рішень на підприємстві. На основі проведених досліджень було розроблено модель аналізу та вивчено практичні аспекти застосування нейронних мереж у маркетинговій інформаційній системі підприємства. Основна мета — вдосконалення інформаційної системи підприємства шляхом впровадження інтелектуальної системи підтримки прийняття рішень (IDSS) на базі нейронних мереж [1, 2].

На сьогодні основою більшості існуючих систем підтримки прийняття рішень (DSS) є методи штучного інтелекту. Створення інтелектуальних DSS стало логічним розвитком традиційних систем цього типу. Інтелектуальні DSS забезпечують ефективну інформаційну підтримку як виробничих процесів, так і процесів безпеки, що є актуальним для державних і комерційних організацій.

Загальні аспекти застосування інтелектуальних систем у правоохоронній діяльності були розглянуті в роботах [3, 7]. Зокрема, правоохоронні органи використовують програмні комплекси для автоматичного розпізнавання облич із порівнянням даних систем відеоспостереження з інформацією, наявною в базах даних. Також ці системи застосовуються для фіксації порушень правил дорожнього руху за допомогою спеціалізованих автоматизованих комплексів. Ці технічні засоби оснащені функціями фото- та відеозапису, що дає змогу в автоматичному режимі виявляти та документувати правопорушення, зберігаючи відповідні дані у базах.

У роботі [4] запропоновано Концепцію моделювання поведінки взаємодіючих агентів, яка базується на трирівневій структурі моделювання суб'єктів і бізнес-процесів у рамках функціонування організації та системи безпеки. Основою цієї концепції є моделювання поведінки антагоністичних агентів. Запропонована методологія дозволяє оцінювати та підвищувати рівень безпеки, зокрема, зменшуючи кількість реалізації гібридних загроз у 1,76 раза, що сприяє зниженню матеріальних збитків у 1,65 раза. Крім того, вона скорочує час на ідентифікацію загроз в онлайн-режимі на 38%, що дає змогу ефективніше обирати засоби протидії.

У підсумку варто зазначити, що тема використання штучного інтелекту для захисту інформаційних систем набирає обертів, і актуальність багатьох напрямків у цій сфері продовжуватиме зростати найближчим часом. Перехід великої кількості людей на віддалений режим роботи через пандемію та військові дії в Україні значно вплинув

на розвиток підходів до забезпечення інформаційної безпеки. Організації змушені адаптувати свої процеси, впроваджувати нові технології для ідентифікації «свій-чужий» і розробляти стратегії захисту в умовах зростаючих ризиків.

Навантаження на підрозділи інформаційної безпеки державних і комерційних установ поступово зростає, що робить використання інструментів на основі штучного інтелекту критично необхідним. Ризики, пов'язані з «розмитим периметром» захисту, значно підвищуються. Серед сучасних трендів у сфері інформаційної безпеки, що активно використовують штучний інтелект, можна виділити EDR/XDR-рішення для кінцевих пристроїв, UEBA, SGRC-продукти, Honey Tokens та інші інструменти класу Deception, IRP (Incident Response), TI/TH-платформи тощо. Важливо підходити до впровадження цих рішень усвідомлено, враховуючи специфіку конкретних задач та умов.

Література

1. Synytsina Y., Abramov S., Manole A. Improving the information system of the enterprise through the use of neural networks. 2022. Vol. 2, № 15. P. 127 – 138. URL: https://er.dduvs.edu.ua/handle/123456789/10350 (дата звернення: 06.12. 2024).
2. Synytsina, Yu, O. Kaut, and T. Fonareva. Intelligent decision support systems in the enterprise management process. Infrastruktura rynku 32 (2019): 208-212.
3. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка в правоохоронній діяльності: навч. посібник. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с. URL: http://85.198.129.37/handle/123456789/8735 (дата звернення: 05.12.2024).
4. Milov, Oleksandr, et al. "Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system." Eastern-European Journal of Enterprise Technologies 6.2 (2020): 108. URL: https://journals.uran.ua/eejet/article/view/218660 (дата звернення: 12.12.20242).

Станкевич Тетяна Володимирівна

курсант 3-го курсу, факультету №2 Львівського державного університету внутрішніх справ

Жуковський Ігор Вячеславович

викладач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ГОЛОСОВОЇ БІОМЕТРІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У сучасних умовах динамічного розвитку інформаційних технологій та зростання загроз у сфері безпеки й оборони впровадження інноваційних рішень стає ключовим завданням для забезпечення ефективності діяльності відповідних органів. Однією з таких технологій є голосова біометрія. Ідентифікація за голосом відома досить давно, людина за відсутності будь-яких технічних засобів ідентифікувала іншу людину за трьома можливими ознаками – голосом, підписом та зовнішністю. Отже голосова ідентифікація – це один із найстаріших методів біометричної ідентифікації. Кожна людина має свій унікальний голос, який відрізняється від усіх інших певними ознаками [1].

Та, не зважаючи на давнє походження цього методу, розпізнавання осіб за особливостями голосу не користується широкою популярністю серед систем інформаційно-аналітичного забезпечення. Основними причинами цього є технічні обмеження попередніх поколінь технологій, недостатня точність розпізнавання в умовах шумового середовища, а також обмежений доступ до високоякісного обладнання та алгоритмів штучного інтелекту.

Перспективи використання голосової біометрії в інформаційно-аналітичному забезпеченні діяльності органів сектору безпеки і оборони України є багатообіцяючими, з огляду на потребу в удосконаленні методів ідентифікації та моніторингу. Голосова біометрія дозволяє забезпечити високий рівень безпеки, доповнюючи традиційні методи автентифікації, такі як паролі чи картки. Це важливо для контролю доступу до конфіденційної інформації та об'єктів.

Також голосова біометрія може бути ефективно використана для моніторингу та аналізу комунікацій, допомагаючи в оперативно-розшуковій діяльності та визначенні достовірності інформації через аналіз голосу. Вона дозволяє автоматизувати процеси збору та обробки даних, що покращує швидкість реагування на загрози та прийняття рішень.

Найбільш актуальною для співпраці зі сферою оперативно-розшукової діяльності є SMIDDLE VOICE ID, продукт SMIDDLE — української міжнародної компанії, яка спеціалізується на розробці програмного забезпечення. Ця технологія голосової біометрії має широкий спектр застосування у тому числі для діяльності правоохоронних органів завдяки своїм унікальним функціям та перевагам. Основними перевагами цієї програми є висока точність розпізнавання та надійна захищеність зібраних даних, що в поєднанні з легкістю інтеграції презентувало SMIDDLE VOICE ID на голову вище за попередників [2].

Попри значні переваги, впровадження цієї технології потребує розвитку нормативно-правової бази, захисту даних від кібератак і вдосконалення технічних систем для розпізнавання голосу в складних умовах. Однак, за умови правильного впровадження, голосова біометрія може стати важливим інструментом для зміцнення національної безпеки.

Література

1. К. В. Нікулін х. В. Л. Голосова ідентифікація диктора як один із сучасних біометричних методів ідентифікації особи. Теорія та практика судової експертизи і криміналістики. 2019. № 19. С. 244.
2. Голосова біометрія | smiddle voice id. Call center software – program solutions for contact center system, pricing | smiddle. Url: https://smiddle.com/uk/solutions/rishennia-dlia-kontakt-tsentru/smiddle-voice-id.

Стах Андріана Євгенівна

курсант 3-го курсу, факультету №2 Львівського державного університету внутрішніх справ

Жуковський Ігор Вячеславович

викладач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЯ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Тема "використання біометричної ідентифікації в інформаційно-аналітичному забезпеченні оперативно-розшукової діяльності" є надзвичайно актуальною, особливо в умовах стрімкого розвитку технологій і зростання рівня загроз. Інтеграція біометричних даних у аналітичні системи дозволяє правоохоронним органам підвищити ефективність пошуку та ідентифікації осіб, залучених до злочинної діяльності, а також зменшити ризики помилок. Біометрична ідентифікація забезпечує швидкий доступ до даних, точність порівняння інформації та значно спрощує взаємодію між різними службами в процесі розслідування. У поєднанні з аналітичними платформами вона сприяє побудові прогнозів і виявленню злочинних мереж, що є важливим для забезпечення правопорядку й безпеки.

Інформаційно-аналітична робота в ОРД – це передбачена законодавством України й урегульована відомчими нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, зокрема й обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави. Основними засобами інформаційно-аналітичної роботи в ОРД є: оперативна техніка та спеціальні технічні засоби, призначені для гласного та негласного отримання інформації; відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи тощо) і різні технічні пристрої, за допомогою яких здійснюється обробка, систематизація та аналіз оперативно-розшукових та інших відомостей фактографічного і криміналістичного характеру [1, с. 38-39].

Таким чином, інформаційно-аналітична робота в ОРД забезпечує збір, обробку та аналіз даних для ефективного виконання завдань, зокрема із використанням сучасних технологій. Біометрична ідентифікація, як складова цього процесу, дозволяє оперативно ідентифікувати осіб на основі унікальних даних (відбитки пальців, розпізнавання облич, ДНК). Інтеграція біометричних технологій у автоматизовані інформаційно-пошукові та аналітичні системи сприяє точності, швидкості розшукової роботи та підвищенню рівня безпеки громадян, суспільства і держави.

Департамент інформаційно-аналітичного забезпечення МВС Україні формує оперативно-довідкові обліки, автоматизовані інформаційно-пошукові системи й банки даних. На сьогодні в оперативно-службовій діяльності успішно використовується інтегрований банк даних регіонального рівня (ІБДР), причому практичні працівники відзначають зручність обміну загальнодоступною інформацією. Обмін інформацією між різними підрозділами Міністерства базується на використанні програмного комплексу

«Діоніс». За твердженням багатьох фахівців, він відстає від сучасних вимог і має численні недоліки (низька швидкість передачі даних, невідповідність вимогам інформаційної безпеки, відсутність продуманого інтерфейсу користувача та ін.). Ефективним засобом інформаційного забезпечення оперативно-розшукової роботи розглядається Єдина інформаційно-телекомунікаційна система, яка ще до 2010 р. повинна була охопити всі підрозділи Національної поліції України. Завданнями були автономізація збору, зберігання й обробки інформації, організація віддаленого доступу співробітників усіх правоохоронних служб до інформаційних ресурсів системи, організація взаємодії з інформаційними системами всіх правоохоронних і державних органів України, а також з Інтерполом [2, с.171].

У рамках інформаційно-аналітичного забезпечення оперативно-розшукової діяльності біометрична ідентифікація, зокрема дактилоскопія, відіграє важливу роль.

В автоматизованих системах дактилоскопічної реєстрації спочатку отримують дактилокарту, яка далі перетворюється в цифровий графічний файл. Далі система в автоматичному режимі аналізує й розпізнає ідентифікаційні ознаки будови папілярних ліній. У результаті на екрані комп'ютера відображається дактилокарта з розпізнаними ознаками. Далі оператор має можливість відкоригувати розміщення ідентифікаційної ознаки на графічному зображенні, якщо відбулася помилка розпізнавання. Після підтвердження оператором правильності дій програма зберігає біометричний зразок [3, с. 298].

Автоматизовані системи ідентифікації за відбитками пальців (АДІС), які використовуються при реєстрації кримінальних правопорушень, широко використовуються вже давно. У Харкові в 2002 р. введено в експлуатацію АДІС «Дакто-2000» [4, с.142]. Інтеграція АДІС у розслідування кримінальних правопорушень дозволяє правоохоронним органам оперативно отримувати точні біометричні дані, перевіряти їх у базах даних і знаходити збіги. Це значно підвищує ефективність виявлення правопорушників та зменшує час на ідентифікацію, роблячи ОРД більш продуктивною та технологічно просунутою.

Отже, інтеграція біометричних технологій у інформаційно-аналітичне забезпечення оперативно-розшукової діяльності висвітлює важливість. Основною перевагою біометричної ідентифікації є її здатність забезпечувати точну і швидку ідентифікацію осіб, що значно підвищує ефективність виконання завдань ОРД.

Інтеграція автоматизованих систем ідентифікації за відбитками пальців (АДІС), таких як «Дакто-2000», дозволяє не лише зменшити час ідентифікації, а й розширити можливості аналітичних платформ, які обробляють оперативно-розшукову інформацію. Завдяки поєднанню АДІС із сучасними аналітичними системами, правоохоронні органи отримують доступ до інтерактивних інструментів аналізу злочинних зв'язків, виявлення тенденцій у кримінальній діяльності та формування прогнозів щодо можливих загроз.

Окрім дактилоскопії, важливе місце в сучасних біометричних технологіях посідають системи розпізнавання облич і голосу, а також аналіз ДНК. Наприклад, розпізнавання облич може бути інтегроване в системи відеоспостереження, що дозволяє в реальному часі ідентифікувати осіб, причетних до злочинів, або розшукуваних правоохоронними органами.

Таким чином, впровадження біометричних технологій в ОРД не лише оптимізує процес ідентифікації осіб, але й розширює можливості інформаційно-аналітичного забезпечення, роблячи його більш адаптивним до сучасних викликів безпеки.

Література

1. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції. Львів, 2017.
2. Дроботов С. А., Албул С.В. Основи оперативно-розшукової діяльності. Київ, 2022.
3. Негребецький В. Біометричні технології в криміналістиці: функції та можливості використання, 2021.
4. Удовиченко О.А. Функціонування регіонального дактилоскопічного обліку в НДКЦ в Харківській області. Криміналістичний вісник, 2010.

Стах Андріана Євгенівна

курсант 3-го курсу, факультету №2 Львівського державного університету внутрішніх справ

Жуковський Ігор Вячеславович

викладач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЯ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Тема "використання біометричної ідентифікації в інформаційно-аналітичному забезпеченні оперативно-розшукової діяльності" є надзвичайно актуальною, особливо в умовах стрімкого розвитку технологій і зростання рівня загроз. Інтеграція біометричних даних у аналітичні системи дозволяє правоохоронним органам підвищити ефективність пошуку та ідентифікації осіб, залучених до злочинної діяльності, а також зменшити ризики помилок. Біометрична ідентифікація забезпечує швидкий доступ до даних, точність порівняння інформації та значно спрощує взаємодію між різними службами в процесі розслідування. У поєднанні з аналітичними платформами вона сприяє побудові прогнозів і виявленню злочинних мереж, що є важливим для забезпечення правопорядку й безпеки.

Інформаційно-аналітична робота в ОРД – це передбачена законодавством України й урегульована відомчими нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, зокрема й обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави. Основними засобами інформаційно-аналітичної роботи в ОРД є: оперативна техніка та спеціальні технічні засоби, призначені для гласного та негласного отримання інформації; відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи тощо) і різні технічні пристрої, за допомогою яких здійснюється обробка, систематизація та аналіз оперативно-розшукових та інших відомостей фактографічного і криміналістичного характеру [1, с. 38-39].

Таким чином, інформаційно-аналітична робота в ОРД забезпечує збір, обробку та аналіз даних для ефективного виконання завдань, зокрема із використанням сучасних технологій. Біометрична ідентифікація, як складова цього процесу, дозволяє

оперативно ідентифікувати осіб на основі унікальних даних (відбитки пальців, розпізнавання облич, ДНК). Інтеграція біометричних технологій у автоматизовані інформаційно-пошукові та аналітичні системи сприяє точності, швидкості розшукової роботи та підвищенню рівня безпеки громадян, суспільства і держави.

Департамент інформаційно-аналітичного забезпечення МВС Україні формує оперативно-довідкові обліки, автоматизовані інформаційно-пошукові системи й банки даних. На сьогодні в оперативно-службовій діяльності успішно використовується інтегрований банк даних регіонального рівня (ІБДР), причому практичні працівники відзначають зручність обміну загальнодоступною інформацією. Обмін інформацією між різними підрозділами Міністерства базується на використанні програмного комплексу «Діоніс». За твердженням багатьох фахівців, він відстає від сучасних вимог і має численні недоліки (низька швидкість передачі даних, невідповідність вимогам інформаційної безпеки, відсутність продуманого інтерфейсу користувача та ін.). Ефективним засобом інформаційного забезпечення оперативно-розшукової роботи розглядається Єдина інформаційно-телекомунікаційна система, яка ще до 2010 р. повинна була охопити всі підрозділи Національної поліції України. Завданнями були автономізація збору, зберігання й обробки інформації, організація віддаленого доступу співробітників усіх правоохоронних служб до інформаційних ресурсів системи, організація взаємодії з інформаційними системами всіх правоохоронних і державних органів України, а також з Інтерполом [2, с.171].

У рамках інформаційно-аналітичного забезпечення оперативно-розшукової діяльності біометрична ідентифікація, зокрема дактилоскопія, відіграє важливу роль.

В автоматизованих системах дактилоскопічної реєстрації спочатку отримують дактилокарту, яка далі перетворюється в цифровий графічний файл. Далі система в автоматичному режимі аналізує й розпізнає ідентифікаційні ознаки будови папілярних ліній. У результаті на екрані комп'ютера відображається дактилокарта з розпізнаними ознаками. Далі оператор має можливість відкоригувати розміщення ідентифікаційної ознаки на графічному зображенні, якщо відбулася помилка розпізнавання. Після підтвердження оператором правильності дій програма зберігає біометричний зразок [3, с. 298].

Автоматизовані системи ідентифікації за відбитками пальців (АДІС), які використовуються при реєстрації кримінальних правопорушень, широко використовуються вже давно. У Харкові в 2002 р. введено в експлуатацію АДІС «Дакто-2000» [4, с.142]. Інтеграція АДІС у розслідування кримінальних правопорушень дозволяє правоохоронним органам оперативно отримувати точні біометричні дані, перевіряти їх у базах даних і знаходити збіги. Це значно підвищує ефективність виявлення правопорушників та зменшує час на ідентифікацію, роблячи ОРД більш продуктивною та технологічно просунутою.

Отже, інтеграція біометричних технологій у інформаційно-аналітичне забезпечення оперативно-розшукової діяльності висвітлює важливість. Основною перевагою біометричної ідентифікації є її здатність забезпечувати точну і швидку ідентифікацію осіб, що значно підвищує ефективність виконання завдань ОРД.

Інтеграція автоматизованих систем ідентифікації за відбитками пальців (АДІС), таких як «Дакто-2000», дозволяє не лише зменшити час ідентифікації, а й розширити можливості аналітичних платформ, які обробляють оперативно-розшукову інформацію. Завдяки поєднанню АДІС із сучасними аналітичними системами, правоохоронні органи

отримують доступ до інтерактивних інструментів аналізу злочинних зв'язків, виявлення тенденцій у кримінальній діяльності та формування прогнозів щодо можливих загроз.

Окрім дактилоскопії, важливе місце в сучасних біометричних технологіях посідають системи розпізнавання облич і голосу, а також аналіз ДНК. Наприклад, розпізнавання облич може бути інтегроване в системи відеоспостереження, що дозволяє в реальному часі ідентифікувати осіб, причетних до злочинів, або розшукуваних правоохоронними органами.

Таким чином, впровадження біометричних технологій в ОРД не лише оптимізує процес ідентифікації осіб, але й розширює можливості інформаційно-аналітичного забезпечення, роблячи його більш адаптивним до сучасних викликів безпеки.

Література

1. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції. Львів, 2017.
2. Дроботов С. А., Албул С.В. Основи оперативно-розшукової діяльності. Київ, 2022.
3. Негребецький В. Біометричні технології в криміналістиці: функції та можливості використання, 2021.
4. Удовиченко О.А. Функціонування регіонального дактилоскопічного обліку в НДКЦ в Харківській області. Криміналістичний вісник, 2010.

Ткачук Ростислав Львович

начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Івануса Андрій Іванович

доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ У ВЕБ-СИСТЕМАХ

Анотація. У роботі аналізуються можливі загрози комп'ютерним мережам та шляхи їх захисту за допомогою технологій VPN. Наведено типові загрози комп'ютерним мережам, проведено аналіз особливостей методів і технологій захисту. Результати аналізу можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами до захисту інформації.

Ключові слова: безпека, інформація, атаки, захист, тунелювання, протоколи, веб-ресурси, VPN.

Вступ. Захист веб-ресурсів залишається одним із важливих напрямків інформаційної безпеки. З кожним роком кількість веб-ресурсів збільшується, а також збільшується кількість конфіденційної інформації, яка локалізується на серверах віддаленого доступу (особливо з використанням хмарних технологій). Багато служб використовують API для зв'язку, і більшість вибирає зв'язок на основі REST. REST API — це архітектурний стиль програмного забезпечення, який описує єдиний інтерфейс між фізично розділеними компонентами [1].

Як наслідок, зростає не лише кількість атак на веб-ресурси, а й економічні наслідки таких атак. Останнім часом уразливість веб-ресурсів під атаками стала небезпечною з політичної сторони як через поширення гібридних війн у світі, так і через зростання терористичних загроз.

Аналіз проблеми. Для того, щоб якісно проаналізувати методи захисту веб-систем, перш за все необхідно розібратися в існуючих загрозах, які є актуальними зараз. Дослідження принципів атак допоможе краще вникнути в тему і провести більш ретельний аналіз методів захисту, оцінити переваги і недоліки кожного з них.

Таким чином, удосконалення методів і систем захисту веб-ресурсів від атак залишається актуальною науковою проблемою, особливо враховуючи постійне вдосконалення методів і засобів атак. Удосконалення методів захисту веб-ресурсів від атак також є актуальним завданням практичного застосування через зростання економічних, соціальних і політичних наслідків зловмисних дій.

Згідно з дослідженням OWASP, існує 10 найбільш критичних ризиків для безпеки веб-додатків:

1) Порушений контроль доступу;

2) Криптографічні збої;

3) Ін'єкція;

4) Небезпечний дизайн;

5) Неправильна конфігурація безпеки;

6) Вразливі та застарілі компоненти;

7) Помилки ідентифікації та автентифікації;

8) Порушення цілісності програмного забезпечення та даних;

9) Помилки реєстрації та моніторингу безпеки;

10) Підробка запитів на стороні сервера;

Найбільшою загрозою є ін'єкції, зокрема SQL-ін'єкції. Це вразливість, яка виникає, коли ви надаєте зловмиснику можливість впливати на запити на мові структурованих запитів (SQL), які програма передає до внутрішньої бази даних [2, 3].

Захист веб-сервісів за допомогою VPN

Організація захисту за допомогою технології віртуальної приватної мережі (VPN) передбачає формування захищеного «віртуального тунелю» між відкритими вузлами мережі, недоступного для потенційних зловмисників. Переваги цієї технології очевидні: апаратна реалізація досить проста, немає необхідності створювати або орендувати дорогу виділену мережу, можна користуватися дешевим і відкритим Інтернетом, а швидкість передачі даних через тунель така ж, як в орендованій мережі.

Віртуальна приватна мережа базується на трьох методах реалізації: тунелювання, шифрування та аутентифікація [4, 5].

Для цілей шифрування найбезпечнішим способом є використання алгоритму RSA з парою відкритого та закритого ключів [6].

Тунель забезпечує передачу даних між двома точками – кінцями тунелю, так що джерело даних і приймач приховують всю мережеву інфраструктуру, розташовану між ними.

Середовище передачі тунелю збирає пакети даних мережевого протоколу, що використовується на вході в тунель, і передає їх до виходу без змін. Найпоширенішим вибором є HTTPS. Створення тунелю достатньо для з'єднання двох мережевих вузлів, щоб вони виглядали підключеними до локальної мережі з точки зору програмного забезпечення, яке на них працює. У цей час протокол SSL з алгоритмом блочного шифрування забезпечує безпеку підключення та передачі даних [7, 8].

Тільки реалізувавши ці три властивості, можна захистити інформаційні ресурси компанії та фізично незахищені канали зв'язку від НРД та витоку інформації.

Протокол VPN точно визначає, як система VPN взаємодіє з усіма системами в Інтернеті та рівень безпеки трафіку. Якщо використовується внутрішній обмін інформацією, то взаємодія не є пріоритетом, якщо ж навпаки, то власні протоколи використовувати не слід. Тобто протокол VPN впливає на рівень безпеки всієї системи. Причиною є використання шифрування між двома кінцевими вузлами. Якщо інформація не захищена, зловмисник може перехопити ключі та розшифрувати трафік.

Щоб сформувати VPN за допомогою апаратного та програмного забезпечення (ПЗ), важливо дотримуватися стандартного механізму, заснованого на протоколі безпеки Інтернет-протоколу (IPSec).

Наступний протокол, який використовується для побудови VPN, — протокол тунелювання «точка-точка» (PPTP), переадресація рівня 2 (L2F) і протокол тунелювання рівня 2 (L2TP), який поєднує 2 описані вище протоколи. Але вони не є комплексними і не є повністю функціональними [5, 9].

Інший протокол Internet Key Exchange (IKE) забезпечує передачу інформації через тунель, виключаючи втручання ззовні. Завдання, за які він відповідає і які він вирішує для безпечного управління та обміну криптографічними ключами між віддаленими пристроями. IKE автоматизує процес передачі ключа за допомогою механізму шифрування з відкритим ключем. IKE змінює ключ підключення, що дозволить підвищити конфіденційність інформації, що передається. При цьому інкапсуляція забезпечує мультиплексування кількох транспортних протоколів одним каналом.

Протокол керування з'єднанням (LCP) – протокол «точка-точка» (PPP) визначає гнучкий LCP для встановлення, налаштування та перевірки з'єднання. LCP узгоджує формат інкапсуляції, розмір пакета, параметр налаштування, розрив з'єднання та параметри автентифікації.

Протоколи керування мережею визначають певні конкретні параметри конфігурації для певних транспортних протоколів.

Для створення VPN-тунелів використовуються протоколи PPTP, L2TP, IPsec, OpenVPN.

За технічною реалізацією виділяють такі групи VPN:

1. На основі мережевої ОС.

Як перевагу даного рішення варто відзначити те, що вартість рішення на основі мережевої операційної системи значно нижча за вартість інших рішень. Недоліком такої системи є недостатній захист PPTP.

2. На базі МЕ.

Головною перевагою цього методу є централізація управління елементами. До недоліків такого підходу можна віднести високу вартість рішення на робочому місці та залежність продуктивності від апаратного забезпечення. А також таке рішення підходять тільки для невеликих мереж з обмеженим обсягом переданої інформації.

3. На основі маршрутизаторів.

Одним з найбільших недоліків цього методу є те, що рішення єдиної проблеми захисту інформації від зовнішніх атак розподіляється між декількома функціонально незалежними пристроями (наприклад, роутерами та МЕ).

4. На основі програмного забезпечення.

Переваги програмного пакета AltaVista Tunnel 97 полягають у простоті інсталяції та легкому управлінні. До недоліків можна віднести нестандартну архітектуру і низьку продуктивність.

5. VPN на основі спеціального обладнання з вбудованим криптографічним процесором.

Недоліком такого рішення є його висока вартість.

Як правило, на практиці використовують комбіновані VPN на основі існуючих рішень.

Висновки. Під час аналізу проблем у локальних і глобальних мережах, де використовується VPN, варто зробити висновок, що ці системи повинні забезпечувати виявлення внутрішніх і зовнішніх загроз і вторгнень, фільтрацію зовнішнього трафіку, контроль використання ресурсів корпоративної мережі та запобігання несанкціонованого доступу. Вхідними даними є інформація про структуру та характеристики трафіку, яка може надати можливість побудувати набір правил, які класифікують нормальні чи аномальні компоненти трафіку. Тоді можна отримати гарантований захист мереж завдяки швидкому реагуванню на набір відомих загроз і нештатних ситуацій за рахунок ідентифікації функціонуючих процесів і управління ними для забезпечення доступності інформаційних сервісів.

Література

1. Бенсліман Д., Дустдар С., Шет А. (2008). «Services Mashups: нове покоління веб-додатків». IEEE Internet Computing. 10 (5): 13–15. doi:10.1109/MIC.2008.110.
2. Боднар О., Ткачук Р. Л. Тактика моделей cyber kill chain і unified kill chain: розкриття анатомії кібератак. Зб. тез доп. VI Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології”. (м. Львів, 30 листопада 2023 р.). Львів : ЛДУБЖД, 2023. С. 22–27.
3. Дейв Хартлі (2012). «Атаки та захист SQL-ін’єкцій», стор. 1–4. doi: 10.1016/B978-1-59-749963-7.00001-3.
4. Беспалько О., Ткачук Р. Л., Андріїв Р. Р. Дослідження методів захисту інформації веб-сайтів на основі моделей розподілення доступу та моніторингу ідентифікаторів користувача. Зб. тез доп. VI Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології”. (м. Львів, 30 листопада 2023 р.). Львів : ЛДУБЖД, 2023. С. 16–19.

5. Хонда Осаму, Осакі Хіроюкі, Імасе Макото, Ісідзука Міка, Murayama Junichi (жовтень 2005). «Розуміння TCP через TCP: вплив тунелювання TCP на наскрізну пропускну здатність і затримку». В Атікуззаман, Мухаммед; Баландін Сергій І (ред.). Продуктивність, якість обслуговування та контроль комунікаційних і сенсорних мереж нового покоління III. том. 6011. doi:10.1117/12.630496.
6. Прасетьо Дені, Відіанто Еко Дідік, Індасарі Іке Пратіві (2019-09-06). "Кодування служби коротких повідомлень за допомогою алгоритму Рівест-Шаміра-Адлемана". Журнал Онлайн Інформатика. 4 (1): 39. doi:10.15575/join.v4i1.264.
7. Ткачук Р. Л., Філіпчук Б. Ю., Федина Б. І. Анонімізація користувача в мережі інтернет за допомогою WHONIX // Безпека інформаційних технологій: матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (9–11 травня 2024, Львів, Україна). – 2024. – С. 203–205.
8. Дудикевич В., Микитин Г., Крет Т. та Ребець А. (2016). «Безпека кіберфізичних систем від концепції до комплексної системи захисту інформації», Досягнення кіберфізичних систем, 6(2), стор. 67–75. doi: 10.23939/acps2016.02.067.
9. Філіпчук Б., Ткачук Р. Л., Репетило Т. Б. Потенційні вразливості брандмауера. Зб. тез доп. IV Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”. (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 111–114.

Федунь А. В.

курсант факультету № 2 Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

В.о. завідувача кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЗДІЙСНЕННІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ НА ОСНОВІ ПРОГНОЗІВ (PREDICTIVE POLICING)

У сьогоденні зростання складності глобальних викликів, зокрема кіберзагроз, військових конфліктів, терористичних актів, природних катастроф та соціальних криз створює необхідність впровадження новітніх технологій для їх прогнозування та ефективного реагування. Штучний інтелект (далі – ШІ) стає ключовим інструментом, який здатен змінити підходи до аналізу, планування і реалізації операцій у різних сферах, починаючи від національної безпеки до цивільної оборони.

Однією із сучасних моделей проактивної правоохоронної діяльності, що стрімко розвивається завдяки розвитку комп’ютерних технологій, є модель здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing). Хоча у правоохоронній практиці органів та підрозділів Національної поліції є певний набутий досвід проведення прогнозування, проте наукове дослідження сучасного зарубіжного досвіду у цій галузі може бути корисним для увідповіднення такого організаційного напряму діяльності до найновіших практик прогнозування, яке використовується не лише як додатковий організаційних напрям діяльності, а як самостійну модель побудови правоохоронної практики [4, с. 81].

2 грудня 2020 року в Україні Розпорядженням Кабінету Міністрів України №1556-р було схвалено Концепцію розвитку ШІ в Україні, яка передбачає визначення основних

напрямів та пріоритетних завдань розвитку технологій ШІ з метою забезпечення конкурентоспроможності національної економіки та захисту технологічних інформаційно-комунікаційних систем. Завдяки застосуванню технологій ІШ відбуватиметься моніторинг соціальних мереж та інтернет-ресурсів, що дасть можливість аналізувати аудиторію, виявляти та попереджати певні проблеми [3]. Відповідно до головної мети Концепції – забезпечення інформаційної безпеки було визначено основні напрями її забезпечення (рис. 1).

Рис. 1. Основні напрями забезпечення інформаційної безпеки [3].

Останнім часом дослідження фахівців у царині наукових знань новітніх цифрових технологій показують, що ШІ із застосуванням системи сучасних методів може успішно використовуватись для прогнозування злочинності. Зокрема, інноваційні цифрові технології дозволяють запобігати вчиненню кримінального правопорушення з боку конкретної особи, тобто на стадії формування злочинної мотивації, готування або замаху на його вчинення. Це стало реальністю завдяки моделюванню майбутньої поведінки окремих осіб на підставі особливостей їх соціально-демографічної (стать, вік, місце проживання, рівень доходів, коло спілкування) та кримінально-правової характеристики (наявність судимості, вид раніше вчиненого кримінального правопорушення). Сприяє підвищенню ефективності роботи поліції та прогнозування кримінальних правопорушень також метод картографування злочинності, за допомогою якого формуються прогнози щодо місцевої злочинності та індивідуальної злочинної поведінки. Отже, завдяки технологій ШІ можуть створюватися обґрунтовані прогнози щодо якісних і кількісних показників злочинності [1, с. 134–138].

Здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing) у сучасному виразі є поліцейською інновацією. Ця модель передбачає застосування різних кількісних методів для того, щоб заздалегідь ідентифікувати приблизний час, місце або осіб, які матимуть стосунок до злочину. І хоча не можна сказати, що модель є повністю новою, проте адаптація до потреб правоохоронної діяльності математичних алгоритмів прогнозування, використання сучасних систем ШІ дають змогу на практиці побачити конкретний результат [2].

Література

1. Шевчук В. М. Проблеми застосування штучного інтелекту у правоохоронній діяльності в контексті російсько-української війни. Підготовка правоохоронців зі спеціальності 262 «Правоохоронна діяльність» нової формації: напрями освітнього та наукового забезпечення : матеріали всеукр. наук.-пед. підв.кваліф., 4 березня – 14 квітня 2024 року. Львів – Торунь : Liha-Pres, 2024. С.134–138.
2. Богінський О. В. Роль і місце кримінальної розвідки в сучасних моделях стримування злочинності. Право і безпека. 2017. № 4 (67). С. 12–17. URL: http://dspace.uni-vd.edu.ua/xmlui/handle/123456789/3081
3. Концепція розвитку штучного інтелекту в Україні [Електронний ресурс]: Розпорядження Кабінету міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
4. Федчак І. А. Концептуальні основи та науково-практичні аспекти проактивних моделей правоохоронної діяльності : монографія. Львів : Львівський державний університет внутрішніх справ, 2024. 628 с.

Федчак Ігор Андрійович

завідувач кафедри інформаційних технологій факультету № 2 (з підготовки фахівців для підрозділів превентивної діяльності та правоохоронних інформаційних систем Національної поліції України) Львівського державного університету внутрішніх справ, доктор юридичних наук, доцент

ЩОДО ВИКОРИСТАННЯ СТРУКТУРОВАНИХ ТЕХНІК ДЛЯ ГЕНЕРУВАННЯ ГІПОТЕЗ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ

Важливу роль у роботі співробітників підрозділів Національної поліції відіграє діяльність з генерування гіпотез. Особливого значення генерування гіпотез набуває у діяльності співробітників підрозділів Департаменту кримінального аналізу, одним із завдань яких є пошук значення з великих масивів даних, які слід аналізувати з метою інформаційного аналітичного супроводу діяльності оперативних підрозділів та органів досудового розслідування. Нерідко формулювання гіпотез є вкрай важливим кроком у прийнятті управлінських рішень про розподіл ресурсів та визначенні напрямів подальших правоохоронних дій, та може бути трудомістким процесом, який займає багато часу.

Формулювання гіпотез передбачає створення обґрунтованих припущень щодо різних аспектів проблеми, які потребують подальшого дослідження та перевірки. Також слід зазначити, що гіпотези бувають різних типів, наприклад прості, складні, альтернативні, логічні, статистичні, або емпіричні.

Філософський енциклопедичний словник визначає поняття «гіпотеза» як спосіб пізнавальної діяльності, побудови ймовірного, проблематичного знання, коли формулюється одна з можливих відповідей на питання, що виникло під час дослідження; одне з можливих розв’язань проблеми… [1, с. 121].

Гіпотеза походить з набору базових припущень, яке формує основу для дій і оцінки результату. Створення гіпотез – це процес, у якому обране за основу обґрунтоване припущення вдосконалюється шляхом збору та аналізу додаткової релевантної до проблеми інформації. Гіпотезу слід формувати на основі того, що відомо, або можливо спостерігати. Наступним кроком при побудові гіпотез буде збір і аналіз даних для перевірки цієї гіпотези, її розвитку або уточнення. На підставі сформульованої та перевіреної гіпотези співробітники правоохоронних органів застосовують наявні гласні та негласні сили та засоби. У подальшому слід проводити відстеження ефективності застосовуваних заходів та дій, за потреби проводити їх корегування. Такий цикл формулювання, тестування та уточнення гіпотез для використання інформації під час прийняття рішень – життєво важливий для прийняття ефективних рішень і вирішення складних проблем боротьби зі злочинністю.

З огляду на критично важливу роль процесу формулювання (розроблення) гіпотез в діяльності правоохоронних органів доречно використовувати структуровані підходи, які дозволяють забезпечити систематичність, логічність та послідовність аналітичного дослідження. Структуровані підходи також дозволяють аналітикові формулювати гіпотези на основі попередніх емпіричних даних, послідовно опрацьовувати змінні, передбачати потенційні взаємозв'язки між ними та створювати надійний алгоритм перевірки висунутих припущень. Крім того, це сприяє мінімізації впливу суб'єктивних чинників, забезпечує прозорість дослідницького процесу, полегшує критичний аналіз та інтерпретацію результатів, а також дозволяє перевірити отримані висновки, що підвищує достовірність дослідження.

Структурований підхід до генерування гіпотез слід застосовувати тоді, коли тема, яку потрібно дослідити, або питання, на яке потрібно дати відповідь, є настільки важливими, що систематична оцінка всіх альтернатив видається виправданою. Також структурований підхід до генерування гіпотез слід використовувати коли необхідно враховувати багато різних змінних, коли існує невизначеність щодо результату та коли аналітики або особи, які приймають рішення, мають різні погляди на досліджуване явище [2].

Структуровані підходи дозволяють аналітикам генерувати найповніші набори взаємовиключних гіпотез. Вони підвищують ймовірність виявлення всіх релевантних гіпотез і, таким чином, підвищують довіру аналітиків до результатів аналізу. Крім того, вони дозволяють розпочати процес аналізу якомога більш неупереджено. Таким чином, можна також зменшити негативний вплив упереджень, неправильно застосованих евристик та інтуїтивних пасток [3, с. 169].

Одним з прикладів застосування структурованого підходу до формулювання гіпотези є техніка «крок за кроком». Реалізація такої техніки передбачає необхідність чіткого визначення проблеми чи питання, для якого слід генерувати гіпотези. У подальшому слід переглянути наявну інформацію та пояснення щодо проблеми, поведінки чи діяльності, які підлягають оцінюванню. Якщо формулювання гіпотез проводиться групою осіб, доцільно, щоб кожен присутній сформулював до трьох різних пояснень/гіпотез. Далі слід видалити дублікати гіпотез. Слід також перевірити чи були враховані всі фактори впливу. У подальшому проводиться об'єднання різних гіпотези в групи, які слід назвати. Учасники процесу мають перевірити те, чи є гіпотези взаємовиключними. Для подальшого розгляду слід обрати найбільш перспективні гіпотези.

У подальшому слід видалити гіпотези, які не мають сенсу, а ті, які заслуговують на відпрацювання слід оцінити, наскільки вони є правдоподібними. Такі гіпотези потрібно проранжувати відповідно до їхньої вірогідності. На завершення аналітику слід

відібрати найбільш перспективні гіпотези для подальшого розгляду та відпрацювання [3, с. 171, 174].

Як висновок слід зазначити, що використання структурованого підходу до формування гіпотез забезпечує систематичний та всебічний підхід до генерації, оцінки та відбору найбільш перспективних пояснень досліджуваної проблеми у сфері правоохоронної діяльності. Цей підхід дозволяє учасникам процесу колективно та послідовно розвивати гіпотези, уникаючи дублювання, забезпечуючи врахування всіх факторів впливу та остаточний відбір найбільш вірогідних і значущих пояснень.

Література

1. Філософський енциклопедичний словник. В. І. Шинкарук та ін. Київ : Інститут філософії імені Григорія Сковороди НАН України : Абрис, 2002. 742 с.
2. Ole Donner. Intelligence Comprehensive Training (Structured Analytic Techniqes in Action) Warsaw. 13th-22nd August 2024. Structured Analysis Germany.
3. Heuer Richards, Pherson Randolph. Structured Analytic Techniques for Intelligence Analysis. 2nd Edition, CQ Press, California, 2015. 384 p.

Царук Юрій Юрійович

ад'юнкт кафедри оперативно – розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ІНФОРМАЦІЙНО – АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ЩОДО ПРОТИДІЇ ВЧИНЕННЯ ШАХРАЙСТВА

Проблематика. Окремі аспекти інформаційно – аналітичного забезпечення оперативних підрозділів Національної поліції України щодо протидії шахрайству, вчиненого шляхом незаконних операцій з використанням електронно – обчислювальної техніки.

Вступ. Згідно з статистичними даними офісу Генерального прокурора України про кримінальні правопорушення у провадженнях, досудове розслідування у яких здійснюється органами Національної поліції, у відсотковому відношенні, від загальної кількості зареєстрованих кримінальних правопорушень у провадженнях, до кількості рішення по яких не прийнято (нерозкриті кримінальні правопорушення), в розрізі років: 2020 р. – 71%; 2021 р. – 63%; 2022 р. – 80%; 2023 р. – 81% [1]; чітко відображено значний приріст скоєння шахрайства, як виду злочину. Для виокремлення проблематики протидії було здійснено аналіз наукового доробку в галузі інформаційно – аналітичного забезпечення підрозділів Національної поліції України в питанні протидії оперативними підрозділами кримінальної поліції Національної поліції України шахрайству, вчиненого шляхом незаконних операцій з використанням електронно – обчислювальної техніки.

Мета. Виокремлення теоретичних навичок застосовування сучасних технологій в процесі розпізнання події кримінального правопорушення та ідентифікації осіб, причетних до його вчинення.

Результати. Результативність діяльності правоохоронних органів у боротьбі зі злочинністю безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності.

На етапі реформування правоохоронних органів спостерігались труднощі в створенні єдиної інтегрованої системи інформаційно – аналітичного забезпечення як у роботі між правоохоронними органами, так і між їхніми оперативними підрозділами, зокрема через відсутність міжвідомчих нормативно – правових актів щодо регулювання доступу до цих інформаційних ресурсів усіх суб'єктів правоохоронної діяльності, а також порядку опрацювання й обміну інформацією між цими суб'єктами електронно, у режимі онлайн [2, с.143].

У нормативно-правових актах та науковій літературі з терміном «інформаційно-аналітичне забезпечення» доволі часто вживаються терміни «інформаційне забезпечення», «інформаційно-аналітична діяльність», «інформаційно-аналітична робота», «аналітична робота».

В аналітичній роботі використовується: оперативний аналіз (аналіз даних телефонних дзвінків, аналіз злочинних угруповань, аналіз справ, порівняльний аналіз); тактичний аналіз (кримінальний аналіз, аналіз кримінальних тенденцій, геопросторовий аналіз, аналіз місць концентрації злочинності, часовий аналіз, МО-аналіз, кримінальні моделі, профілі підозрюваних/жертв); стратегічний аналіз (SWOT-аналіз, PEST-аналіз, аналіз моделей/форм злочинності та профілювання, аналіз тенденцій, аналіз з використанням географічного профілювання); аналіз даних з відкритих джерел (OSINT); аналіз даних з багатьох джерел (Multi-Source Analysis).

У теорії та практиці ОРД із терміном «інформаційне забезпечення» вживається термін «інформаційно-аналітичне забезпечення», під яким розуміється кількісне (консолідація масивів інформації у вигляді баз і банків даних, упорядкування, систематизація), а також якісно-змістовне перетворення оперативної інформації (виробництво нових знань, ухвалення управлінських рішень) на основі інформаційної аналітики.

Головним завданням інформаційно-аналітичного забезпечення є систематичне і своєчасне надходження в оперативні підрозділи достовірної оперативної інформації [3, с.35-36].

Для ефективної боротьби зі злочинністю оперативним підрозділам НП та інших правоохоронних органів необхідно мати відповідну інформацію відносно діяльності кримінальних структур та процесів, що відбуваються у злочинному середовищі.

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (система ІПНП) призначена для інформаційно-аналітичного забезпечення діяльності Національної поліції України, наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до єдиної інформаційної системи МВС (ЄІС МВС), забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу та електронної взаємодії з МВС, іншими органами державної влади. З метою забезпечення оперативно-розшукової діяльності оперативних підрозділів кримінальної поліції, на виконання вимог Закону України «Про оперативно-розшукову діяльність», Наказу МВС України від 05.05.2016 р. № 07, у Національній поліції України впроваджено окрему інформаційну систему – автоматизовану інформаційну систему оперативного призначення, в якій організовано обробку інформації з грифом секретності «таємно» (далі – АІС ОП) [4, с.67-72].

Розробляючи продукти стратегічного аналізу, використовують різні методи і техніки, але однією з основних навичок стратегічного аналітика є розуміння того, які аналітичні інструменти чи техніки найбільше відповідають цілям аналізу.

Основна мета аналітичних інструментів – створення аналізу більш точним. Існує широкий перелік інструментів і технік стратегічного управління, які використовуються у різних сферах життєдіяльності. Для поліцейської роботи найкращі результати у стратегічному аналізі можуть бути отримані завдяки застосуванню таких інструментів і технік, як: SWOT-аналіз; аналіз ризиків; PEST-аналіз; SOCTA; OSINT (аналіз інформації з відкритих джерел); аналіз злочинних моделей та профілів; аналіз тенденцій; аналіз географічних профілів. Допоміжну функцію можуть виконувати: аналіз результатів; аналіз явищ; ситуаційний аналіз; статистичний аналіз [4, с.207-256].

Досліджені обставини, в результаті їх сукупності, можуть суттєво покращити інформаційно – аналітичне забезпечення оперативних підрозділів Національної поліції України щодо протидії шахрайству, вчиненого шляхом незаконних операцій з використанням електронно – обчислювальної техніки.

Висновки. Застосовування сучасних технологій в процесі розпізнання події кримінального правопорушення та ідентифікації осіб, причетних до його вчинення, є невід'ємною складовою інформаційно – аналітичного забезпечення діяльності оперативних підрозділів Національної поліції України у протидії шахрайству, вчиненому шляхом незаконних операцій з використанням електронно – обчислюваної техніки, та є «ключовим» моментом найефективнішого вирішення завдань оперативно – розшукової діяльності.

Реалізація основних форм інформаційно – аналітичної роботи в оперативно – розшуковій діяльності передбачає різний вияв функціонального аспекту організації ОРД, в тому числі збір, обробку, аналіз і оцінку інформації з метою підвищення ефективності діяльності оперативних підрозділів Національної поліції України.

Література

1. Сайт офісу Генерального прокурора України. [Електронний ресурс]. - Режим доступу: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.
2. Поляк С. (2017). Інформаційно-аналітичне забезпечення діяльності підрозділів карного розшуку в процесі протидії втягненню неповнолітніх у злочинну діяльність. Jurnalul juridic national: teorie şi practică, 28(6-1), 140-144.
3. Мовчан А.В. Інформаційно – аналітична робота в оперативно – розшуковій діяльності Національної поліції: навчальний посібник / А.В. Мовчан. – Львів: ЛьвДУВС, 2017. – 244 с.
4. Федчак І.А. Основи кримінального аналізу: навчальний посібник / І.А. Федчак. - Львів: Львівський державний університет внутрішніх справ, 2021. - 288 с.

Ящук Валентина Ігорівна

доцент кафедри управління інформаційною безпекою Львівського державного університет безпеки життєдіяльності, Львів, Україна, к.е.н., доцент

ПРОБЛЕМИ ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМУ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В ОРГАНАХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Дослідження присвячено дослідженню теоретичних основ, науково-методичних підходів та організаційно-функціональних аспектів впливу штучного інтелекту на

систему захисту державної таємниці. В роботі визначено сучасні тенденції у сфері захисту державної таємниці та розроблено методичні рекомендації для оцінки потенційних ризиків, пов'язаних із застосуванням штучного інтелекту. Запропоновано концептуальну модель, яка дозволяє структурувати процес вирішення науково-практичної проблеми забезпечення безпеки державної таємниці в умовах розвитку технологій штучного інтелекту.

Ключові слова: захист державної таємниці, штучний інтелект, кібербезпека, інформаційна війна, критична інфраструктура, дезінформація.

The research is devoted to the study of theoretical foundations, scientific and methodological approaches and organizational and functional aspects of the impact of artificial intelligence on the system of state secret protection. The work identifies current trends in the field of state secret protection and develops methodological recommendations for assessing potential risks associated with the use of artificial intelligence. A conceptual model is proposed that allows structuring the process of solving the scientific and practical problem of ensuring the security of state secrets in the context of the development of artificial intelligence technologies.

Keywords: state secret protection, artificial intelligence, cybersecurity, information warfare, critical infrastructure, disinformation.

Штучний інтелект (ШІ) стрімко еволюціонує, дедалі ширше впроваджуючись у різноманітні аспекти людської діяльності, включаючи сферу безпеки. Використання ШІ для захисту державної таємниці супроводжується як значними перевагами, так і потенційними ризиками, що робить дослідження його впливу на цю сферу вкрай актуальною науковою задачею.

Наявні дослідження здебільшого акцентуються на аналізі можливих загроз, які можуть виникати в результаті застосування ШІ. Зокрема, серед основних ризиків виокремлюють зловмисне використання ШІ, питання визначення відповідальності за його дії, а також загрозу упередженості алгоритмів. ШІ здатний сприяти створенню більш складних та ефективних кібератак, розробці новітніх видів зброї або поширенню дезінформації. Виникає питання, хто відповідатиме за наслідки роботи ШІ, якщо вони призведуть до витоку державної інформації. Окрім того, алгоритми ШІ можуть містити приховані упередження, що здатне призводити до прийняття помилкових рішень.

Разом з тим, існують дослідження, які розглядають позитивні аспекти використання ШІ в захисті державної таємниці, такі як: автоматизація рутинних завдань, покращення точності аналізу даних, створення більш ефективних систем захисту. ШІ може автоматизувати багато рутинних завдань, пов'язаних з аналізом великих обсягів даних, що дозволяє звільнити фахівців для виконання більш складних задач. ШІ здатний виявляти загрози, які можуть бути пропущені людським аналітиком. ШІ може бути використаний для розробки більш інтелектуальних систем захисту інформації, які здатні адаптуватися до нових загроз.

Разом з тим невирішеними залишаються питання забезпечення безпечного використання ШІ в державних органах, правові та етичні проблеми при використанні ШІ в захисті державної таємниці, оцінювання ризиків, пов'язаних з використанням ШІ, та розроблення ефективних заходів протидії, забезпечення прозорості систем, що базуються на ШІ.

Вплив ШІ на захист державної таємниці спричиняє виникнення як загроз так і можливостей. Серед основних загроз можна виокремити **с**творення кібератак більшої

складності, генерація дезінформації, соціальна інженерія. ШІ може бути використаний для автоматизації процесу пошуку вразливостей в системах безпеки, розробки нових видів шкідливого програмного забезпечення та проведення масштабних DDoS-атак. Також ШІ може бути використаний для створення великих обсягів фейкових новин та інших видів дезінформації, що може дестабілізувати суспільство і підірвати довіру до державних інституцій. ШІ може бути використаний для створення більш переконливих фішингових листів та інших видів соціальної інженерії, що дозволяє здобувати конфіденційну інформацію.

Досліджуючи можливості варто відзначити збільшення ефективності аналізу даних, автоматизація рутинних завдань, розроблення нових методів захисту. ШІ може аналізувати великі обсяги даних в режимі реального часу, виявляючи підозрілу активність та прогнозуючи потенційні загрози. ШІ може автоматизувати багато рутинних завдань, таких як моніторинг мережі, аналіз логів та ідентифікація загроз, що дозволяє звільнити фахівців для виконання більш складних задач. ШІ може бути використаний для розроблення нових методів захисту інформації, таких як адаптивні системи захисту, які здатні самонавчатися і адаптуватися до нових загроз.

Штучний інтелект є потужним інструментом, який може бути використаний як для захисту, так і для атаки. Для того щоб максимізувати переваги ШІ і мінімізувати ризики, виникає потреба у розробленні комплексного підходу до його використання в сфері безпеки. Цей підхід повинен включати в себе розроблення ефективних систем управління ризиками, створення правової бази, міжнародне співробітництво, постійне навчання та підвищення кваліфікації фахівців. Запровадження комплексного підходу вимагає розроблення методів оцінювання ризиків, пов'язаних з використанням ШІ, та розроблення заходів для їх мінімізації. Також виникає потреба у розробленні нових правових норм, які регулюють використання ШІ в сфері безпеки. Співпраця з іншими країнами для розробки спільних стандартів безпеки ШІ дозволить підвищити ефективність захисту таємної інформації.

Загалом, ШІ відкриває нові можливості для забезпечення безпеки держави, але його використання потребує обережного та зваженого підходу. Підсумовуючи викладене вище, можна виокремити такі рекомендації, як розвиток національних стратегій в галузі кібербезпеки, які враховуватимуть використання ШІ, інвестування в дослідження та розробки в галузі ШІ та кібербезпеки, створення міжнародних форумів для обговорення питань, пов'язаних з використанням ШІ в сфері безпеки, розроблення системи сертифікації систем ШІ, що використовуються в державних органах, проводити навчання та підвищення кваліфікації фахівців в галузі ШІ та кібербезпеки.

Незважаючи на значну кількість досліджень в цій галузі, багато питань залишаються відкритими. Необхідно проводити подальші дослідження в таких напрямах, як розроблення методів оцінювання стійкості систем ШІ до атак, дослідження впливу ШІ на міжнародну безпеку та розробка нових алгоритмів машинного навчання для виявлення аномалій в мережевому трафіку. Завдяки впровадженню цих рекомендацій можна мінімізувати ризики, пов'язані з використанням ШІ, та максимізувати його потенціал для забезпечення національної безпеки. Використання ШІ в захисті державної таємниці є перспективним напрямком досліджень, який вимагає подальшого розвитку.

Література

1. Ящук В.І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами / Ящук В.І. // Scientific Collection «InterConf+», 45(201): with the Proceedings of the 8thInternational Scientific and Practical Conference «International Scientific Discussion: Problems, Tasks and Prospects» (May19-20, 2024; Brighton, United Kingdom)/ comp. by LLC SPC «InterConf».Brighton: A.C.M. Webb Publishing Co Ltd., 2024. 678p.(P.632-641).
2. Ящук В.І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави / В.І.Ящук // Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 364 (С. 259-286).

Зміст

Наукове видання

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
20 грудня 2024 року

Опубліковано в авторській редакції

Формат 60×84/8. Умовн. друк арк. 9,3.

Львівський державний університет внутрішніх справ Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції ДК № 2541 від 26 червня 2006 р.

І 78 **ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ**: матеріали Науково-практичної конференції (Львів, 20 грудня 2023) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2025. –137 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України», що проводилася 20 грудня 2024 року у Львівському державному університеті внутрішніх справ.

УДК 004