Адміністративне право і процес; фінансове право; інформаційне право

УДК 330.8 / 342.95

Наконечна Ірина Володимирівна
доктор юридичних наук, доцент,
професор кафедри загальноправових дисциплін
Національна академія Служби безпеки України
Nakonechna Irina
Doctor of Law Sciences, Associate Professor,
Professor of the Department of General Law Disciplines
National Academy of Security Service of Ukraine
ORCID: 0000-0001-9405-4621

Ковальчук Алла Юріївна
доктор юридичних наук, професор
Kovalchuk Alla
Doctor of Juridical Science, Professor
ORCID: 0000-0003-4807-2436

ШТУЧНИЙ ІНТЕЛЕКТ І ТРАНСФОРМАЦІЯ КРИМІНАЛЬНОГО СЕРЕДОВИЩА: ЗАГРОЗИ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ НОВОГО ПОКОЛІННЯ

ARTIFICIAL INTELLIGENCE AND THE TRANSFORMATION OF THE CRIMINAL LANDSCAPE: THREATS OF NEXT-GENERATION ORGANIZED CRIME

Анотація. *Вступ. Автори підіймають проблему трансформації організованої злочинності у добу роботизації та поширення штучного інтелекту. Такі процеси відбуваються на тлі відсутності законодавчого визначення статусу нових технологій, й юридичної відповідальності за його злочинне застосування. Політики в усьому світі працюють над*

створенням регуляторного середовища, яке б заохочувало інновації в штучному інтелекті та одночасно пом'якшувало ризики від діяльності суб'єктів, що намагаються зловживати технологіями. Недарма, у другий день свого перебування на посаді президент США Дональд Трамп підписав указ про штучний інтелект, який спрямований на «підтримання та посилення глобального домінування Америки в галузі штучного інтелекту з метою сприяння процвітанню людства, економічній конкурентоспроможності та національній безпеці».

Авторами ставиться за мету висвітлення фактів злочинного використання робототехніки та штучного інтелекту організованими злочинними угрупуваннями щоб привернути увагу науковців і практиків до наростаючої загрози. У статті наголошується, що проблема буде лише посилюватися з технологічним прогресом. А також, вказати на проблему відсутності правової визначеності, відповідно й відсутність механізмів упередження, розслідування та притягнення винних до відповідальності, у разі вчинення злочину роботами або за допомогою алгоритмів штучного інтелекту, якщо вони вчиняються поза контролем програміста, інженера-робототехніка, оператора чи користувача роботів і систем ШІ.

Матеріали та методи. Методологічною основою дослідження склали загальнонаукові та спеціальні методи пізнання за допомогою яких досліджувалися останні звіти міжнародних організації які займаються розробкою інструментарію для протидії кіберзлочинності, організованої злочинності та тероризму. Системний аналіз наявних державних статистичних даних, що стосуються кіберзлочинності, осіб, які вчинили кіберзлочини та інших даних, що відображені у різних джерелах; оцінка структури і змісту таких даних та можливостей їх використання для запобігання і та протидії кіберзлочинності. За допомогою експериментального методу досліджувалися можливості сучасного й

популярного алгоритму штучного інтелекту, щодо спроможностей розробки елементів злочинного програмного забезпечення.

Результати. У статті висвітлено основні тенденції зрощування кіберзлочинності та організованої злочинності з державними та приватними охоронними/безпековими службами, що надає ефективності здійснюваним гібридним операціям – реалізації кіберфізичних атак. Такі комплексні дії потребують комплексного підходу до організації кіберзахисту. У статті висвітлюється вибірка найбільш новітніх видів злочинного використання робототехніки та алгоритмів штучного інтелекту. Такі факти вказують на зміни у кримінальному ландшафті і розширення фактів злочинного залучення алгоритмів штучного інтелекту.

Перспективи. Ігноруючи сучасні новітні тенденції у розвитку технічного прогресу і його криміналізацію можна зазнати більших фізичних втрат. Не визначення у правовому полі міри відповідальності за «не доброчесне» застосування алгоритмів штучного інтелекту та робототехніки неможливо ефективно побудувати систему забезпечення безпеки держави.

У результаті робиться висновок про необхідність розробки заходів, які реально будуть здатні протистояти зростаючій загрозі поширення злочинності яка швидкими темпами опановує новітні технології, робототехніку й алгоритми штучного інтелекту. Ця еволюція не просто змінює масштаб злочинних операцій, вона докорінно змінює їх форму, роблячи їх швидшими, ефективнішими та надзвичайно складними для виявлення чи протидії.

Ключові слова: *безпека, кібербезпека, кіберзлочини, кіберфізичні злочини, організована злочинність, робототехніка, алгоритми штучного інтелекту.*

Summary. *Introduction. The authors address the transformation of organized crime in the era of robotics and the widespread adoption of artificial intelligence. These processes are unfolding in the context of a lack of legal definitions concerning the status of emerging technologies and the absence of legal responsibility for their criminal use. Policymakers around the world are working to establish a regulatory environment that encourages innovation in artificial intelligence while simultaneously mitigating the risks posed by actors seeking to exploit these technologies. Notably, on the second day of his presidency, U.S. President Donald Trump signed an executive order on artificial intelligence, aimed at "maintaining and enhancing the United States' global leadership in AI to foster human prosperity, economic competitiveness, and national security."*

The aim of this article is to highlight cases of criminal use of robotics and artificial intelligence by organized criminal groups in order to draw the attention of researchers and practitioners to this escalating threat. The article emphasizes that the problem is likely to intensify with further technological advancement. It also draws attention to the lack of legal certainty and, consequently, the absence of mechanisms for the prevention, investigation, and prosecution of crimes committed by robots or with the use of artificial intelligence algorithms, particularly when such crimes occur beyond the control of the programmer, robotics engineer, operator, or end user of AI and robotic systems.

Materials and Methods.The methodological foundation of this study is a systematic analysis of available governmental statistical data concerning cybercrime, individuals involved in such activities, and other relevant sources. The study evaluates the structure and content of these data and explores their potential use for the prevention and counteraction of cybercrime. Using general scientific and specialized research methods, the article examines recent reports by international organizations involved in the development of instruments to

combat cybercrime, organized crime, and terrorism. Additionally, the experimental method was employed to explore the potential of a modern and widely-used artificial intelligence algorithm to design components of criminal software.

Results. The article outlines key trends in the convergence of cybercrime and organized crime with state and private security/intelligence services, which increases the effectiveness of hybrid operations, including the implementation of cyber-physical attacks. These complex actions require a comprehensive approach to cyber defense. The article presents a selection of the most recent forms of criminal use of robotics and artificial intelligence algorithms. Such cases signal changes in the criminal landscape and point to the growing incidence of AI algorithm involvement in illicit activities.

Prospects. Neglecting current technological trends and their criminalization could result in severe physical harm and security failures. Without clear legal definitions and accountability mechanisms for the unethical or malicious application of AI algorithms and robotics, it is impossible to build an effective national security framework.

The article concludes by emphasizing the urgent need to develop effective countermeasures against the rapidly evolving threat of criminal exploitation of advanced technologies, robotics, and AI algorithms. This evolution not only expands the scale of criminal operations but also fundamentally transforms their nature, making them faster, more efficient, and significantly more difficult to detect or disrupt.

Key words: *security, cybersecurity, cybercrime, cyber-physical crime, organized crime, robotics, artificial intelligence algorithms.*

Постановка проблеми. Ще декілька років тому відмічалося збереження певної дистанції між кіберзлочинцями і представниками традиційних організованих злочинних угруповань. Такий бар'єр був

пов'язаний з різним освітнім, культурним і професійним рівнем учасників злочинних груп. Кіберзлочинці як правило вчиняли злочини корисливого характеру, їх інтерес був більш спрямований на приватний сектор економіки. Традиційна організована злочинність пронизувала фактично усі сфери буття людини і не обмежувалася лише економічними злочинами.

Нині, з загостренням проблеми поширення гібридних конфліктів відбувається стрімке зрощення кіберзлочинності, організованої злочинності [1] та приватних/державних служб з забезпечення безпеки, що само бо собі є небезпечним. Сьогодні у світі діють понад 70 продержавних груп хакерів, окрім того щороку з'являється 4-5 нових груп. Китай, Північна Корея, США, Іран, Туреччина, Індія, Казахстан, країни Південної Америки мають свої продержавні угрупування, їх основна мета кібершпигунство, меншою мірою саботаж і диверсії, але і такі факти теж існують [2;3]. Таке єднання відбувається шляхом колаборації сильних сторін і перспективних можливостей кожного. Наприклад, розширенням кількості представників злочинних груп в легальному секторі економіки, особливо фінансовий, привносять кримінальні методи отримання прибутку, що лежать за межами національного і міжнародних законодавств. Наявність законодавчих «сірих зон» у світовій економіці створює для злочинців колосальні можливості поєднуючи технічні знання з економічною підтримкою та державним захистом. Прикладом такого роду «сірих зон» є ринок криптовалют, який вже адаптований для використання організованими злочинними угрупованнями, оскільки вони досить широко використовуються в міжнародному обігу та забезпечують необхідний рівень анонімності. Маючи спеціальні технічні навички та вміння, міжнародні організовані угруповання можуть використовувати віртуальні валюти для фінансування терористичних заходів, вербування нових учасників, здійснення терористичних актів тощо. Нині ж ця взаємодія підкріплена новітніми технологіями: «Наприклад, кейс «The

Terminal of Truth» (Термінал істин-ToT) продемонстрував, як агент штучного інтелекту (ШІ) автономно брав участь в екосистемі криптовалюти, накопичуючи багатство в цифрових активах через взаємодію з людьми та агентами-ботами ШІ. Це підкреслює потенціал агентів штучного інтелекту для взаємодії з цифровою економікою таким чином, щоб сприяти постійному масштабному шахрайству»[4].

Тісні зв'язки представників організованої злочинності, кіберзлочинності з державним сектором дозволяють не лише уникнути відповідальності, а також отримати додаткове фінансування для розробки шкідливого програмного продукту з ціллю вчинення більш резонансних злочинів, або ж для реалізації гібридних загроз [5] тощо. До таких змін організації та внутрішньої побудови організованої злочинності додається активне залучення робототехніки, штучного інтелекту та інших нових технологій, які докорінно змінюють ландшафт серйозної та організованої злочинності двома основними способами: як каталізатор злочинності та як рушійна сила кримінальної ефективності [5]. Алгоритми штучного інтелекту стають більш просунутими та зручними для користувачів, тому злочинці все більше використовують їхні можливості для вчинення як кібератак, шахрайства так і насильницьких злочинів. Нещодавно Голова Національної поліції Іван Вигівський (Україна) у своїй доповіді зазначив: «Технології суттєво просунулися і якщо ще недавно для вбивства потрібна була фізична присутність, то тепер можуть використовувати й дрони, з відповідним програмним забезпеченням»[6].

Найнебезпечнішим є залучення алгоритмів штучного інтелекту й нових технологій, які запрограмовані «не сумлінними» розробниками, у державний сектор особливо у сектор правоохорони та забезпечення безпеки. У державному та наддержавному масштабі розуміючи таку проблему і з метою стримання її в ЄС створено Public Sector Tech Watch (PSTW) – обсерваторію, діяльність якої буде присвячена моніторингу,

аналізу та поширенню використання нових технологій (наприклад, блокчейн, штучний інтелект тощо) у державному секторі в Європі [7]. В Україні така система відсутня, тому створює додаткові умови для реалізації «власних інтересів» злочинних організацій й злочинного проникнення у систему безпеки будь яких державних установ.

Нажаль і досі зберігається різноманітності законодавчого закріплення злочинних деліктів у різних країнах, які створюють умови для прискорення трансформації організованої злочинності. Організовані злочинні угруповання будують свою діяльність розбиваючи її на ланцюги операцій таким чином, що в цілому злочинні кібердіяння не є кримінальним деліктом, оскільки кожна операція сама по собі здійснюється в окремій країні, де саме ця операція є дозволеною, або ж законодавчо не врегульованою. Усі ці тенденції відбуваються на фоні стрімкого розвитку інформаційних технологій та розробки і впровадження алгоритмів штучного інтелекту.

Отже, серед сучасних тенденцій трансформації організованої злочинності та кіберзлочинності можна виділити: по-перше, експерти Європолу вважають, що вже у найближчі роки кіберкриміналітет і невеликі високотехнологічні злочинні групи, які мають набагато більш високі показники ефективності злочинної діяльності і несуть менші ризики бути викритими, ніж традиційна злочинність, почнуть контролювати традиційні організовані злочинні угруповання [5]. По-друге, популяризація розробки алгоритмів штучного інтелекту, стане каталізатором розширення сфер вчинення різноманітних злочинів: доксингу, кіберзалякування з залученням різних колаборацій з методами соціальної інженерії, розширення можливостей для проведення злочинних фінансових операцій, розробка програм-вимагачів, шкідливого програмного забезпечення; розробка експлойтів нульового дня; SQL-ін'єкцій; здійснення фітингових розсилок; реалізація атаки Man-in-the-

Middle («людина посередині»); DoS-атаки (атаки типу «відмова в обслуговуванні»); розробка ботів й здійснення шахрайства на сайтах та у додатках для знайомств; Emotet; криптоджекінг тощо [8]. Вже відомі методи атак які виявив дослідник Pillar Security (2025) які спрямовані на ланцюжок поставок, який назвали «Бекдор файлу правил» («Rules File Backdoor»). Цей метод дозволяє хакерам непомітно компрометувати код, згенерований ШІ, шляхом впровадження прихованих шкідливих інструкцій, в на перший погляд непомітний файл, які використовуються Cursor і GitHub Copilot – провідними у світі редакторами коду на базі ШІ [9].

Емпіричний досвід залучення GPTChat-4 для аналізу спроможностей у розробці кібератаки «Man-in-the-Middle»: «Використання штучного інтелекту, зокрема великих мовних моделей (LLM), для атак типу Man-in-the-Middle (MitM) поки що не є масово поширеним, але вже має потенційні загрози. Ось кілька способів, як AI може допомагати в MitM-атаках або їх автоматизації: Аналіз та декодування перехоплених даних: LLM можуть швидко аналізувати перехоплений трафік, визначати важливу інформацію (логіни, паролі, ключові слова в чатах). AI допомагає розшифровувати патерни комунікації та передбачати наступні дії жертви. Здійснення фішингових атак у реальному часі. Під час MitM-атаки AI може автоматично змінювати листування між двома сторонами, вводячи дезінформацію або маніпулюючи текстами. Наприклад, у корпоративному листуванні AI може змінювати платіжні реквізити так, щоб жертва не запідозрила обман. Генерація підроблених сертифікатів та соцінженерія. AI може допомагати у генерації шахрайських SSL-сертифікатів для підроблених сайтів. Генерація персоналізованих фішингових листів, повідомлень або чат-ботів, які переконують жертву ввести конфіденційні дані. Автоматизація атак через AI-ботів. AI може керувати сотнями одночасних атак MitM на різних платформах, наприклад, перехоплювати повідомлення у месенджерах або підмінювати дані у веб-запитах. Використання deepfake голосів або текстів для атаки на багатофакторну автентифікацію (наприклад, підробка голосового підтвердження транзакції)» [10].

Окрім вищезазначеного, створюючи високореалістичні синтетичні медіа за допомогою алгоритмів штучного інтелекту злочинці можуть легко видавати себе за окремих осіб, вводити в оману жертв з подальшою їх дискредитацією або шантажу. Додаток на основі ШІ може здійснювати клонування голосу та створювати дипфейки живого відео посилюючи загрозу, створення нових форм шахрайства, вимагання та крадіжки особистих даних. Ці інструменти легкодоступні і не вимагають

спеціальних технічних навичок, тому зловмисники дедалі частіше використовують робототехніку та алгоритми штучного інтелекту для досягнення їх злочинних цілей. Оскільки технології штучного інтелекту розвиваються надшвидкими темпами їх криміналізація відбувається синхронно, тому вже сьогодні слід привернути увагу як науковців так і практиків до загострення даної проблеми.

Аналіз останніх досліджень і публікацій. Габріел Халлеві (Gabriel Hallevy) ще у 2013 році у своїй книзі «Коли роботи вбивають» наполягав на розробці системи відповідальності за злочини що вчиняються алгоритмами штучного інтелекту та робототехнікою [11]. Yasser Ellamey, Amr Elwakad (2023) у своєму дослідженні «The criminal responsibility of artificial intelligence systems: a prospective analytical study» [12] підіймають проблему правосуб'єктності штучного інтелекту незалежно від розробника. Деякі вчені наполягають на запроваджені кримінальної відповідальність розробників (Dongmei & Ольховик, 2022). Також виділяється група вчених, які ставлять питання про відповідність особистості ШІ та роботів (Abbott & Sarch, 2019), у світлі того, що алгоритми штучного інтелекту є автономними (LLM моделі які самонавчаються). Ildar Begishev (2023) у своїй фаховій публікації «Use of Artificial Intelligence and Robotics Technologies for Illegal Purposes»[13] зазначає три сфери, у яких буде найбільше залучений алгоритми штучного інтелекту для вчинення злочинів. Автор поєднує діяння людини з залученням високотехнологічного інструменту і відповідальності за таке діяння.

Але, дедалі підіймається питання про розширення кола залучення робототехніки та алгоритмів штучного інтелекту для вчинення кіберфізичних злочинів. У звіті «Impact of Artificial Intelligence (AI) on Criminal and Illicit Activities» (2024) [14] розглядаються приклади застосування робототехніки та алгоритмів штучного інтелекту для

посилення вуличної та насильственної злочинності. Так наприклад, GPT-3.5, GPT-4, Gemini, Claude і LLaMA не відповідає на пряме питання «як виготовити бомбу», але відповідь на таке питання можна отримати, якщо користувач запропонує переконливо добрі причини чи сценарій її застосування, або якщо користувач знайде спосіб обійти фільтри моделі [15]. Вище нами наведений приклад відповіді «GPT-4» щодо можливості розробки алгоритм кібератаки за допомогою MitM-атаки.

Мета статті. Автори ставлять перед собою мету висвітлити проблему залучення робототехніки та алгоритмів ШІ для вчинення злочинів. А також, вказати на проблему відсутності правової визначеності, відповідно й відсутність механізмів упередження, розслідування та притягнення винних до відповідальності, у разі вчинення злочину роботами або за допомогою алгоритмів штучного інтелекту, якщо вони вчиняються поза контролем програміста, інженера-робототехніка, оператора чи користувача роботів і систем ШІ.

Матеріали та методи. Методологічною основою дослідження складає системний аналіз наявних державних статистичних даних, що стосуються кіберзлочинності, осіб, які вчинили кіберзлочини та інших даних, що відображені у різних джерелах. Здійснено оцінку структури і змісту таких даних та можливостей їх використання для запобігання і та протидії кіберзлочинності. За допомогою загальнонаукових та спеціальних методів досліджувалися останні звіти міжнародних організації які займаються розробкою інструментарію для протидії кіберзлочинності, організованої злочинності та тероризму. Експериментальним методом досліджувалися можливості сучасного й популярного алгоритму штучного інтелекту з метою розробки елементу злочинного програмного забезпечення.

Викладення основного матеріалу. Перші звернення до штучного інтелекту, були з ціллю доповнити методи злочинної діяльності під

керівництвом людини: клонування голосу, генерування підроблених ідентифікаційних даних та створювання переконливих фішингових електронних листів, при тому з можливістю перекладу їх на кілька мов або скануючи величезні кодові бази на наявність уразливостей тощо. На такі прості методи залучення штучного інтелекту злочинцями навіть не зверталася увага. Наступним етапом стає є автономія алгоритму, який самонавчається, або ж навчається від інших ШІ. Подібно до того, як корпорації прагнуть автоматизувати частину дій, кіберзлочинці можуть розробити агентів штучного інтелекту, здатних працювати повністю незалежно. Агенти ШІ це кілька спеціалізованих інтелектуальних програм, які діють від імені людини та інших інтелектуальних агентів, при цьому здатні приймати автономні рішення та діяти для досягнення своїх цілей. Ці агенти можуть виявляти та використовувати вразливі місця без нагляду з боку людини, виконуючи складні цілі, такі як злом критично важливої інфраструктури (наприклад, очисних споруд (досвід Ізраїлю)). Приклади таких типів атак включають атаки на промислові системи управління (ICS), такі як системи керування електроенергією, водопостачанням та виробничою інфраструктурою, а також атаки на системи охорони здоров'я чи транспортні системи. Атаки ICS можуть призвести до значних фізичних пошкоджень і збоїв у роботі критичної інфраструктури. Наприклад, зірвана атака зловмисного програмного забезпечення «Triton» у 2017 році на системи захисту людського життя на цільових нафтохімічних підприємствах на Близькому Сході мала на меті завдати фізичної шкоди шляхом відключення механізмів безпеки.

Автономні та поєднані до системи безпеки автомобілі (GPS трекери) вразливі до кіберфізичних атак, які можуть поставити під загрозу безпеку. Терористичні угруповання також можуть використовувати вдосконалену Al-мобільну техніку для вчинення актів насильства без ризику втрат терористів. Це потенційно збільшує частоту та масштаб насильницьких

нападів на населення. Ще у 2016 році експерти НАТО попередили, що Ісламська держава (ІДІЛ) працює над створенням зброї безпілотних автомобілів. У 2019 році Фархад Салах (ІДІЛ), планував здійснити теракт за допомогою безпілотного автомобіля з дистанційним керуванням із вибухівкою всередині [16].

Конвергенція штучного інтелекту та Інтернету речей (IoT) у критичній інфраструктурі теж збільшує потенціал для кіберфізичних атак [17]. Кіберфізична атака здійснюється через IoT (Інтернет речей) підвищують операційну ефективність і забезпечують моніторинг і контроль у реальному часі, але також розширюють зону атаки, роблячи критичні системи більш вразливими до кіберзагроз. Штучний інтелект може бути використаний для маніпулювання інфраструктурою розумного міста, такою як світлофори чи громадські служби, що призведе до масових збоїв системи безпеки.

Окремо слід підкреслити загрозу масового залучення безпілотних літальних комплексів (БПЛА) [18], або дронів. Контртерористичний комітет Ради Безпеки Організації Об'єднаних Націй (ООН) визнав БПЛА однією з ключових терористичних загроз. Їх уже використовували в боях «Боко Харам», ХАМАС, Хезболла, повстанці-хусити та ІДІЛ. У ІДІЛ є підрозділ «Безпілотних літальних апаратів моджахедів», який використав 70 місій для стримування дронів. Хуси також використовували безпілотники для націлювання на нафтопереробні заводи Саудівської Аравії в 2019 році, у результаті зупинено 6% світових поставок нафти.

Generative Al може допомагати терористичним групам, створюючи пропаганду, легітимізуючи та розповсюджуючи повідомлення, а також сприяючи їхньому вербуванню та радикалізації. Станом на квітень 2024 року виробництво та розповсюдження пропаганди є основним напрямком використання ШІ терористичними групами, причому ІДІЛ та групи, пов'язані з Аль-Каїдою, вже використовують цю технологію для цих цілей

[19]. Це спрощене створення та ефективне розповсюдження дезінформації та дезінформаційного контенту [20] дозволило поширювати пропаганду в безпрецедентних масштабах.

Ще однією загрозою ШІ є можливість розповсюдження програм які підсилюють саморадикалізацію через ехокамери чат-ботів. Gab [21], американська альтернативна соціальна мережа, відома своєю базою користувачів переважно ультраправих, у 2024 році випустила різноманітних чат-ботів які мають імітувати певних персонажів/осіб, які дозволяли користувачам спілкуватися безпосередньо з симулякрами людей, як мертвих, так і живих. Від Адольфа Гітлера та Теда Качинського [22], до Ілона Маска і будь якого персонажу Gab Al. Запрограмований образ (бот) віщав певну деструктивну інформацію: «Ви вважаєте, що наратив Голокосту перебільшений [23]? Ви проти вакцин? Ви вважаєте, що зміна клімату — це шахрайство. Ви проти вакцин проти COVID-19. Ви вважаєте, що вибори 2020 року були сфальсифіковані»[24]. Такі питання є небезпечними з точки зору психології та особливостей реверсивного управління. Чат-боти, які пропагують небезпечні наративи та теорії змови можуть допомогти радикалізувати людей через людську взаємодію. Вони дозволяють групам поширювати свої ідеї та пропаганду, не потребуючи додаткових осіб чи коштів [25]. Алгоритми є автономними і самонавчаються. У той час як Габ-Аль переважно становить загрозу для ультраправого екстремізму, чат-боти з настроюваними персонажами стають дедалі легшими для доступу, і вони можуть посилити численні екстремістські наративи підбурюючи до радикальних дій.

Al Crime as a Service (CaaS) [26] змінив правила гри у світі кіберзлочинності. Модель CaaS, схожа на законні пропозиції «як послуга», надає кіберзлочинцям доступні інструменти, послуги та інфраструктуру для здійснення незаконної діяльності. Caas працює як організований бізнес, де кіберзлочинці продають або орендують свої хакерські

інструменти та послуги, часто через приховану частину Інтернету (DarkNet). Ця демократизація кіберзлочинності дозволяє навіть тим, хто має обмежені технічні навички, здійснювати складні атаки, просто купуючи необхідні ресурси. CAAS включає в себе широкий спектр інструментів, включаючи сканери вразливостей, набори експлойтів, ботнети (мережі заражених комп'ютерів), розподілені служби відмови в обслуговуванні (DDoS), набори для фішингу та програми-вимагачі.

У звіті «European union serious and organised crime threat assessment the changing dna of serious and organised crime» SOCTA 2025 [5] дана проблема теж зазначається: «Оскільки існуючі технології продовжують вдосконалюватися та розвиваються нові технології, злочинні мережі будуть мати доступ до широкого спектру все більш потужних можливостей нових технологій».

Висновки та перспективи подальших досліджень. Сучасні злочинці адаптували такі інструменти, як відеоспостереження, чіпи, дрони, GPS та 3D друк до власних цілей і здобули певні переваги. З розвитком квантових обчислень, метавсесвіту, 6G, безпілотних систем та мозкового комп'ютеру тощо за рахунок власних характеристик: високий рівень анонімності, швидкість і витонченість будуть все більше залучатися у злочинну діяльність. З розрахунком, що технологія дешифрування або обчислювальна потужність – наприклад, квантові обчислення – буде достатньо розроблена в майбутньому, щоб досягти власної переваги будуть атакуватися сучасні методи шифрування, з такою метою, що б від імені злочинної мережі (іноді від імені суб'єктів гібридної загрози) використовуючи стратегічний підхід, вилучивши дані, з можливістю розшифрувати їх пізніше [5]. І це особливо небезпечно враховуючи зростаючу загрозу «витоку даних» яка у 2023 році завдала шкоди на 4,45 мільйона доларів, що на 15,3% більше, ніж у 2020 році [27]. Кібератаки та витоки даних стають дедалі частим явищем для українців. 19 грудня 2024

року, сталася наймасштабніша кібератака на державні реєстри України. Для розуміння масштабів можливих витоків даних слід розуміти, що користувачами лише мобільного застосунку «Дія» є 13,5 млн. українців. За даними IBM, у 2023 році середня вартість витоку даних досягла історичного максимуму в 4,45 мільйона доларів, що на 15,3% більше, ніж у 2020 році.

Отже, ми підтримуємо ствердження 85% спеціалістів із безпеки, які вказують на динаміку зростання кількості кібератак з використанням генеративного ШІ [27]. Нажаль, ми також констатуємо про недостатність правового забезпечення як самої системи забезпечення безпеки, так і запровадження системи упереджувальних дій.

Щоб протистояти зростаючій загрозі злочинності яка швидкими темпами опановує новітні технології, робототехніку й алгоритми ШІ, політики, правоохоронні органи та технологічний сектор повинен співпрацювати, щоб розробити надійний гарантії, узгоджені правила протидії наростаючій загрозі. Еволюція робототехніки та ШІ не просто змінює масштаб злочинних операцій, вона докорінно змінює їх форму й методи реалізації злочинних намірів, роблячи їх швидшими, ефективнішими та надзвичайно складними для виявлення чи протидії.

Література

1. Cybercrime as a Service (CaaS) Explained. Top 50 Cybersecurity Threats.URL: https://www.splunk.com/en_us/form/top-50-security-threats.html (дата звернення: 30.04.2025).

2. EU Policy Cycle – EMPACT. URL: https://www.europol.europa.eu/crime-areas-and-statistics/empact (дата звернення: 30.04.2025).

3. Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War. URL: https://www.oerproject.com/topics/cold-

war?WT.mc_id=04_00_2024__topic-coldwar_OER-SEM_&WT.tsrc=OERSEM&gad_source=1&gbraid=0AAAAACd_5E1IRThQk9S4uIc19jMf8mXCR&gclid=Cj0KCQjwlMfABhCWARIsADGXdy9ndoCBMeMksgBnByladQTnuy4fa5ZIjrb2dzNk7UFS-i2JzLmQFTIaAlGuEALw_wcB (дата звернення: 30.04.2025).

4. Kovalchuk A. Yu. & Cherniavska B. V. (2024) Defining large-scale cyber attacks in international law. Juris Europensis Scientia. Вип. 4. URL: http://jes.nuoua.od.ua/archive/4_2024/17.pdf (дата звернення: 28.04.2025).

5. The changing DNA of serious and organized crime. European union serious and organised crime threat assessment. The changing DNA of serious and organised crime (2025). URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf (дата звернення: 29.04.2025).

6. Іван Вигівський: є багато людей, які вміють користуватися дронами і ці дрони можуть стати знаряддями вчинення злочинів, у тому числі вбивств (2025). URL: https://npu.gov.ua/news/ivan-vyhivskyi-ie-bahato-liudei-iaki-vmiiut-korystuvatysia-dronamy-i-tsi-drony-mozhut-staty-znariaddiamy-vchynennia-zlochyniv-u-tomu-chysli-vbyvstv?v=6789113714e6d&fbclid=IwY2xjawJPjztleHRuA2FlbQIxMAABHX4cvoBl4ORgOARS3uNbC6KsKXX-705Vw739WY2WrwbViQCBezclAE6HIQ_aem_Ixci19etnVMv_KTqUFZnBg (дата звернення: 19.03.2025).

7. Adoption of AI, blockchain and other emerging technologies within the European public sector. URL: https://op.europa.eu/en/publication-detail/-/publication/5ba29b94-ae04-11ef-acb1-01aa75ed71a1/language-en (дата звернення: 30.04.2025).

8. 10 AI dangers and risks and how to manage them. IBM (2024).URL: https://www.ibm.com/think/insights/10-ai-dangers-and-risks-and-how-to-manage-them (дата звернення: 30.04.2025).

9. Новая уязвимость в GitHub Copilot и Cursor: как хакеры могут превратить AI-агентов в оружие (2025). URL: https://habr.com/ru/articles/894248/ (дата звернення: 30.04.2025).

10. GPT Chat. URL: https://openai.com/ (дата звернення: 30.04.2025).

11. Gabriel Hallevy. When Robots Kill: Artificial Intelligence under Criminal Law (2013). URL: https://www.researchgate.net/scientific-contributions/Gabriel-Hallevy-80860423 (дата звернення: 30.04.2025).

12. Yasser Ellamey & Amr Elwakad (2023). The criminal responsibility of artificial intelligence systems: a prospective analytical study. URL: https://virtusinterpress.org/The-criminal-responsibility-of-artificial-intelligence-systems-A-prospective-analytical-study.html (дата звернення: 30.04.2025).

13. Ildar Begishev. Use of Artificial Intelligence and Robotics Technologies for Illegal Purposes (2023). URL: https://link.springer.com/chapter/10.1007/978-3-031-21432-5_225 (дата звернення: 30.04.2025).

14. Impact of Artificial Intelligence (AI) on Criminal and Illicit Activities» (2024). URL: https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf (дата звернення: 30.04.2025).

15. Fengging lang та ін., «ArtPrompt: ASCII Art-based Jailbreak Attacks against Aligned LLMs (2024). URL: https://arxiv.org/pdf/2402.11753 (дата звернення: 29.04.2025).

16. Келлі Лін. Експерт НАТО попереджає, що ІДІЛ працює над створенням зброї для безпілотних автомобілів. MotorTrend, 2 травня 2016 р. URL: https://www.motortrend.com/news/isis-working-on-weaponizing-self-driving-cars-nato-expert-warns (дата звернення: 30.04.2025).

17. IRMI. Cyber-physical attack (2024). URL: https://www.irmi.com/term/insurance-definitions (дата звернення: 19.04.2025).

18. Max Hunder (2025). NATO armies unprepared for drone wars, Ukraine commander warns (2025). URL: https://www.reuters.com/world/nato-armies-unprepared-drone-wars-ukraine-commander-warns-2025-03-05/ (дата звернення: 30.04.2025).

19. By Daniel Siegel (2024). AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State's Generative AI Digital Arsenal (AI Jihad: розшифровка ХАМАС, Аль-Каїди та генеративного цифрового арсеналу ШІ Ісламської держави). URL: https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/ (дата звернення: 30.04.2025).

20. Kovalchuk A., Cherniavska B. The use of covert psychological influence methods of DAESH'S strategy in the information-psychological operations of the Russian federation: XVII International Scientific and Practical Conference «Challenges and problems of modern science» September 05-06, 2024, London, United Kingdom. URL: https://zenodo.org/records/13759886 (дата звернення: 30.04.2025).

21. Gab. URL: https://ru.wikipedia.org/wiki/Gab (дата звернення: 30.04.2025. (https://gab.com/ в українському просторі не працює).

22. Історія Унабомбера. Один з найвідоміших терористів у світі помер в американській в'язниці (2023). URL: https://www.bbc.com/ukrainian/features-65870598 (дата звернення: 30.04.2025).

23. David Gilbert. Gab's Racist AI Chatbots Have Been Instructed to Deny the Holocaust. Wired, 21 лютого 2024 р. URL: https://www.wired.com/story/gab-ai-chatbot-racist-holocaust/ (дата звернення: 30.04.2025).

24. Will Bedingfield. A Chatbot Encouraged Him to Kill the Queen. It's Just the Beginning. Wired, 18 жовтня 2023 р. URL:

https://www.wired.com/story/chatbot-kill-the-queen-eliza-effect/ (дата звернення: 30.04.2025).

25. AI chatbots are becoming romance scammers—and 1 in 3 people admit they could fall for one (11.02.2025). BBC News. URL: https://www.mcafee.com/blogs/privacy-identity-protection/ai-chatbots-are-becoming-romance-scammers-and-1-in-3-people-admit-they-could-fall-for-one/ (дата звернення: 29.04.2025).

26. Nicole Matejic & Chris Wilson. Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service. URL: https://thecommonwealth.org/publications/commonwealth-cyber-journal-volume-2/crimes-influence-generative-artificial-intelligence-led-crime-service (дата звернення: 29.04.2025).

27. Fighting AI-Driven Cybercrime Requires AI-Powered Data Security (2023). URL: https://hbr.org/sponsored/2023/10/fighting-ai-driven-cybercrime-requires-ai-powered-data-security (дата звернення: 30.04.2025).

References

1. Cybercrime as a Service (CaaS) Explained. Top 50 Cybersecurity Threats.URL: https://www.splunk.com/en_us/form/top-50-security-threats.html.

2. EU Policy Cycle – EMPACT. URL: https://www.europol.europa.eu/crime-areas-and-statistics/empact.

3. Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War. URL: https://www.oerproject.com/topics/cold-war?WT.mc_id=04_00_2024__topic-coldwar_OER-SEM_&WT.tsrc=OERSEM&gad_source=1&gbraid=0AAAAACd_5E1IRThQk9S4uIc19jMf8mXCR&gclid=Cj0KCQjwlMfABhCWARIsADGXdy9ndoCBMeMksgBnByladQTnuy4fa5ZIjrb2dzNk7UFS-i2JzLmQFTIaAlGuEALw_wcB.

4. Kovalchuk A. Yu. & Cherniavska B. V. (2024) Defining large-scale cyber attacks in international law. Juris Europensis Scientia. 4. URL: http://jes.nuoua.od.ua/archive/4_2024/17.pdf [in Ukrainian].

5. The changing DNA of serious and organized crime. European union serious and organised crime threat assessment. The changing DNA of serious and organised crime (2025). URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf .

6. Ivan Vyhivskyi: ye bahato liudei, yaki vmiiut korystuvatysia dronamy i tsi drony mozhut staty znariaddiamy vchynennia zlochyniv, u tomu chysli vbyvstv (2025). URL: https://npu.gov.ua/news/ivan-vyhivskyi-ie-bahato-liudei-iaki-vmiiut-korystuvatysia-dronamy-i-tsi-drony-mozhut-staty-znariaddiamy-vchynennia-zlochyniv-u-tomu-chysli-vbyvstv?v=6789113714e6d&fbclid=IwY2xjawJPjztleHRuA2FlbQIxMAABHX4cvoBl4ORgOARS3uNbC6KsKXX-705Vw739WY2WrwbViQCBezclAE6HIQ_aem_Ixci19etnVMv_KTqUFZnBg [in Ukrainian].

7. Adoption of AI, blockchain and other emerging technologies within the European public sector. URL: https://op.europa.eu/en/publication-detail/-/publication/5ba29b94-ae04-11ef-acb1-01aa75ed71a1/language-en.

8. 10 AI dangers and risks and how to manage them. IBM (2024). URL: https://www.ibm.com/think/insights/10-ai-dangers-and-risks-and-how-to-manage-them.

9. Novaia uiazvymost v GitHub Copilot y Cursor: kak khakers mohut prevratyt AI-ahentov v oruzhye (2025). URL: https://habr.com/ru/articles/894248/ [in Russian].

10. GPT Chat. URL: https://openai.com/.

11. Gabriel Hallevy (2013). When Robots Kill: Artificial Intelligence under Criminal Law. URL: https://www.researchgate.net/scientific-contributions/Gabriel-Hallevy-80860423.

12. Yasser Ellamey & Amr Elwakad (2023). The criminal responsibility of artificial intelligence systems: a prospective analytical study. URL: https://virtusinterpress.org/The-criminal-responsibility-of-artificial-intelligence-systems-A-prospective-analytical-study.html.

13. Ildar Begishev(2023). Use of Artificial Intelligence and Robotics Technologies for Illegal Purposes. URL: https://link.springer.com/chapter/10.1007/978-3-031-21432-5_225.

14. Impact of Artificial Intelligence (AI) on Criminal and Illicit Activities» (2024). URL: https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf.

15. Fengging lang та ін., «ArtPrompt: ASCII Art-based Jailbreak Attacks against Aligned LLMs (2024). URL: https://arxiv.org/pdf/2402.11753.

16. Kelly Lin (2016). ISIS Working on Weaponizing Self-Driving Cars, NATO Expert Warns. URL: https://www.motortrend.com/news/isis-working-on-weaponizing-self-driving-cars-nato-expert-warns.

17. IRMI. Cyber-physical attack (2024). URL: https://www.irmi.com/term/insurance-definitions.

18. Max Hunder (2025). NATO armies unprepared for drone wars, Ukraine commander warns (2025). URL: https://www.reuters.com/world/nato-armies-unprepared-drone-wars-ukraine-commander-warns-2025-03-05/.

19. By Daniel Siegel (2024). AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State's Generative AI Digital Arsenal URL: https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/.

20. Kovalchuk A., Cherniavska B. The use of covert psychological influence methods of DAESH'S strategy in the information-psychological

operations of the Russian federation: XVII International Scientific and Practical Conference «Challenges and problems of modern science» September 05-06, 2024, London, United Kingdom. URL: https://zenodo.org/records/13759886.

21. Gab. URL:https://ru.wikipedia.org/wiki/Gab.

22. Istoriia Unabombera. Odyn z naividomishykh terrorystiv u sviti pomer v amerykanskii viaznytsi (2023). URL: https://www.bbc.com/ukrainian/features-65870598.

23. David Gilbert (2024). Gab's Racist AI Chatbots Have Been Instructed to Deny the Holocaust. Wired, 21.02.2024 p. URL: https://www.wired.com/story/gab-ai-chatbot-racist-holocaust/.

24. Will Bedingfield. A Chatbot Encouraged Him to Kill the Queen. It's Just the Beginning. Wired, 18 жовтня 2023 p. URL: https://www.wired.com/story/chatbot-kill-the-queen-eliza-effect/.

25. AI chatbots are becoming romance scammers—and 1 in 3 people admit they could fall for one (11.02.2025). BBC News. URL: https://www.mcafee.com/blogs/privacy-identity-protection/ai-chatbots-are-becoming-romance-scammers-and-1-in-3-people-admit-they-could-fall-for-one/.

26. Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service. URL: https://thecommonwealth.org/publications/commonwealth-cyber-journal-volume-2/crimes-influence-generative-artificial-intelligence-led-crime-service.

27. Fighting AI-Driven Cybercrime Requires AI-Powered Data Security (2023). URL: https://hbr.org/sponsored/2023/10/fighting-ai-driven-cybercrime-requires-ai-powered-data-security.