

РОЛЬ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОНІЙ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ТА ОБОРОНОЗДАТНОСТІ УКРАЇНИ

THE ROLE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN LAW ENFORCEMENT ACTIVITIES AND ENSURING THE SECURITY AND DEFENSE CAPACITY OF UKRAINE

Шевчук В.М., д.ю.н., професор, заслужений юрист України,
завідувач кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого,
провідний науковий співробітник

*Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса
Національної академії правових наук України*

Досліджено актуальні проблеми значення та ролі технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України в контексті воєнної російської агресії, цифровізації та європейської інтеграції. Визначено та проаналізовано основні тенденції формування та розвитку концептуальних підходів застосування можливостей технологій штучного інтелекту у підвищенні ефективності та оптимізації правоохоронної діяльності в секторі безпеки та оборони нашої країни в реаліях сьогодення, окреслено перспективні напрями наукових досліджень у цій царині знань. Обґрунтовано появу та формування нових напрямів криміналістики, обумовлених науково-технічним прогресом, процесами європізації, технологізації та цифровізації, що зумовлює появу нових завдань криміналістики та необхідність пошуку нових засобів та технологій, спрямованих на підвищенні результативності правоохоронної діяльності в сфері забезпечення національної безпеки та обороноздатності України.

Зазначено, що важливо враховувати сучасні тенденції розвитку юридичної науки, криміналістики та судової експертології, пов'язані з формуванням окремих нових напрямів, зокрема медичної, ядерної, цифрової, воєнної криміналістики. В умовах війни в Україні особливої актуальності та значимості набувають проблеми дослідження криміналістичного забезпечення розслідування воєнних злочинів та сучасних реалій значного поширення застосування цифрових технологій у слідчій, судовій та експертній діяльності задля забезпечення безпеки та оборони нашої держави.

Обґрунтовано, що значною мірою успіх реалізації завдань в секторі безпеки та оборони України тісно пов'язаний із розробленням та впровадженням новітніх цифрових технологій штучного інтелекту. Вирішення таких завдань може здійснюватися за певними напрямами, які окреслені та розглянуті в запропонованому дослідженні.

Вбачається, що контроль за створенням та використанням ШІ необхідно здійснювати не тільки суто технічним регулюванням, а й шляхом формування комплексного вітчизняного законодавства. Європейський підхід має визначити концептуально нові засади розвитку оборонних технологій, зростання конкурентоспроможності озброєнь українського виробництва, посилить обороноздатність і національну безпеку, сприятиме економічному зростанню країни та відновленню об'єктів держави, знищених та пошкоджених в результаті воєнної агресії РФ. Виокремлено та висвітлено позитивні та негативні аспекти застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України в умовах воєнного стану та повоєнний період. Розглянуто та проаналізовано найбільш актуальні та перспективні проблеми дослідження означеної проблематики.

Ключові слова: правоохоронна діяльність, криміналістичні засоби протидії, спеціальні знання, штучний інтелект, судова експертиза, кримінальне провадження, криміналістика, воєнні злочини, цифрові технології, методика розслідування, криміналістичні інновації.

Current problems of the importance and role of artificial intelligence technologies in law enforcement activities and ensuring the security and defense capability of Ukraine in the context of Russian military aggression, digitalization and European integration are studied. The main trends in the formation and development of conceptual approaches to the application of artificial intelligence technologies to increase the efficiency and optimization of law enforcement activities in the security and defense sector of our country in today's realities have been identified and analyzed, and promising directions of scientific research in this field of knowledge have been outlined. The emergence and formation of new areas of criminalistics due to scientific and technological progress, processes of Europeanization, technologization and digitalization, which leads to the emergence of new tasks of criminalistics and the need to find new means and technologies aimed at increasing the effectiveness of law enforcement activities in the field of ensuring national security and defense capability of Ukraine, are substantiated.

It is noted that it is important to take into account the modern trends in the development of legal science, criminalistics and forensic expertise related to the formation of certain new directions, in particular, medical, nuclear, digital, and military criminalistics. In the conditions of the war in Ukraine, the problems of the study of forensic support for the investigation of war crimes and the modern realities of the significant spread of the use of digital technologies in investigative, judicial and expert activities to ensure the security and defense of our state become especially relevant and important. It is substantiated that to a large extent the success of the implementation of tasks in the security and defense sector of Ukraine is closely related to the development and implementation of the latest digital technologies of artificial intelligence. Solving such tasks can be carried out in certain directions, which are proposed and considered in the proposed study.

It is believed that control over the creation and use of AI must be carried out not only by purely technical regulation, but also by forming comprehensive domestic legislation. The European approach should define conceptually new principles for the development of defense technologies, increase the competitiveness of Ukrainian-made weapons, strengthen defense capabilities and national security, contribute to the economic growth of the country and the restoration of state facilities destroyed and damaged as a result of the military aggression of the Russian Federation. The positive and negative aspects of the use of AI in the field of ensuring national security and defense capability of Ukraine in the conditions of martial law and the post-war period are highlighted and highlighted. Considered and analyzed the most relevant and promising problems of the research of the specified problem.

Key words: law enforcement activity, criminalistic countermeasures, expertise, Artificial Intelligence, forensic examination, criminal proceedings, criminalistics, war crimes, digital technologies, investigation methodology, criminalistic innovations.

Постановка проблеми. В реаліях сьогодення Україна зіштовхнулася із новими викликами та загрозами, які суттєво вплинуло на усі сфери нашого життя. Передусім, для України та усього світу серед таких викликів та глобальних загроз ХХІ століття безпрецедентним

та шокуючим стала воєнна агресія РФ і повномасштабне вторгнення російських військ на територію нашої держави 24 лютого 2022 року [1, с. 47]. Злочини, що вчиняються військовими РФ на території нашої держави, є надзвичайно масштабними і їх фіксація, документування

та розслідування передбачає дослідження значного обсягу подій, збирання великого масиву доказової інформації, допиту величезної кількості свідків та потерпілих, залучення експертів та проведення судових експертиз, тобто застосування спеціальних знань та засобів сучасної криміналістики [2, с. 582–604].

Серед таких викликів та глобальних загроз специфічного значення набувають технології штучного інтелекту, цифрові технології, та їх використання у злочинній діяльності [3, с. 12–46]. Очевидно, що у сучасних умовах цифрова реальність сьогодення нині тісно пов'язана із появою *нових форм злочинності* – кіберзлочинів, інформаційного шахрайства, проведення кібероперацій РФ, вчинення великої кількості кібератак на підприємства та установи, в тому числі, й державні бази даних. У сучасних умовах цифровізації злочинці нині досить активно використовують найсучасніші та найпередовіші технології. Значного поширення набувають вірусні кіберзагрози, біотероризм, кібершахрайство, сьогодні воєнні злочини вчиняються із використанням технологій ШІ [4, с. 199]. Глобальні загрози пов'язані із застосуванням зброї масового знищення [5, с. 208–216].

Безумовно, що такі виклики зумовили необхідність вирішення низки завдань, що потребують застосування сучасних досягнень науки й техніки та використання інноваційних підходів у протидії злочинності й забезпеченні безпеки та обороноздатності України. Тому одним із пріоритетних напрямків підвищення ефективності протидії сучасній злочинності та забезпеченні безпеки та оборони нашої держави є застосування інноваційних засобів, систем та методів, які тісно пов'язані із активним впровадженням технологій штучного інтелекту в умовах воєнного стану.

Реалії сьогодення, пов'язані із збройною російською агресією України, активними процесами цифровізації та європеїзації нашої держави, визначають сучасні тенденції розвитку юридичної науки, у тому числі й криміналістики щодо формування перспективних інноваційних напрямків застосування криміналістичних знань. За таких умов особливої актуальності набувають проблеми активізації розроблення та впровадження інноваційних підходів у криміналістиці, новітніх технологій та криміналістичних засобів та їх активне використання у слідчій (детективній), судовій та експертній діяльності у протидії злочинності та забезпеченні безпеки та обороноздатності нашої держави.

Аналіз останніх досліджень та публікацій. Вагомий внесок у дослідження ролі технологій штучного інтелекту в судочинстві, правоохоронній діяльності, при розслідуванні окремих видів кримінальних правопорушень, воєнних злочинів та їх значення для підвищення ефективності органів кримінальної юстиції в умовах воєнного стану здійснили такі науковці, як: Л. Аркуша, О. Ващук, В. Гусева, В. Журавель, І. Когутич, В. Коновалова, Є. Лук'янчиков, М. Р. Степанюк, В. Тищенко, Ю. Черноус, Д. Цехан, В. Шевчук, В. Шепітько, В. Юсупов та ін. Певна увага приділялась і дослідженню окремих проблем застосування спеціальних технологій штучного інтелекту в судочинстві, правоохоронній діяльності, при розслідуванні окремих видів кримінальних правопорушень: Г. Авдєєва [13], Ю. Балтрунене [16], О. Бугера [16], О. Дуфенюк [1], С. Матульєне [3], В. Мисливий [14], Т. Павленко [26], Н. Пацурія [25], К. Юргаєва [18] та ін.

Водночас, проблематика дослідження ролі технологій штучного інтелекту у правоохоронній діяльності, забезпеченні безпеки та обороноздатності України в сучасних реаліях воєнного часу, на сьогодні залишається недо-дослідженою. Вбачається, що значення цієї проблематики для підвищення ефективності реалізації правоохоронної діяльності для забезпечення безпеки та оборони нашої країни в умовах воєнного стану є сьогодні досить актуальними. Усе викладене свідчить про те, що обрана тематика

є затребувана практикою і сьогодні, як ніколи, потребує проведення спеціальних комплексних наукових досліджень у цій царині знань.

Метою статті є дослідження та аналіз ролі технологій штучного інтелекту у правоохоронній діяльності, у забезпеченні безпеки та обороноздатності України в сучасних реаліях, розроблення рекомендацій щодо підвищення ефективності та результативності такої роботи, визначення перспективних напрямів досліджень означеної проблематики.

Виклад основного матеріалу. В сучасних умовах головним завданням криміналістики є розроблення та застосування засобів, прийомів та методів, що дозволяють збирати, досліджувати, використовувати доказову інформацію в умовах війни та глобальних загроз. За таких обставин постає необхідність криміналістичного забезпечення розслідування воєнних злочинів, що вчиняються військовими РФ, для того щоб задіяти всі доступні національні та міжнародні правові механізми для притягнення до кримінальної відповідальності усіх винних в цій війні [6, с. 387]. Крім цього, потребують особливої уваги розроблення інноваційних підходів до розслідування злочинів у кіберпросторі, застосування цифрових технологій у виявленні, фіксації, розслідуванні кримінальних правопорушень, воєнних злочинів, злочинів геноциду, фактів застосування зброї масового знищення, та інших злочинів, що вчиняються російськими окупаційними військами в Україні.

За офіційними статистичними даними Офісу Генерального прокурора серед злочинів, вчинених в період повномасштабного вторгнення РФ, найпоширенішими є такі: а) злочини агресії та воєнні злочини – зареєстровано (станом на 18.04.2024 р.) – 134453 злочинів; б) злочинам проти національної безпеки – 17812 злочинів; в) злочини проти дітей – загинули 551 дітей, поранено 1389 дітей; 4) магістральна справа щодо агресії РФ – 698 підозрюваних представники військово політичного керівництва РФ (військове командування, посадовці, міністри, депутати, керівники правоохоронних органів та ін.) [7]. Наразі серед офіційної статистики Офісу ГПУ є інформація про 19,5 тисяч українських дітей, які були депортовані окупантами до РФ. Очевидно, що ця цифра не є остаточною.

Вбачається, що трансформація злочинності в Україні під час війни значно вплинули на зміну пріоритетів завдань криміналістики та особливості формування і застосування криміналістичних знань [8]. У таких умовах мова йде про формування та необхідність розроблення нових напрямів у криміналістиці, зокрема, криміналістичної інноватики, стратегії криміналістики, цифрової криміналістики, воєнної криміналістики та новітніх криміналістичних технологій тощо [9, с. 73–77]. Очевидно, що серед нових напрямів дослідження та використання технологій штучного інтелекту у правоохоронній діяльності щодо протидії злочинності і забезпеченні безпеки та обороноздатності нашої держави є важливим інструментом підвищення ефективності роботи органів правопорядку у цій царині знань.

Вбачається, що штучний інтелект – це система, що поводить розумно, аналізуючи своє оточення й ухвалюючи доволі автономні рішення для досягнення мети [10, с. 203]. Системи штучного інтелекту можуть бути заснованими виключно на програмному забезпеченні та працювати у віртуальному світі (наприклад, голосові синтезатори, програмне забезпечення для аналізу відеозаписів, пошукові системи, системи розпізнавання мовлення й обличчя) або можуть бути інтегрованими в апаратне забезпечення (наприклад, робототехніка, безпілотні транспортні засоби, дрони чи об'єкти мережі «Інтернету речей» (англ. *Internet of Things, IoT*)). Сучасна людина використовує штучний інтелект щодня – наприклад, для

перекладу текстів, створення субтитрів для відео або блокування електронних листів (спаму). Тому штучний інтелект як останнє наукове досягнення потребує нових криміналістичних ідей і методів, пов'язаних із його використанням у боротьбі зі злочинністю [11].

Розроблення та впровадження новітніх цифрових технологій та ШІ у правоохоронній діяльності щодо протидії злочинності може здійснюватися за такими напрямками: 1) інформаційно-аналітичне забезпечення правоохоронної діяльності; 2) інформаційно-довідкове забезпечення правоохоронної діяльності; 3) створення спеціалізованих інформаційних інтелектуальних систем оперативного-розшукового призначення; 4) формування та розвиток інтелектуальних систем відеоспостереження; 5) охорона об'єктів; 6) створення відомчих спеціалізованих інтелектуальних інформаційних систем; 7) впровадження інтелектуальних інформаційних освітніх систем; 8) запровадження інформаційно-телекомунікаційної системи досудового [12, с. 135–140].

Останнім часом застосування технологій штучного інтелекту у практиці правоохоронної діяльності набуло неабиякої актуальності. Передусім, це обумовлено необхідністю протистояти злочинням, які дедалі частіше використовують найсучасніші інноваційні технології й досягнення четвертої промислової революції, зокрема: моделі блокчейну, дрони, робототехніку та ін. [13]. Правоохоронна діяльність – це діяльність органів державної влади спрямована на попередження і припинення правопорушень та притягнення правопорушників до юридичної відповідальності, шляхом застосування заходів фізичного і юридичного впливу. При цьому варто враховувати, що серед видів правоохоронної діяльності виокремлюються такі: забезпечення громадського порядку, оперативно-розшукова діяльність, досудове розслідування. Крім цього, до правоохоронної діяльності можна віднести: а) діяльність із забезпечення охорони учасників кримінального судочинства; б) діяльність органів прокуратури, поліції, пенітенціарних органів тощо; в) діяльність із виявлення, запобігання та розслідування кримінальних правопорушень, оскільки і оперативно-розшукова діяльність забезпечує ці види діяльності; г) діяльність із захисту національної безпеки, державного кордону та правопорядку на всіх рівнях і всіма органами держави та певними службовими особами.

Кожен із названих напрямів правоохоронної діяльності має свої власні суттєві особливості, специфічні ознаки і в свою чергу можливості застосування технологій штучного інтелекту, врахування та грамотне врахування яких дає фундамент формування та забезпечення ефективної державної військово-промислової політики України в сучасних умовах воєнного часу.

Правоохоронні органи України, суттєво підвищуючи ефективність своєї роботи й оптимізуючи розв'язання завдань із протидії злочинності, активно послуговуються такими технологіями штучного інтелекту: 1) ідентифікація російських окупантів завдяки розпізнаванню облич за соціальними мережами й записами камер відеоспостереження; 2) убезпечення дорожнього руху, виявлення та фіксування порушень правил дорожнього руху [14, с. 55–60]; 3) використання безпілотників для протидії незаконному обігу вогнепальної зброї й наркотиків [15, с. 105], для проведення військових операцій і збирання доказової інформації в умовах війни й ведення активних бойових дій із метою фіксування воєнних злочинів; 4) попередження кримінальних правопорушень із використанням інтелектуальних систем безпеки з різними пристроями (датчиками) збирання інформації [16, с. 85]; 5) прогнозування кримінальних правопорушень методом картографування злочинності (за допомогою якого прогнозують місцеву злочинність та індивідуальну злочинну поведінку) [17, с. 66–72].

Для прикладу варто зауважити, що завдяки технологіям штучного інтелекту можна складати обґрунтовані

прогнози щодо темпоральних, територіальних і якісних показників злочинності, які оптимізуватимуть використання правоохоронними органами наявних ресурсів і виконання поліцейських функцій [18, с. 99–104]. Крім того, за допомогою технологій штучного інтелекту можна ідентифікувати російських військових за соціальними мережами й записами камер відеоспостереження. Штучний інтелект руйнує міфи про нібито невмирущих солдатів так званої «спецоперації», розпізнаючи обличчя трупів окупантів, відшуковуючи їх у соціальних мережах і за допомогою автодозвонів повідомляючи родичів про їхню смерть. Міністерство оборони України застосує технологію розпізнавання обличчя *Clearview AI* для боротьби з дезінформацією, розпізнавання й ідентифікації загиблих і воєнних злочинців [19].

Технології штучного інтелекту досить активно застосовуються в секторі безпеки і оборони. Передусім це 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 і оборони України.

Сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки. Функції та повноваження складових сектору безпеки і оборони визначаються законодавством України. До складу сектору безпеки і оборони входять: Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транс-порту, 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, Управління державної охорони України. Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику [20, с. 6–8].

Очевидно, що кожен із названих суб'єктів сектору безпеки і оборони України мають свої повноваження, функції особливості діяльності, що суттєво впливає на можливості та перспективи застосування технологій штучного інтелекту. Тому в сучасних умовах використання ШІ у роботі правоохоронних органів є актуальними та затребуваними практикою. Розглянемо їх.

Розпізнавання обличчя. Аналіз міжнародного і вітчизняного досвіду свідчить про те, що правоохоронці вже досить давно використовують програмні комплекси, які дозволяють автоматично розпізнавати обличчя, порівнюючи із системами відеоспостереження та інформацією яка вже є у базі. При цьому висока точність розпізнавання досягається завдяки застосуванню технологій індексу за біометричними параметрами обличчя. Правоохоронці зазначають, що майже 30% кримінальних правопорушень виявлено та розкрито завдяки таким відеокерам.

Більше того, за допомогою технологій штучного інтелекту здійснюється ідентифікація російських військових окупантів у соціальних мережах та камерах відеозапису. За інформацією Міністерства цифрової трансформації України, технології штучного інтелекту цього відомство

вже зчитували обличчя, коли громадяни України підписувались в мобільному додатку «Дія». Такі технології розпізнають обличчя трупів окупантів та знаходять їх в соцмережах, а автодозвони повідомляють родичів про їхню смерть. Міноборони України активно використовує технологію розпізнавання обличчя «Clearview AI», щоб розпізнавати російських нападників, боротися з дезінформацією, ідентифікувати загиблих та воєнних злочинців-окупантів. У воєнних реаліях повномасштабної військової агресії РФ на території України інструменти цифрової криміналістики значно допомагають у виявленні, розкритті та розслідуванні воєнних злочинів.

Забезпечення безпеки на дорогах. Фіксація даних щодо правопорушень на дорогах реалізується за допомогою комплексів автоматичної фіксації, а саме спеціальних технічних засобів, укомплектованих функціями фото- і відеозапису, що надає можливість в автоматичному режимі здійснювати виявлення та документування в базах даних фактичних подій, які містять ознаки адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху. Установлення стаціонарних технічних засобів здійснюється на аварійно-небезпечних місцях та місцях концентрації дорожньо-транспортних пригод, автомобільних доріг загального користування, державного та місцевого значення, вулиць і доріг у містах та інших населених пунктах за погодженням із відповідним уповноваженим підрозділом Національної поліції. Так, в Україні ГУ Національної поліції у Вінницькій області запровадило в свою роботу безпечний проект «Vezha». Система відрізняє номерні знаки понад 70 країн, а також визначає марку, модель на колір авто з точністю 95%. Аналізує траєкторію авто та будує його маршрут. Зберігає дату і час, коли авто було на певній ділянці. В систему можна завантажити базу даних номерів, і якщо система фіксує один з номерів з бази на мапі – одразу надсилає про це сповіщення. Модуль розпізнавання номерних знаків допомагає у пошуках розшукуваних авто, перехопленнях і затримання правопорушників.

Використання безпілотників. Сьогодні в реаліях військового часу в Україні найширша сфера застосування БПЛА. За їх допомогою здійснюється протидія незаконному обгіг вогнепальної зброї та боєприпасів, наркозлочинності в сучасних умовах. Також безпілотники можуть виявляти незаконні рубки лісу, знаходити лісові пожежі, фіксувати незаконний видобуток корисних копалин, допомагати шукати заблукалих в лісі, горах, виявляти ділянки, засіяні конопами. Національна поліція України проводить роботу по формуванню спецгруп аеророзвідки у кожному регіоні країни.

Попередження та профілактика кримінальних правопорушень. Одним із поширених способів використання штучного інтелекту для профілактики та запобігання вчинення кримінальних правопорушень є задіяння так званих інтелектуальних систем безпеки з різноманітними пристроями (датчиками) збору інформації, насамперед, відеокамерами високої роздільної здатності. Модернізовані камери зі штучним інтелектом можуть розпізнавати людей, автомобілі, зброю і навіть підозрілу поведінку. Зокрема, технологічна компанія Coban Technologies аносувала запуск модернізованої версії камер з штучним інтелектом для поліцейських автомобілів. Камери реагують набагато швидше за людей, вони ідентифікують інші автомобілі, перехожих та водіїв, а також можуть визначити підозрілу поведінку. Coban Technologies має намір перетворити свій проект на цілу платформу, що дозволить іншим розробникам вдосконалювати камеру, наприклад, за допомогою спеціального додатку, що розпізнає зброю. Існуюча версія смарт-камери розпізнає об'єкти лише на записаному нею відеопотоці. Розробники повідомляють, що в перспективі буде створена камера, яка аналізуватиме поведінку людей безпосередньо на вулицях в режимі онлайн. Однак

360-градусний огляд кожному поліцейському автомобілю зможуть забезпечити 6 камер Coban Technologies. Відомо, що в Україні також офіційно використовується програмне забезпечення з елементами ШІ «Касандра», яке аналізує можливість повторного порушення закону злочинцем. Насьогодні цей напрямок застосування штучного інтелекту є досить перспективним.

Прогнозування кримінальних правопорушень. Останнім часом дослідження фахівців у царині наукових знань новітніх цифрових технологій показують, що штучний інтелект 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 технології ШІ можуть створюватися обґрунтовані прогнози щодо якісних і кількісних показників злочинності [21, с. 134–138].

Вбачається, що у реаліях військової агресії інструменти цифрової криміналістики істотно сприяють виявленню, розкриттю та розслідуванню воєнних злочинів. Практика показує, що основними напрямками використання ШІ є такі: 1) аналіз супутникових знімків; 2) аналіз відео- та фотоматеріалів; 3) обробка аудіоматеріалів; 4) аналіз соціальних мереж; 5) аналіз даних з медичних закладів; 6) розпізнавання обличчя; 7) аналіз текстової інформації. Ця проблематика має бути врахована при формуванні програм, навчальних дисциплін і удосконаленні методики викладання криміналістики у сучасних умовах [22]. Крім цього, необхідно відстоювати тезу про те, що вивчення криміналістики в контексті сучасних наукових знань є обов'язковим для підготовки майбутніх правників [23, с. 77].

Штучний інтелект відіграє важливу роль у забезпеченні безпеки та обороноздатності України. Безпечення безпекової ситуації, обороноздатності та безпекового середовища в державі є одним із головних завдань, яке поставало перед Україною впродовж її багатовікової історії. Повномасштабна збройна агресія РФ проти України оголила численні загрози, що виникли не тільки перед нашою державою, а й перед всією світовою системою безпеки в цілому [24]. Тому забезпечення національної безпеки та оборони України має стати головним пріоритетом діяльності України та військово-політичного керівництва держави.

Важливо зауважити, що розроблення правового регулювання застосування технологій ШІ наразі відбувається вкрай повільно стосовно стрімкого розвитку цифрових технологій, які одночасно охоплюють усі сфери суспільних відносин. Тому контроль за створенням та використанням ШІ необхідно здійснювати не тільки суто технічним регулюванням (вимоги, технічні стандарти, регламенти, оцінки відповідності технічним стандартам, контроль відповідності вимогам технічних регламентів, етичних стандартів), а й шляхом формування комплексного законодавства [25, с. 68–78]. Більше того, що триваюча російська військова агресія змушує по-новому осмислити місію і завдання національного ОПК в сучасних реаліях. Відтворення тенденцій розвитку озброєних стандартів НАТО в ОПК України має визначити концептуально нові засади

розвитку оборонних технологій, зростання конкурентоспроможності озброєнь українського виробництва, посилить обороноздатність і безпеку, сприятиме економічному зростанню країни [26, с. 41–47].

Європейський напрям цифровізації суспільства та розвитку і поширення ІІТ підтриманий Україною на законодавчому рівні. Сьогодні в нашій країні сформовано бачення напряму розвитку спеціального законодавства застосування технологій ІІТ на основі існуючих оборонних та безпекових потреб. Проте цілісний стратегічний документ, як-то *Стратегія розвитку ІІТ у сфері забезпечення національної безпеки та обороноздатності України*, на жаль, відсутній, що потребує негайного усунення.

Вбачається, що контроль за створенням та використанням ІІТ необхідно здійснювати не тільки суто технічним регулюванням (вимоги, технічні стандарти, регламенти, оцінки відповідності технічним стандартам, контроль відповідності вимогам технічних регламентів, етичних стандартів), а й шляхом формування комплексного законодавства. Більше того, що триваюча російська військова агресія змушує по-новому осмислити завдання національного ОПК в сучасних воєнних реаліях. Європейський підхід має визначити концептуально нові засади розвитку оборонних технологій, зростання конкурентоспроможності озброєнь українського виробництва, посилить обороноздатність і національну безпеку, сприятиме економічному зростанню країни та відновленню об'єктів держави, знищених та пошкоджених в результаті воєнної агресії РФ.

Вивчення фахової літератури дає можливість виокремити позитивні та негативні аспекти застосування ІІТ у сфері забезпечення національної безпеки та обороноздатності України в умовах воєнного стану та повоєнний період.

Позитивним є, зокрема: а) підвищення ефективності – ІІТ може допомогти в зборі та аналізі великих обсягів даних, що забезпечує більш швидкий та точний аналіз інформації, скорочуючи час, необхідний для прийняття рішення; б) мінімізація ризиків – застосування ІІТ може допомогти у попередженні катастроф та мінімізації ризиків для військового персоналу, що забезпечує безпеку та захист держави; в) забезпечення безпеки – ІІТ може бути використаний для забезпечення безпеки країни, а саме, для забезпечення контролю над в'їздом та виїздом на кордоні, для виявлення та запобігання терористичним актам і злочинам; г) автоматизація процесів – ІІТ може допомогти в автоматизації багатьох процесів у сфері оборони, що зменшує ризик помилок та підвищує ефективність; д) удосконалення озброєння – ІІТ може бути використаний для розроблення та вдосконалення зброї, що забезпечує перевагу військам на полі бою. ІІТ може бути використаний для створення систем розвідки та контролю, які можуть виявляти загрози національній безпеці та вживати заходів для їх запобігання [25, с. 68–78].

Визначаючи переваги використання ІІТ для розвитку обороноздатності країн світу, необхідно враховувати, що надмірна залежність від систем ІІТ призведе до появи нових значних загроз і невирішених питань для подальших досліджень. Крім цього, значний вплив на формування та розвиток військового потенціалу матиме ІІТ, вбудований у супутні технології, такі як: ядерні, аерокосмічні, кібернетичні, технології розробки нових матеріалів та біотехнології; віртуальна реальність; квантові обчислення; автономність, моделювання, клауди; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних. Ці наслідки матимуть такий самий стратегічний вплив на зміну у військових технологіях, зокрема й упровадження ядерної зброї. ІІТ також може бути застосований для оптимізації військових операцій, що дає змогу зменшити ризики для життя військових, підвищити ефективність воєнних дій, у аеророзвідці, у використанні БПЛА тощо [27, с. 17–26].

Одночасно, вбачається, що разом з перевагами, ІІТ може становити загрозу національній безпеці та обороноздатності нашій країні, оскільки країна-агресор може використовувати ІІТ для вчинення воєнних злочинів, кібератак, що можуть негативно впливати на національну безпеку. В сучасних реаліях існує також ризик, що й інші держави можуть використовувати ІІТ для проведення кібершпигунства та кібератак на інфраструктуру країни. Більше того, ІІТ може порушувати етичні принципи та права людини, а використання автономної зброї, керованої ІІТ, може створити ризики для безпеки і стати причиною аварій тощо.

Проведений аналіз дає підстави зазначити, що задля забезпечення національної безпеки та обороноздатності України в умовах воєнного стану та повоєнний період необхідно розробляти та впроваджувати у національне законодавство найкращі світові практики. Такі підходи мають враховувати потенційні можливості та загрози ІІТ і в свою чергу зможуть забезпечити ефективність та швидкість виконання завдань у військовій сфері, значно знизити ризик втрат, підвищити захищеність військових систем та зменшити витрати на оборону [28]. Необхідно забезпечити належний рівень кібербезпеки в державі, захистити критичну інфраструктуру та розробити відповідні алгоритми та процедури для виявлення і запобігання різноманітним кіберзагрозам.

Вбачається, що забезпечення національної безпеки та обороноздатності України за допомогою використання технологій штучного інтелекту має системний, міжвідомчий та міжнародний характер, що включає комплекс заходів, як національного, так і міжнародного рівнів. При цьому визначення стратегічних пріоритетів та правильне розуміння проблем у сфері національної безпеки і оборони, пошук оптимальних способів їх вирішення, тісна співпраця правоохоронних та спеціалізованих інституцій сектору безпеки і оборони України та інших держав у створенні ефективної системи протидії сучасним загрозам сприятимуть забезпеченню національної безпеки нашої країни та міжнародній безпеці у світі. Очевидно, що тільки у міжнародній співпраці та міжвідомчій взаємодії, як на національному, так і зарубіжному рівнях, можна вирішити актуальні стратегічні завдання забезпечення національної безпеки у складних світових умовах та нових глобалізаційних викликах.

Висновки. Таким чином, реалії сьогодення воєнного часу, перед криміналістикою ставлять нові завдання, змінюються парадигма криміналістичної науки, що впливає на особливості формування та застосування системи криміналістичних знань, застосування яких спрямоване на забезпечення національної безпеки та обороноздатності України. Засоби криміналістики (прийоми, методи, технології, рекомендації) мають відповідати сьогоdnішнім викликам, успішно протидіяти злочинності в умовах збройної агресії РФ та глобальних загроз суспільству. У сучасних реаліях відбуваються процеси оновлення криміналістичних знань, зважаючи на появу нових видів злочинності та необхідність розроблення криміналістикою для їх протидії інноваційних методів та засобів. Тому формування і розвиток криміналістичних знань, *застосування криміналістичних інновацій*, новітніх технологій є своєрідною відповіддю на виклики сучасності, на появу нових способів та механізмів злочинної діяльності в умовах війни під впливом сучасних тенденцій розвитку науки, техніки та суспільства в сучасних умовах глобальних загроз.

Особливу увагу у сфері забезпечення національної безпеки та обороноздатності України слід звернути на підвищення ролі криміналістичної підготовки слідчих, прокурорів, суддів, детективів, слідчих-криміналістів, судових експертів у цій царині знань. На часі – започаткування нової професії та здійснення підготовки *цифро-*

вого криміналіста у сфері забезпечення національної безпеки та обороноздатності України. За таких обставин сучасну парадигму криміналістики доцільно спрямувати на формування й подальший розвиток нових галузей криміналістики (цифрової, воєнної) для ефективного розв'язання нових завдань в сучасних умовах задля забезпечення національної безпеки та обороноздатності держави. При цьому важливо враховувати сучасні тенденції розвитку криміналістики, пов'язані із формуванням нових її напрямів, що дасть змогу суттєво підвищити роль та прикладне значення застосування криміналістич-

них знань у сфері забезпечення національної безпеки та оборони.

Отже, штучний інтелект може стати важливим інструментом у сфері забезпечення національної безпеки та обороноздатності нашої країни в сучасних умовах воєнного часу та повоєнний період. За таких умов слід враховувати сучасні тенденції розвитку криміналістики, пов'язанні із формуванням нових її напрямів, що дасть змогу суттєво підвищити роль та прикладне значення застосування криміналістичних знань в сучасних реаліях воєнного часу та глобальних загроз світовій цивілізації.

ЛІТЕРАТУРА

1. Dufenyuk O. M. Investigation of war crimes in Ukraine: challenges, standards, innovations. *Baltic Journal of Legal and Social Sciences*. 2022. № 1. Pp. 46–56.
2. Shevchuk V. Criminalistic means, methods and technologies of combating crimes in the field of national security in the context of european integration. *Legal support of European integration: general legal and sectoral aspect*: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2024. 712 p. Pp. 582–604.
3. Matulienė, S., Shevchuk, V., & Baltrūnienė, J. (2023). Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics*, 29(4), 12–46.
4. Shevchuk V.M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver), 2023. Pp. 198–219.
5. Shevchuk, V., Kapustina, M., Zatenatskyi, D., Kostenko, M., & Kolesnikova, I. (2023). Criminalistic support of combating iatrogenic criminal offenses: Information system prospects. *Social & Legal Studies*, 6(4), 208–216.
6. Konovalova V. O., Shevchuk V. M. Innovations in the methodic of teaching criminalistics in modern realities of war. *Modern scientific research: achievements, innovations and development prospects*: Proceedings of the 15th International scientific and practical conference (August 14–16, 2022). MDPC Publishing. Berlin, Germany. 2022. Pp. 385–396.
7. Сайт Офіса Генерального прокурора URL: <https://www.gp.gov.ua/>
8. Shevchuk V., Vapniarchuk V., Borysenko I., Zatenatskyi D., Semenogov V. Criminalistic methodics of crime investigation: Current problems and promising research areas. *Revista Juridica Portucalense*, 32, 2022. Pp. 320–341.
9. Konovalova V.O., Shevchuk V.M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries of modern science: experience, approaches and innovations*: collection of scientific papers "SCIENTIA" of the III International Scientific and Theoretical Conference, January 20, 2023. Amsterdam, The Netherlands: European Scientific Platform. Pp. 73–77.
10. Baltrūnienė J. Dirbtinis intelektas ir duomenų apsauga kriminalistikos plėtros kontekste / *Kriminalistikos teorijos plėtra ir teismo ekspertologijos ateitis: liber amicorum profesoriui Egidijui Vidmantui Kurapkai*. Kolektyvinė monografija. Vilnius, 2022. P. 203.
11. Jackson S. Artificial Intelligence Changing the World of Forensics Science. *EasyChair Preprint*. 2021. No. 5815. 3 p.
12. Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Digital transformation of criminal proceedings under martial law*: materials of the All-Ukrainian round table (Kharkov, December 16, 2022); National Law University named after Yaroslav the Wise; Kharkiv, 2022. Pp.135–140.
13. Шевчук В.М., Авдеева Г.К. Використання технологій штучного інтелекту та спеціальних знань у розслідуванні воєнних злочинів. *Правнича наука та законодавство України: європейський вектор розвитку в умовах воєнного стану*: монографія; Нац. акад. прав. наук України. Харків: Право, 2023. С. 491–503.
14. Мисливий В. А. Штучний інтелект як фактор запобігання дорожньо-транспортної злочинності. *Використання технологій штучного інтелекту у протидії злочинності*: мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 55–60.
15. Мовчан А. В., Мовчан М. А. Використання безпілотних літальних апаратів у діяльності правоохоронних органів. *Соціально-правові студії*. 2020. Вип. 3 (9). С. 104–110.
16. Бугера О. І. Використання штучного інтелекту для запобігання злочинності. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки*. 2021. Т. 32 (71). № 6. С. 82–86.
17. Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів. *Право і безпека*. 2020. № 4 (79). С. 66–72.
18. Юртаєва К. В. Використання технологій штучного інтелекту в реалізації стратегій «predictive policing»: можливості, проблеми та перспективи для України. *Використання технологій штучного інтелекту у протидії злочинності*: наук.-практ. семінар (Харків, 05.11.2020). Харків, 2020. С. 99–104.
19. Федоров М. Технології з розпізнавання облич та штучний інтелект дозволяють знайти кожного / *SUNDRIES*. 09.04.2022. URL: <https://sundries.com.ua/teknologii-z-rozpiznavannia-oblych-ta-shtuchnyi-intelekt-dozvoliaut-znaiti>.
20. Правоохоронні та спеціалізовані інституції сектору безпеки і оборони України: навчально-методичний посібник / за заг. ред. О. Ю. Бусол. Київ: Юрінком Інтер, 2024. 492 с.
21. Шевчук В. М. Проблеми застосування штучного інтелекту у правоохоронній діяльності в контексті російсько-української війни. *Підготовка правоохоронців зі спеціальності 262 «Правоохоронна діяльність» нової формиції: 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.
22. Shevchuk V. M. Criminalistics support for the investigation of military criminal offenses and war crimes: digitalization, innovations, prospects. *Military offences and war crimes: background, theory and practice*: collective monograph. Ed. by V.M. Stratonov. Riga, Latvia: «Baltija Publishing», 2023. Pp. 795–822.
23. Konovalova V.O., Shevchuk V.M. Prospective directions of research of innovations of separate criminalistic methodics. *Scientific practice: modern and classical research methods: Collection of scientific papers «ЛОГОС» of the I International Scientific and Practical Conference* (Vol. 1), Boston, February 26, 2021. Boston – Vinnytsia: Primedia eLaunch& European Scientific Platform, 2021. P. 81–85.
24. Матулене С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. Вип. 4 (29). 2023. С.12–46.
25. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи військового періоду. *Теорія і практика інтелектуальної власності*, 3, 2023. С. 68–78.
26. Павленко Т.А. Технології штучного інтелекту в забезпеченні національної безпеки та обороноздатності України: перспективи стратегії розвитку. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «ПРАВО»*. Вип. 38. 2023. С. 41–47.
27. Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. *Бізнесінформ*. 2022. № 3. С. 17–26. С. 24.
28. Shevchuk V.M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver, Canada), 2023. Pp. 198–219.