УДК 343.148:004
DOI https://doi.org/10.24144/2788-6018.2024.05.105

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Герасименко О.М.,
кандидат юридичних наук, докторант,
Національна академія Служби безпеки України
ORCID: 0009-0005-5078-3829

Герасименко О.М. Проблеми та перспективи застосування штучного інтелекту у протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури.

Стаття присвячена дослідженню проблем та перспектив використання штучного інтелекту у протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури. Розглянуто особливості державної політики, сучасний стан правового регулювання використання інноваційної технології в Україні, проаналізовано проблемні питання застосування штучного інтелекту у ході виконання завдань попередження, виявлення, припинення, досудового розслідування кримінальних проваджень у відповідній сфері.

Опрацьовано основні напрями застосування штучного інтелекту у протидії кримінальним правопорушенням на об'єктах критичної інфраструктури такі як: інтелектуальне виявлення загроз у процесі протидії; автоматизація алгоритмів протидії протиправним посяганням; інформаційно-аналітичне забезпечення.

Висвітлено ключові методи та технології штучного інтелекту, що можуть бути використані у процесі протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури, зокрема: глибоке навчання, машинне навчання, обробка природної мови та комп'ютерне бачення. Окреслено потенційні ризики та проблемні питання впровадження штучного інтелекту у автоматизований процес протидії кримінальним правопорушенням на об'єктах критичної інфраструктури. Звернута увага на дотримання принципів прозорості та підзвітності діяльності, законності, відповідальності за помилкові рішення, забезпечення прав і свобод людини, попередження ризиків дискримінації, надмірного покладання на штучного інтелекту.

Констатовано про необхідність удосконалення правових засад використання штучного інтелекту у протидії кримінальним правопорушенням на об'єктах критичної інфраструктури, а також внесення змін та доповнень до законодавства України, що стосується кримінально-процесуальної діяльності СБ України. Перспективним напрямом подальших досліджень визначено впровадження технологій штучного інтелекту в систему протидії кримінальним правопорушенням на об'єктах критичної інфраструктури.

Ключові слова: критична інфраструктура, кримінальні правопорушення, інформаційно-аналітичне забезпечення, штучний інтелект, протидія кримінальним правопорушенням, машинне навчання.

Gerasimenko O.M. Problems and prospects of the application of artificial intelligence in the combat of criminal offenses by The Security Service of Ukraine at critical infrastructure facilities.

The article is devoted to the study of the problems and prospects of the use of artificial intelligence in countering criminal offenses by the Security Service of Ukraine at critical infrastructure facilities. The peculiarities of state policy, the current state of legal regulation of the use of innovative technology in Ukraine are considered, and problematic issues of the use of artificial intelligence in the course of the tasks of prevention, detection, termination, and pretrial investigation of criminal proceedings in the relevant field are analyzed.

The main areas of application of artificial intelligence in combating criminal offenses at critical infrastructure facilities have been worked out, such as: intelligent detection of threats in the process of countermeasures; automation of algorithms for combating illegal encroachments; information and analytical support.

The key methods and technologies of artificial intelligence that can be used in the process of combating criminal offenses at critical infrastructure facilities by the Security Service of Ukraine are highlighted, in particular: deep learning, machine learning, natural language

processing and computer vision. The potential risks and problematic issues of introducing artificial intelligence into the automated process of combating criminal offenses at critical infrastructure facilities are outlined. Attention is drawn to compliance with the principles of transparency and accountability of activity, legality, responsibility for erroneous decisions, ensuring human rights and freedoms, prevention of risks of discrimination, excessive reliance on artificial intelligence.

The need to improve the legal basis for the use of artificial intelligence in combating criminal offenses at critical infrastructure facilities, as well as introducing changes and additions to the legislation of Ukraine concerning the criminal-procedural activity of the Security Service of Ukraine, was noted. The introduction of artificial intelligence technologies into the system of combating criminal offenses at critical infrastructure facilities is identified as a promising direction for further research.

Key words: critical infrastructure, criminal offenses, information and analytical support, artificial intelligence, combating criminal offenses, machine learning.

Постановка проблеми. Сучасні загрози безпеці об'єктам критичної інфраструктури, включаючи кіберзлочинність, терористичні акти, диверсії та інші кримінальні правопорушення з використанням високотехнологічних знарядь протиправних посягань, вимагають нових підходів до організації діяльності Служби безпеки України з протидії їм. В умовах широкого застосування на об'єктах критичної інфраструктури інноваційних цифрових технологій, зростання обсягів інформаційних даних, які генеруються та обробляються в системах критичної інфраструктури, технологічної складності функціонування систем, їх частин та сукупності, традиційні методи захисту критичної інфраструктури від кримінальних посягань недостатньо забезпечують належний рівень національної безпеки. У зв'язку з цим, організація протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури, як однієї з загроз, потребує застосування прогресивних технологій. Це потребує проведення наукової розвідки з метою підготовки пропозицій правового та практичного спрямування застосування можливостей штучного інтелекту у процесі діяльності Служби безпеки України за означеним напрямом.

Актуальність опрацювання визначеної теми також обумовлена дискусійністю серед науковців проблем використання штучного інтелекту, що посилилася після схвалення Кабінетом Міністрів України «Концепції розвитку штучного інтелекту в Україні» від 02.12.2020 № 1556-р та вимогами п. 1 ст. 24 Закону України «Про Службу безпеки України», в частині здійснення інформаційно-аналітичної діяльності з питань, пов'язаних з національною безпекою України [1, 2].

Зважаючи на значущість означеного назвою статті предмета дослідження, дискусійність розв'язання проблем, а також з огляду сучасних потреб теорії та практики, вбачається актуальним проведення дослідження визначеної теми.

Аналіз останніх досліджень і публікацій. Аналіз результатів досліджень проблем кримінального процесу та криміналістики, оперативно-розшукової діяльності, питань законодавчого забезпечення протидії кримінальним правопорушенням на об'єктах критичної інфраструктури засвідчує, що в межах предметів своїх робіт окремими питання займалися такі вітчизняні науковці як: С.М. Бортник – розкрив особливості регулювання використання штучного інтелекту у правоохоронній системі (2021 р.) [3]; А. Клян – розкрив особливості правового регулювання штучного інтелекту в Україні та світі (2021 р.) [4]; К.С. Токарєва та Н.О. Савліва – проаналізували особливості правового регулювання штучного інтелекту в Україні (2021 р.) [5]; Ю.І. Когут – проаналізував актуальні вектори та проблеми розвитку штучного інтелекту, як інструментарію безпеки та інтелектуальної зброї майбутнього (2024 р.) [7]; О.І. Бугера – проаналізував використання штучного інтелекту для запобігання злочинності (2021 р.) [8]; Р.І. Благута та А.В. Мовчан – опрацювали сучасний стан і проблеми використання новітніх технологій у розслідуванні злочинів (2020 р.) [10]; Г.В. Форос та О.А. Балтовський – розв'язали проблеми інформаційно-аналітичного забезпечення правоохоронної діяльності (2022 р.) [13]; О.І. Зачек та Д.І. Йосифович – дослідили перспективи та проблеми застосування штучного інтелекту в діяльності правоохоронних органів (2023 р.) [16]; М.В. Карчевський – розкрив проблеми використання штучного інтелекту у протидії злочинності (2020 р.) [17]; В.М. Шевчук – проаналізував використання технологій штучного інтелекту та процесу цифровізації криміналістики в умовах війни (2021 р.) [21] та ін.

Зазначені вище здобутки, що отримані у ході проведення досліджень, частково розкривають визначений нами предмет розвідки. Отже, комплексного та актуального системного дослідження, яке вирішує проблеми теоретичного, правового та організаційного забезпечення використання штучного інтелекту у протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури – немає, що негативно впливає на ефективність практичної діяльності вітчизняної спецслужби, а

тому є потреба проведення розвідки окресленого назвою статті питання.

Метою статті – є вирішення проблем використання технологій штучного інтелекту у протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури. За результатами аналізу наукових матеріалів передбачається підготовка пропозицій удосконалення відповідної діяльності, розв'язання проблем, а також формулювання напрямів подальших розвідок.

Виклад основного матеріалу. За останнє десятиліття набуло значної вагомості, особливо серед гуманітарних наук, питання застосування технологій штучного інтелекту (далі – ШІ) у сфері правоохоронної діяльності. Цифровізація економіки, оборони та інших секторів забезпечення національної безпеки України, комп'ютеризація систем управління об'єктами критичної інфраструктури (далі – ОКІ), а також зростаюча динаміка рівня загроз та шкоди останнім від кримінальних правопорушень, актуалізували завдання впровадження технологій ШІ у правоохоронну діяльність, одним з напрямів якої є протидія Службою безпеки України (далі – СБ України) кримінальним посяганням на ОКІ. Зазначене передусім обумовлено технологічним потенціалом програмних продуктів ШІ та необхідністю виконання в сучасних складних умовах завдань попередження, виявлення, припинення, досудового розслідування СБ України кримінальних правопорушень на ОКІ. Водночас використання ШІ у діяльності СБ України наразі обмежене невідповідністю чинних правових засад потребам практичної діяльності, на що звертають увагу вітчизняні науковці.

Так, С.М. Бортник робить висновок, що використання ШІ у правоохоронних органах України є недостатнім через складну фінансову ситуацію та слабке правове регулювання [3].

Своєю чергою А. Клян відмічає, що в українському законодавстві немає правового визначення та регулювання використання ШІ, а також відсутні нормативні положення щодо відповідальності за його неправомірне застосування [4].

Наведене вище підтримують К.С. Токарєва та Н.О. Савліва, які зазначають, що українські правові акти не регулюють діяльність ШІ, тому планується співпраця з міжнародними організаціями для розробки стандартів та Етичного кодексу використання ШІ в Україні [5].

Про зазначене йдеться й у затвердженій розпорядженням Кабінетом Міністрів України від 02.12.2020 року № 1556-р «Концепції розвитку штучного інтелекту» (далі – Концепція), в якій однієї з проблем закріплена «відсутність або недосконаліть правового регулювання штучного інтелекту (в тому числі у сферах освіти, економіки, публічного управління, кібербезпеки, оборони)» [6]. Першочерговим завданням у сфері науково-технологічних досліджень Концепція визначає піднесення ролі технологій штучного інтелекту в Україні, а «основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об'єкти критичної інфраструктури)…» [6].

Отже, можемо зробити висновок, що сучасний стан формування та реалізації державної політики України в частині застосування можливостей ШІ у процес протидії кримінальним правопорушенням на ОКІ знаходиться на початковому етапі, що не відповідає потребам національних інтересів. Тому однією з наших пропозицій є внесення до переліку завдань розділу Концепції «Кібербезпека» доповнень в такій редакції: «формування та ефективна реалізація єдиної скоординованої державної політики, спрямованої на розв'язання проблем правового забезпечення застосування ШІ у процесі протидії кримінальним правопорушенням на об'єктах критичної інфраструктури та впровадження їх на практиці».

Продовжуючи дослідження теми у контексті зазначених вище проблем, розглянемо основні наукові підходи та можливі напрями застосування інноваційних можливостей ШІ, які, на наш погляд, можуть бути практично корисними у ході здійснення кримінально-правових, оперативно-розшукових та контррозвідувальних заходів протидії СБ України кримінальним правопорушенням на ОКІ.

Так, з приводу наведеного Ю.І. Когут звертає увагу на те, що використання штучного інтелекту у захисті критичної інфраструктури дозволяє краще виявляти загрози та захищатися від них [7].

Доповнює зазначене О.І. Бугера, який у своєму дослідженні, яке присвячено використанню ШІ для запобігання злочинності, наголошує на тому, що інтелектуальні системи безпеки, які використовують відеоспостереження на основі камер зі штучним інтелектом, дають змогу запобігати злочинам і терористичним атакам, завдяки чому рівень злочинності в середньому може суттєво знижуватися [8, с. 83].

Важливість інтелектуальної протидії протиправним посяганням на ОКІ закріплена Законом України від 05.10.2017 р. № 2163-VIII. «Про основні засади забезпечення кібербезпеки України», який визначає необхідність «створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз» [9].

Враховуючи наведене проаналізуємо окремі методи та алгоритми ШІ, які, на наш погляд,

дозволять автоматизувати вирішення завдань попередження, виявлення, припинення, досудового розслідування СБ України, а також забезпечать створення умов щодо документування протиправної діяльності на стадіях готування, замаху і вчинення кримінальних правопорушень на ОКІ у реальному часі, зокрема:

– аналіз аномалій та поведінковий аналіз. Системи на основі ШІ здатні аналізувати великий обсяг даних в режимі реального часу, що може бути використано для пошуку і фіксації ознак кримінальних посягань. Наприклад, з метою забезпечення кібербезпеки на об'єктах критичної інфраструктури ШІ може аналізувати трафік мережі та виявляти аномальні активності, які можуть свідчити про готування вчинення кібератак, терактів, диверсій та ін. та повідомляти про це;

– раннє виявлення загроз. Алгоритми глибокого навчання дозволяють системам ШІ «навчатися» на історичних даних про інциденти та загрози. Зазначене забезпечить можливість не лише реагувати на поточні загрози, але й прогнозувати потенційні кримінальні посягання ще до їх фактичного виникнення. Завчасне попередження є критично важливим для вжиття заходів запобігання та мінімізації шкоди від кримінальних правопорушень на ОКІ;

– ідентифікація у реальному часі. Використання ШІ допомагає у виявленні ознак складних та багаторівневих кримінальних правопорушень на ОКІ, що можуть проходити непоміченими традиційними методами. ШІ може автоматично адаптуватися до нових атак, аналізуючи їх у реальному часі та допомагаючи створювати нові захисні стратегії [10, 11].

З приводу наведеного звертаємо увагу на те, що ст. 86 «Допустимість доказу» Кримінального процесуального кодексу України закріплю (далі – КПКУ), що «1. Доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом. 2. Недопустимий доказ не може бути використаний при прийнятті процесуальних рішень, на нього не може посилатися суд при ухваленні судового рішення» [12]. Таким чином, використання отриманих із застосуванням ШІ доказів можливе за умови внесення змін до відповідних статей КПКУ. Тому пропонуємо внести відповідні зміни та закріпити положення статей в такій редакції: ч. 1 ст. 84 «Докази» КПКУ – «1. Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку (у тому числі із застосуванням штучного інтелекту), на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню»; ч. 1 ст. 99 «Документи» КПКУ – «1. Документом є спеціально створений (у тому числі з використанням штучного інтелекту) з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [12].

Таким чином можемо зробити висновок, що зазначені вище пропозиції дозволять посилити автоматизацію протидії СБ України кримінальним правопорушенням на ОКІ. Застосування ШІ створить можливість оркеструвати дії між різними системами та підрозділами під час кіберзагрози, що забезпечить мінімізацію заподіяння шкоди від кримінальних посягань на ОКІ. Завдяки цьому можна скоротити час реагування, що є критично важливим у багатьох випадках. У разі виявлення ознак готування протиправного посягання, системи на основі ШІ можуть також надавати рекомендації щодо найбільш ефективних заходів для їх попередження та мінімізації шкоди. Це забезпечить можливість скоротити витрати часу на прийняття управлінських рішень.

Продовжуючи зазначимо, що не менш важливим напрямом застосування ШІ з протидії СБ України кримінальним правопорушенням на ОКІ є інформаційно-аналітичне забезпечення. Завдяки здатності ШІ аналізувати величезні обсяги даних з різних джерел, виявляти приховані закономірності та прогнозувати потенційні ризики, його використання підвищить ефективність інформаційно-аналітичної діяльності з питань, що пов'язані з національною безпекою України для ОКІ [2].

На це звертають увагу автори Г.В. Форос та О.А. Балтовський, які зазначають, що інформаційно-аналітичне забезпечення в контексті кримінального процесу є важливим інструментом для оптимізації досудового розслідування, а також захисту об'єктів критичної інфраструктури (ОКІ), що включає енергетичні системи, транспортні мережі, телекомунікаційні системи, водопостачання, медичні установи тощо. В умовах зростаючої цифровізації та глобалізації ОКІ стають мішенями для кіберзлочинців, терористів. Ефективне інформаційно-аналітичне забезпечення полягає в моніторингу, зборі, аналізі та інтерпретації даних для виявлення потенційних загроз, їхньої оцінки та розробки відповідних заходів протидії [13].

Застосування штучного інтелекту в інформаційно-аналітичному забезпеченні протидії СБ України кримінальним правопорушенням на ОКІ можуть ґрунтуватися на широкому спектрі методів і технологій, що можуть забезпечити виявлення загроз, прогнозування подій та підтримку прийняття рішень. Важливими напрямами є

глибоке навчання, машинне навчання, обробка природної мови, комп'ютерне бачення та ін. інноваційні підходи.

Проаналізуємо можливість застосування зазначених методів і технологій в діяльності з протидії СБ України кримінальним правопорушенням на ОКІ.

Так, глибоке навчання (анг. Deep Learning) є підгалуззю машинного навчання, яка використовує багатошарові нейронні мережі для вивчення складних патернів у великих наборах даних [14]. Без використання нейронних мереж обробка вхідного візуального контенту стає надзвичайно трудомістким завданням. Також ручне опрацювання графічної інформації неминуче супроводжується помилками через природну втому та інші психофізичні чинники. Тому цей метод має кілька важливих застосувань у сфері безпеки критичної інфраструктури:

– згорткові нейронні мережі (анг. Convolutional Neural Networks, CNN). CNN є ефективними для розпізнавання образів та аналізу відео. Вони можуть виявляти підозрілі дії осіб, що готують вчинення кримінального правопорушення на ОКІ або об'єкти на відео з камер спостереження. Наприклад, CNN можуть розпізнавати залишені без нагляду предмети, що можуть бути вибухівками, або визначати незвичайну поведінку осіб, що може свідчити про потенційну загрозу;

– рекурентні нейронні мережі (анг. Recurrent Neural Networks, RNN). RNN, включаючи їхні варіанти, такі як Long Short-Term Memory (LSTM), використовуються для аналізу послідовних даних, таких як мережевий трафік або динаміка показників систем. Вони можуть допомогти в прогнозуванні загроз на основі аналізу історичних даних, виявляючи патерни, які передують атакам на ОКІ;

– автоенкодери. Ці нейронні мережі можуть використовуватися для виявлення аномалій в даних, наприклад, для виявлення аномальної мережевої активності, що може свідчити про потенційні кібератаки. Вони здатні «навчатись» на нормальних даних і виявляти відхилення від типових патернів [15, с. 101–110].

Як зазначають О.І. Зачек та Д.І. Йосифович, одним із найсучасніших штучних інтелектів на сьогодні є ChatGPT (англ. Generative Pretrained Transformer), можливості якого можуть бути адаптовані для протидії СБ кримінальним правопорушенням на ОКІ. Він здатний аналізувати тексти, фотографії та відео, що публікуються на сторінках злочинців у соціальних мережах, з метою виявлення ознак протиправних посягань. Може також розпізнавати ключові слова та фрази в текстових повідомленнях, що вказують на готування протиправних посягань. Програма може розпізнавати обличчя правопорушників, автомобілі, номерні знаки та інші важливі ознаки у відео та зображеннях з камер спостереження, що допомагає в ідентифікації злочинців. ChatGPT може використовуватися також для аналізу даних про злочинність і надання рекомендацій щодо превентивних заходів [16, с. 65].

Що стосується машинного навчання, то воно охоплює широкий спектр методів, які дозволяють алгоритмам навчатися з даних і покращувати свої результати без явного програмування. Основні методи машинного навчання, що можуть використовуватися у протидії СБ України кримінальним правопорушенням на ОКІ, включатимуть:

– методи класифікації. Алгоритми, такі як Support Vector Machines (SVM), Random Forest, і K-Nearest Neighbors (KNN), можуть застосовуватися для класифікації подій або об'єктів на підставі їх характеристик. Наприклад, ці методи можуть використовуватися для класифікації трафіку в мережі на звичайний і потенційно небезпечний;

– алгоритми кластеризації. Методи, такі як K-Means або DBSCAN, можуть бути застосовані для виявлення груп схожих об'єктів у великих масивах даних. Вони корисні для виявлення ознак кримінальних правопорушень, які можуть свідчити про їх підготовку;

– рекомендаційні системи. Методи машинного навчання, такі як Collaborative Filtering і Content-Based Filtering, можуть бути застосовані для створення систем попередження, які зможуть прогнозувати готування до вчинення кримінального правопорушення на основі аналізу поведінкових патернів користувачів або інших системних суб'єктів;

– Баєсові мережі. Можуть використовуватись для моделювання ймовірності скоєння кримінальних правопорушень на ОКІ на основі історичних даних та залежностей між ними. Ці моделі допоможуть прогнозувати загрози та рекомендувати заходи протидії кримінальним правопорушенням на ОКІ [14].

Одночасно М.В. Карчевський з приводу зазначеного вище звертає увагу на те, що алгоритми машинного навчання можуть ухвалювати рішення, спираючись на дані, які можуть бути необ'єктивними або неповними, що потенційно призводить до дискримінації. Це пов'язано з тим, що будь-яка людська діяльність має певну упередженість. Якщо навчання алгоритмів ґрунтуватиметься на результатах такої діяльності, то штучний інтелект також стане упередженим, і з часом ця упередженість може посилюватися [17, с. 33-34]. Зазначене повинно бути обов'язково враховано під час організації протидії СБ України кримінальним правопорушенням на ОКІ.

Обробка природної мови (Natural Language Processing, NLP) є критично важливою техноло-

гією для аналізу текстових даних, зокрема великих обсягів неструктурованих даних, таких як звіти, новини, соціальні мережі та повідомлення на форумах [18]. Основні методи NLP включають:

– аналіз тональності (анг. Sentiment Analysis): може бути адаптована з метою оцінки емоційного забарвлення текстів, що дозволяє виявляти потенційні загрози або визначати протиправні наміри на основі аналізу публікацій у соціальних мережах або інших відкритих джерелах;

– тематичне моделювання (анг. Topic Modeling): алгоритми, такі як Latent Dirichlet Allocation (LDA), можуть бути використані з метою ідентифікації основних тем у великих обсягах тексту, що дозволяє виявляти нові загрози чи тренди в інформаційному просторі;

– іменоване розпізнавання сутностей (анг. Named Entity Recognition, NER): метод для виділення ключових об'єктів, таких як імена осіб, організацій, місць тощо, що може бути корисним для виявлення потенційних кримінальних груп чи планів протиправних посягань на ОКІ;

– семантичний аналіз (анг. Semantic Analysis): використовується для розуміння змісту та сенсу тексту, що дозволяє автоматично інтерпретувати дані та створювати відповідні рекомендації для дій [18].

Своєю чергою комп'ютерне бачення (анг. Computer Vision) та відеоаналітика є підходом, який використовується для аналізу відеопотоків та зображень. Його застосування включатиме:

– розпізнавання облич (анг. Face Recognition) – використовується для ідентифікації та відстеження підозрілих осіб у реальному часі на ОКІ. Ця технологія може також бути інтегрована в системи контролю доступу;

– аналіз поведінки (анг. Behavior Analysis) – використання алгоритмів для виявлення підозрілої поведінки або аномальної активності у відеопотоці. Наприклад, виявлення осіб, які переміщуються в забороненій зони, або виявлення покинутих предметів;

– розпізнавання автомобільних номерів (анг. License Plate Recognition) – використовується для моніторингу транспортних засобів на об'єктах критичної інфраструктури, що дозволяє автоматично виявляти підозрілі транспортні засоби;

– відеоаналітика з використанням дронів – використання дронів з інтегрованими системами комп'ютерного бачення для моніторингу великих територій та виявлення загроз у віддалених або важкодоступних місцях [19; 10, С. 82–84].

Варто також відзначити переваги інтеграції різних методів ШІ в єдині системи підтримки прийняття рішень, що, на наш погляд, є важливим кроком для ефективної протидії кримінальним правопорушенням на ОКІ. Такі системи включають: а) системи експертного аналізу – інтеграція ШІ у системи експертного аналізу, що дозволяють аналізувати великі обсяги даних і надавати рекомендації для прийняття рішень як під час проведення заходів оперативно-розшукової діяльності, так і у ході кримінально-процесуальної діяльності. Ці системи можуть використовуватися для управління кризовими ситуаціями на ОКІ; б) інтелектуальні системи реагування – включають автоматизовані рішення для реакції на виявлені загрози в реальному часі, такі як блокування доступу, активація протоколів безпеки або інформування відповідних служб; в) системи підтримки ситуаційної обізнаності – включають об'єднання даних з різних джерел (сенсори, відео, текстові дані) і використання алгоритмів ШІ для створення цілісної картини ситуації на об'єктах критичної інфраструктури [20].

Враховуючи зазначене вище можемо зробити логічний висновок, що застосування методів і технологій ШІ дозволить суттєво підвищити ефективність протидії СБ України кримінальним правопорушенням на ОКІ. Водночас впровадження технологій штучного інтелекту у діяльність СБ України несе в собі не лише значні переваги, але й низку потенційних ризиків та проблемних питань, про які необхідно зазначити.

Так, важливим питанням, на наш погляд, є забезпечення прозорості та підзвітності роботи ШІ. Часто алгоритми ШІ працюють як «чорний ящик», і процес прийняття рішень може бути незрозумілим для людей. Це ускладнює можливість оскарження рішень, прийнятих на основі ШІ, та створює ризики порушення прав людини, зокрема права на приватність та захист персональних даних [17].

Використання ШІ для автоматизованого прийняття рішень у кримінальному провадженні, наприклад, щодо запобіжних заходів, також викликає занепокоєння з погляду дотримання права на справедливий суд. Алгоритми не здатні врахувати всі нюанси конкретної справи та індивідуальні обставини підозрюваного чи обвинуваченого. Окрім того, відсутність прозорості та можливості оскарження рішень, згенерованих ШІ, ставить під сумнів реалізацію таких засад судочинства як змагальність та презумпція невинуватості [8].

З погляду В.М. Шевчука використання штучного інтелекту у судочинстві та правоохоронній діяльності можливе лише з урахуванням принципів верховенства права, дотримання основних прав людини, поваги до честі та гідності, рівності перед законом і судом, пропорційності, змагальності сторін, прозорості, неупередженості та справедливості. Однак, повна заміна судді на штучний інтелект наразі неможлива, але ніщо не заважає покращити роботу суду шляхом впровадження таких технологій. Штучний інте-

лект має розглядатися не як заміна судді, а як інструмент, що допомагає здійснювати правосуддя [21, с. 174].

Як зазначає М.В. Карчевський, одним з викликів є забезпечення надійності та стійкості алгоритмів ШІ до потенційних атак, таких як «adversarial attacks», коли зловмисники намагаються обманути модель ШІ. Обробка даних у реальному часі також вимагає значної обчислювальної потужності та низької затримки передачі даних, що може бути складно реалізувати на великих ОКІ [17].

З погляду С.М. Бортника, проблемним моментом є й ризик надмірного покладання на системи ШІ та применшення ролі людського фактора. Правоохоронці можуть почати сприймати результати аналізу ШІ як незаперечну істину, ігноруючи можливість помилок чи спотворень. Це загрожує ключовому принципу верховенства права – остаточні рішення щодо долі людини мають прийматись відповідальними посадовими особами, а не машинами [3]. Тому важливо забезпечити належний рівень взаємодії людини та ШІ, щоб уникнути надмірної залежності від автоматизованих систем та зберегти можливість людського контролю у критичних ситуаціях. Для мінімізації означених ризиків, впровадження технологій ШІ у правоохоронну діяльність має супроводжуватись розробкою чітких етичних стандартів та правових рамок. З метою розв'язання етичних питань застосування ШІ у кримінальному судочинстві необхідна тісна співпраця між розробниками ШІ-систем, правоохоронними органами та експертами з етики. Повинні бути розроблені етичні принципи та стандарти, які будуть покладені в основу розробки та використання ШІ у цій чутливій сфері [3].

Отже, використання ШІ у протидії кримінальним правопорушенням на об'єктах критичної інфраструктури має значний потенціал, але водночас пов'язане з низкою проблемних питань та ризиків. Забезпечення точності, надійності, прозорості та етичності роботи ШІ-систем є ключовими викликами, які потребують комплексного підходу та співпраці всіх зацікавлених сторін. В іншому випадку, замість підвищення ефективності правоохоронної системи ми ризикуємо отримати потужний інструмент для зловживань та утисків з боку держави. Водночас цей процес має відбуватись максимально виважено та відповідально, з неухильним дотриманням фундаментальних прав і свобод людини. Лише у такий спосіб переваги від впровадження ШІ переважать потенційні ризики та загрози.

Підсумовуючи викладене вище, можемо відзначити, що з повагою ставимося до наукових здобутків учених, які свого часу вирішували у рамках предметів своїх досліджень наукові проблеми, характерні для використання штучного інтелекту у протидії СБ України кримінальним правопорушенням на ОКІ. Наступним кроком наукового дослідження стане розробка проблематики організації впровадження штучного інтелекту в систему протидії кримінальним правопорушенням на об'єктах критичної інфраструктури з урахуванням положень Кримінального процесуального кодексу України та потреб практики.

Висновки. Об'єкти критичної інфраструктури, такі як енергетичні системи, транспортні мережі, системи водопостачання та зв'язку, є життєво важливими для функціонування держави та забезпечення безпеки її громадян. Однак, в умовах воєнного стану вони все частіше стають об'єктами для кримінальних правопорушень, що вчиняються з використанням сучасних технологій та методів. Кіберзлочинність, тероризм, диверсії та інші форми злочинної діяльності становлять серйозну загрозу для критичної інфраструктури. У зв'язку з цим, ефективна протидія кримінальним правопорушенням на об'єктах критичної інфраструктури вимагає застосування сучасних інформаційно-аналітичних інструментів та технологій штучного інтелекту. Інформаційно-аналітичне забезпечення дозволяє збирати, обробляти та аналізувати величезні обсяги даних з різних джерел, виявляти закономірності та прогнозувати потенційні загрози. Штучний інтелект здатний автоматизувати процеси аналізу даних, розпізнавання образів та прийняття рішень, що значно підвищує ефективність протидії злочинності.

Незважаючи на очевидні переваги використання штучного інтелекту в інформаційно-аналітичному забезпеченні протидії СБ України кримінальним правопорушенням, їх практичне застосування все ще є недостатнім. Це пов'язано з проблемами правового забезпечення, етичними аспектами використання технологій, забезпечення безпеки даних та конфіденційності, необхідність спеціальної підготовки фахівців.

Подальше використання отриманих у ході дослідження результатів вбачаємо в закріплені висунутих пропозицій в нормативно-правових актах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. Кабінет Міністрів України : офіц. сайт. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення: 26.08.2024).
2. Про Службу безпеки України: Закон України від 25 березня 1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення 22.08.2024).

3. Бортник С.М. Особливості регулювання використання штучного інтелекту у правоохоронної системі. Застосування інформаційних технологій у діяльності правоохоронних органів: матеріали круглого столу (м. Харків, 14 грудня 2021 р.). Харків: ХНУВС, 2021. С. 28–31.
4. Клян А. Правове регулювання штучного інтелекту в Україні та світі. GOLAW. 03.02.2022. URL: https://golaw.ua/ua/insights/publication/pravoveregulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti (дата звернення: 02.09.2024).
5. Токарєва К.С., Савліва Н.О. Особливості правового регулювання штучного інтелекту в Україні. *Юридичний вісник*. 2021. № 3(60). С. 148–153. URL: https://jrnl.nau.edu.ua/index.php/UV/article/view/15967/23255 (дата звернення: 02.09.2024).
6. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/ laws/show/1556-2020-%D1%80 (дата звернення: 08.09.2024).
7. Когут Ю.І. Штучний інтелект і безпека: практичний посібник / за ред. А.С. Довгопола. Київ: Консалтингова компанія «СІДКОН»; ВД Дакор, 2024. 294 с.
8. Бугера О.І. Використання штучного інтелекту для запобігання злочинності. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2021. Том 32(71), № 6. С. 82–86. URL: https://www.juris.vernadskyjournals.in.ua/journals/2021/6_2021/15.pdf (дата звернення: 02.09.2024).
9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.08.2024).
10. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
11. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков. Електронні текстові дані (1 файл: 19,9 Мбайт). Київ : КПІ ім. Ігоря Сікорського. 2022. 82 с.
12. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 22.08.2024).
13. Форос Г.В., Балтовський О.А. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навчально-методичні матеріали. Одеса: ОДУВС, 2022. 26 с.
14. Машинне навчання проти глибокого навчання – ключові відмінності. URL: https://www.unite.ai/uk/machine-learning-vs-deep-learning-key-differences/ (дата звернення: 12.08.2024).
15. Хома В.В., Хома Ю.В., Сабодашко Д.В., Хома П.П. Автоенкодери для опрацювання промахів сигналів ЕКГ у системі біометричної автентифікації. *Штучний інтелект*. 2019. № 1-2. С. 101–110.
16. Зачек О.І., Йосифович Д.І. Перспективи та проблеми застосування штучного інтелекту в діяльності правоохоронних органів. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 22 грудня 2023 р.). Львів: ЛьвДУВС, 2024. 192 с.
17. Карчевський М.В. Штучний інтелект та протидія злочинності. Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листопада 2020 р.). Харків: Право, 2020. 112 с.
18. Що таке обробка природної мови (NLP) та як вона може використовуватися у бізнесі. URL: https://metinvest.digital/ua/page/1052 (дата звернення: 12.08.2024).
19. Розпізнавання зображень Vs. Комп'ютерний зір: у чому відмінності? URL: https://www.unite.ai/uk/image-recognition-vs-computer-vision / (дата звернення: 12.08.2024).
20. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков. Електронні текстові дані (1 файл: 19,9 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. 82 с.
21. Шевчук В.М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. Актуальні проблеми протидії злочинності та корупції: матеріали наук.-практ. конф. (м. Харків, 2023 р.). Харків, 2023. С. 171–176.