

маційного забезпечення та аналіз нормативно-правових актів, що регламентують порядок функціонування інформаційно-аналітичних систем надають можливість стверджувати, що функція інформаційної безпеки реалізується шляхом застосування комплексної системи захисту інформації. Під останньою розуміють єдину сукупність організаційних, технічних, криптографічних та інші заходів і засобів, що забезпечують захист інформації від несанкціонованих дій (доступу до інформації та/або її модифікації), навмисних (або ненавмисних) спроб порушення конфіденційності, цілісності та доступності ресурсів системи та інших загроз¹.

Резюмуючи вищезазначене, вважаємо, що функціонування інформаційно-аналітичних систем органів кримінальної юстиції забезпечує організаційні, управлінські, аналітичні, інформаційні потреби їх користувачів.

===== 2.5. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень (В. Шевчук)

Реалії сьогодення, пов'язані із збройною російською агресією України, активними процесами цифровізації та європеїзації нашої

¹ Вишня В. Б. Основи інформаційної безпеки : навч. посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. С.19; Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>; Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: затв. Наказом Генерального прокурора від 17.08.2023 № 231. URL: <https://zakon.rada.gov.ua/laws/show/v0298905-20#Text>; Положенням про інформаційно-телекомунікаційну систему досудового розслідування «іКейс»: затвер. Наказом Національного антикорупційного бюро України, Офісу Генерального прокурора, Ради суддів України, Вищого антикорупційного суду 15 грудня 2021 року № 175/390/57/72. URL: <https://zakon.rada.gov.ua/laws/show/v0390886-21#Text>; Положення про Електронний реєстр геномної інформації людини: затв. Наказом Міністерства внутрішніх справ України від 04 серпня 2023 року № 639. URL: <https://zakon.rada.gov.ua/laws/show/z1657-23#Text>; Положення про Єдиний реєстр осіб, зниклих безвісти за особливих обставин: затв. Наказ Міністерства внутрішніх справ України 29 серпня 2022 року № 535. URL: <https://zakon.rada.gov.ua/laws/show/z0998-22#Text>

держави, визначають сучасні тенденції розвитку юридичної науки, у тому числі й криміналістики щодо формування перспективних інноваційних напрямів 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. Серед них найбільш перспективними є використання технологій штучного інтелекту в сучасних умовах глобальних загроз та воєнних викликів.

Останнім часом стан злочинності в Україні та її динаміка під час війни значно вплинули на зміну пріоритетів завдань криміналістики і особливості формування й застосування криміналістичних знань. Інформатизація соціального середовища призвела до «технологізації» криміналістики, розроблення і впровадження інформаційних, цифрових, телекомунікаційних та інших технологій¹. За таких обставин постає необхідність криміналістичного забезпечення розслідування воєнних злочинів, злочинів проти національної безпеки України². Серед пріоритетних напрямів удосконалення криміналістичної методики розслідування воєнних злочинів та кримінальних правопорушень, пов'язаних із війною, постають проблеми використання технологій штучного інтелекту³.

В реаліях російської військової агресії інструменти штучного інтелекту істотно сприяють виявленню, розкриттю та розслідуванню злочинів проти людяності та геноциду і кримінальних правопору-

¹ Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України*. 2022. № 2. С. 76–90. С. 83.

² Shevchuk V. M. Development of digital criminalistics in the conditions of war in Ukraine. *Diversity and inclusion in scientific area*. II International Scientific and Practical Conference (January 26–28, 2023; Warsaw, Poland). №. 140. Warsaw, Poland, Ceac Polonia, SPC «InterConf», 2023. Pp. 442–450.

³ Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану*: матеріали всеукраїнського круглого столу (м. Харків, 16 грудня 2022 р.); Національний юридичний ун-т ім. Ярослава Мудрого; НДІ ВПЗ імені акад. В. В. Сташиса НАПр України. Харків, 2022. С. 81.

шень, пов'язаних із воєнною агресією РФ проти України. Практика показує, що за допомогою технологій штучного інтелекту можна ідентифікувати російських військових за соціальними мережами й записами камер відеоспостереження¹. Достатньо активно застосовуються технології розпізнавання обличчя *Clearview AI* для боротьби з дезінформацією, розпізнавання й ідентифікації загиблих і воєнних злочинців². Використання технологій штучного інтелекту допомагає руйнувати міфи про нібито невмирущих солдатів так званої «спецоперації», розпізнаючи обличчя трупів російських військових окупантів, відшуковуючи їх у соціальних мережах і за допомогою автодозвонів повідомляючи родичів про їхню смерть³.

В сьогоденнішніх реаліях штучний інтелект використовується у повсякденній діяльності людини, наприклад, для перекладу текстів, створення субтитрів для відео або блокування електронних листів (спаму)⁴. При цьому штучний інтелект розглядається як сукупність методів, способів, технологій і засобів (зокрема, апаратних), комп'ютерних програм, які реалізують одну, кілька або всі когнітивні функції, еквівалентні когнітивним функціям людини⁵; це сконструйований людиною пристрій або комп'ютерна програма зі здобування, оброблення й застосування інформації та формування вмінь, подібних

¹ Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistikairteismo ekspertologija : mokslas, studijos, praktika*. 2022. Т. 18. С. 32.

² Федоров М. Технології з розпізнавання облич та штучний інтелект дозволяють знайти кожного / SUNDRIES. 09.04.2022. URL: <https://sundries.com.ua/tekhnolohii-z-rozpiznavannia-oblych-ta-shtuchnyi-intelekt-dozvoliaut-znaity>

³ Konovalova V. O., Shevchuk V. M. Application of digital technologies in criminalistics in the conditions of war. *Цифрова трансформація кримінального провадження в умовах воєнного стану: матеріали круглого столу, присвяч. Всеукр. тижню права* (м. Харків, 23 груд. 2022 р.): електрон. наук. вид.; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2022. С. 141–146.

⁴ Shevchuk V. M. Transformation of the tasks of criminalistics and forensic examination under the influence of martial law. *Transformation of the legal system and human rights protection under the influence of martial law: collective monograph*. Ed. by V. M. Stratonov. Riga, Latvia: «Baltija Publishing», 2024. Pp. 438–461.

⁵ Баранов О. Ідентифікація роботи зі штучним інтелектом як суб'єкта права. *Інтернет речей: проблеми правового регулювання та впровадження* : мат.-ли друг. наук.-практ. конф. (Київ, 29.11.2018). Київ, 2018. С. 9. URL: http://ippi.org.ua/sites/default/files/zbirnik_tez_19.12.2018-maket_3-converted.pdf

до дій, свідомо виконуваних людиною¹. Штучний інтелект – це система, що поводить себе розумно, аналізуючи своє оточення й ухвалюючи доволі автономні рішення для досягнення мети². 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») тощо.

Попри всі позитивні можливості й потенціал штучного інтелекту, останнім часом такими технологіями дедалі частіше послуговуються злочинці, винаходячи нові способи злочинної діяльності і з використанням новітніх технологій штучного інтелекту. До того ж криміногенні чинники застосування штучного інтелекту спричиняють нові загрози та виклики охоронюваним законом інтересам як окремих громадян, так і держави й суспільства загалом, потребуючи адекватних засобів протидії таким кримінально-правовим³ і криміналістичним засобам⁴. Тому штучний інтелект як останнє наукове досягнення потребує нових криміналістичних ідей і методів, пов'язаних із його використанням у боротьбі зі злочинністю⁵.

Під час війни арсенал традиційних криміналістичних засобів і форм збирання доказів вчинення воєнних злочинів в Україні доволі

¹ Мічурін Є. О. Правова природа штучного інтелекту. *Форум Права*. 2020. № 64 (5). С. 67–75. DOI: 10.5281/zenodo.4300624

² 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. P. 201–220.

³ Radutniy O. E. Novel Criminal Delicts Related to Digital Human Being. *Вісник Асоціації кримінального права України*. 2020. Т. 1. № 13. С. 16–28. URL: <http://vakp.nlu.edu.ua/issue/view/12594>

⁴ Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science : Proceedings of the 5th International scientific and practical conference (August 7–9, 2022)*. Lviv, 2022. Pp. 896–903.

⁵ Jackson C. Artificial Intelligence Changing the World of Forensics Science. EasyChair Preprint. 2021. No. 5815. 3 p. URL: <https://easychair.org/publications/preprint/1Fmk>

обмежений через небезпеку для всіх учасників слідчих (розшукових), негласних слідчих (розшукових) дій та неможливість безпосереднього доступу до місця події¹, тому виникає потреба у застосуванні технологій штучного інтелекту. Крім цього, про європейський вектор розвитку криміналістики та судової експертизи в Україні свідчить застосування європейських стандартів доказування під час кримінального провадження².

Сьогодні важливо враховувати, що для судового розгляду воєнних злочинів та військових кримінальних правопорушень, зокрема, як для судів України, так і будь-якого міжнародного суду основоположним буде встановлення причинно-наслідкового зв'язку між винними діями країни-агресора й не тільки окремих військових російських окупантів, а й військово-політичного керівництва РФ та наслідками, що настали, тобто заподіяною шкодою. Для цього досить важливим є правильна робота з доказовою базою, зокрема, збирання, документування та розслідування воєнних злочинів, яка має здійснюватися із врахуванням міжнародного досвіду та європейських стандартів доказування, що є досить важливим³.

При цьому, однією із проблем використання технологій штучного інтелекту під час досудового розслідування можливим є порушення прав людини (щодо захисту конфіденційності особистих даних і втручання у приватне життя). Тому важливо не перебільшувати потенціал і переваги штучного інтелекту: варто зважати на його окремі недоліки. Убачаємо, що застосовувати штучний інтелект у судочинстві та правоохоронній діяльності припустимо тільки за умови

¹ Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. №4. С. 369–374. DOI: 10.32782/2524-0374/2022-4/88

² Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України*. 2022. №2. С. 87.

³ Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. *Використання цифрових технологій у криміналістиці та судовій експертизі* : матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К. Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. С та шиса НАПрН України. Харків: Право, 2024. С.133–136.

обов'язкового дотримання принципів верховенства права, основних прав людини, поваги до її честі й гідності, рівності перед законом і судом, пропорційності, змагальності сторін, прозорості, неупередженості та справедливості тощо.

В сучасних реаліях воєнних та глобальних загроз усі практики у сфері міжнародного кримінального правосуддя повинні покращувати своє технічне розуміння новітніх технологій штучного інтелекту¹ і повинні культивувати глибше сучасне розуміння застосування того, як соціальні мережі, геолокації, розмови мобільного зв'язку, комп'ютерна інформація та інші цифрові сліди й комунікації використовуються в зонах проведення воєнних дій². Зважаючи на воєнну агресію російськими військами на територію України та вчинення ними масових вбивств, гвалтувань, мародерства, сьогодні гостро постає проблема збирання доказів воєнних злочинів. Це потребує активізації та поширення застосування технологій штучного інтелекту при виявленні, документуванні та розслідуванні воєнних злочинів, злочинів проти людяності та геноциду.

Застосування штучного інтелекту в розслідуванні воєнних злочинів в Україні може бути корисним в багатьох аспектах. Основними напрямками, в яких він може бути використаний, є такі:

1) *аналіз супутникових знімків*. Штучний інтелект може допомогти аналізувати великі обсяги супутникових знімків для виявлення змін у ландшафті, зокрема будівель, доріг, об'єктів інфраструктури, які можуть бути пов'язані з воєнними злочинами, а також допомогти в ідентифікації місць, де можуть бути поховані тіла жертв воєнних злочинів³;

¹ Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

² Freeman, L. Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials. *Fordham International Law Journal*, 2018, 41 (2), 284–336. С. 335. Available at: <https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1>

³ Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: <https://nv.ua/ukr/opinion/viy-na-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochiny-rf-v-ukrajini-novini-ukrajini-50248411.html>

2) *аналіз відео- та фотоматеріалів*. Штучний інтелект може бути використано для аналізу великого обсягу відео- та фотоматеріалів, які були зняті на місцях вчинення воєнних злочинів, що, у свою чергу, може допомогти в ідентифікації підозрюваних та свідків, а також встановити, чи були зображені на них об'єкти, які можуть містити криміналістично-значущу інформацію для розслідування таких злочинів¹;

3) *обробка аудіоматеріалів*. За записами телефонних розмов та під час обробки аудіоматеріалів щодо розслідування воєнних злочинів штучний інтелект може допомогти в ідентифікації голосів, які містяться на таких носіях, а також визначити місця, де були здійснені ці розмови;

4) *аналіз соціальних мереж*². Аналізуючи соціальні мережі, штучний інтелект може допомогти виявити зв'язки між підозрюваними, які можуть бути пов'язані з воєнними злочинами, та ідентифікувати осіб, які можуть бути свідками воєнних злочинів або мати інформацію про них³;

5) *аналіз даних з медичних закладів*. Штучний інтелект може допомогти в ідентифікації тіл жертв воєнних злочинів, встановленні причини смерті, ідентифікації військовополонених, військових злочинців та їх пошук за даними про хворобу та відомостями про їх ідентифікаційні ознаки, які допомагають встановленню конкретної особи⁴;

¹ Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, – LIGA.net URL: <https://tech.liga.net/ua/ukraine/novosti/iskusstvennyy-intellekt-mintsifry-razoblachil-okkupanta-popavshego-v-gospital-v-krivom-roge>

² Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

³ Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С.142–146.

⁴ Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL: <https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogilu-ukrayinskih-vijskovih-ta-ponad-460-novih-mogil-foto>

6) *розпізнавання облич*. Штучний інтелект може бути використаний для розпізнавання облич на фото та відео з місць вчинення воєнних злочинів. Це може допомогти в ідентифікації підозрюваних, причетних до вчинення таких злочинів, та встановленню свідків, які можуть повідомити важливу інформацію про розслідувану подію воєнного злочину;

7) *аналіз текстової інформації*. Аналіз штучним інтелектом текстової інформації (наприклад, повідомлень у соціальних мережах та інших джерелах), пов'язаної з воєнними злочинами, сприятиме ідентифікації підозрюваних і свідків та з'ясуванню криміналістично значущої інформації про воєнні злочини, які розслідуються¹.

Отже, застосування штучного інтелекту може бути корисним для ефективного розслідування воєнних злочинів, злочинів проти людяності та геноциду й допомогти встановити винних і притягти їх до відповідальності за вчиненні злочини. Проте, варто зазначити, що використання штучного інтелекту в розслідуванні таких злочинів має свої виклики та обмеження. Один з найбільших викликів полягає у тому, що війна є ситуацією, в якій може бути складно отримати достовірну інформацію через високу ступінь конфлікту та непередбачуваність ситуації на місці. Також, існує ризик використання штучного інтелекту для переслідування політичних опонентів або некоректного відображення даних через певні алгоритмічні недосконалості. Крім того, важливо враховувати законодавчі обмеження щодо застосування штучного інтелекту в розслідуванні злочинів, зокрема, заборони на використання деяких видів даних, які можуть порушувати права людини². Усі ці фактори потребують ретельного аналізу та планування перед застосуванням штучного інтелекту в розслідуванні воєнних злочинів. Водночас, застосування штучного інтелекту є потужним

¹ 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). 2022. С.12–46. С. 37. URL: <https://khrife-journal.org/index.php/journal/issue/view/18/4-22>

² Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану* : мат-ли Всеукр. круглого столу (Харків, 16.12.2022). Харків, 2022. С. 139.

інструментом в розслідуванні воєнних злочинів в Україні та може допомогти забезпечити справедливість та притягнути винних до відповідальності за вчинені такі злочини¹.

Застосування штучного інтелекту та сучасних цифрових технологій у воєнних реаліях дає змогу суттєво підвищити ефективність і прискорити розслідування воєнних злочинів, злочинів проти людяності та геноциду. Відомо, що майже будь-яку діяльність людей (зокрема, злочинців по використанню технологій штучного інтелекту) у сучасному світі супроводжує своєрідна «слідова картина», особливе місце в якій посідають цифрові сліди² як важливе джерело криміналістичної інформації. За таких обставин можна стверджувати про активізацію тенденцій формування та застосування нового наукового напрямку – цифрової криміналістики (*Digital Criminalistics*)³, яка має стати стратегічним напрямом у розвитку криміналістики⁴.

Сучасні підходи до розслідування воєнних злочинів дають змогу визначити джерела цифрової інформації, якими зумовлено напрями збирання й дослідження цифрових слідів для отримання інформації: із мобільних пристроїв, вилучених в учасників кримінального провадження телефонів; із персональних комп'ютерів фізичних і юридичних осіб; із серверів та інших накопичувачів інформації в організаціях та установах; із радіочастотних ідентифікаторів, *GPS*-трекерів, датчиків, стаціонарних і мобільних вимірювальних пристроїв із використанням систем геолокації, відеоспостереження та позиціону-

¹ 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. Pp. 582–604.

² Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання й дослідження у кримінальному провадженні. *Цифрові трансформації України 2020: виклики та реалії* : зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за мат-ми кругл. столу (Харків, 18.09.2020). Харків, 2020. С. 92–97.

³ Латиш К. *Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika*, 2022. T. 18. С. 31–37.

⁴ 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.

вання; із мережевих сервісів, що забезпечують голосовий і відеозв'язок між комп'ютерами через інтернет (*ICQ, Skype, WhatsApp, Viber, Telegram* та ін.); із банківських систем на цифрових носіях (*HDD, SSD, флешкартках* тощо); від стільникових операторів зв'язку щодо деталізації абонентського зв'язку й визначення місця знаходження абонента за допомогою геолокації; із записів камер відеоспостереження комерційних і державних структур; із вилучених в учасників кримінального провадження фотоапаратів і відеокамер¹.

Вбачається, що застосування технологій штучного інтелекту та процес цифровізації криміналістики є закономірним етапом розвитку й формування сучасних криміналістичних знань², який передбачає активне впровадження цифрових технологій у різні галузі криміналістики, судової експертології та юридичної практики³. За таких умов в реаліях сьогодення необхідно активізувати розроблення цифрової криміналістики як стратегічного напрямку розвитку криміналістики. При цьому особливу увагу потрібно звернути на роль криміналістичної дидактики⁴, зокрема, криміналістичну підготовку слідчих, судів, прокурорів, детективів, судових експертів у сфері цифрових технологій. Сучасна парадигма криміналістики повинна бути спрямована на подальший розвиток та формування цифрової криміналістики для ефективного вирішення нових завдань в умовах воєнного стану та процесів цифровізації суспільства.

¹ 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). 2022. С. 37. URL: <https://khrife-journal.org/index.php/journal/issue/view/18/4-22>

² Шевчук В. М. Штучний інтелект в криміналістиці : проблеми, можливості, перспективи. *Інформаційне забезпечення розслідування злочинів*: матеріали Х Міжнародного круглого столу (м. Одеса, 19 травня 2023 р.). Одеса: Видавництво «Юридика», 2023. С. 89–97.

³ Shepitko V. Yu., Kononova V. O., Shevchuk V. M. et. al. Scientific and technical support of investigative activities in the context of an adversarial criminal procedure. *Issues of Crime Prevention*. Vol. 1, 2021, 42, 92–102.

⁴ Malewski H., Kurapka V. E., Tamelè I. Motivation and expectations of students-animportant factorin theimplementation of the new bachelor's degreeprogram «Law and Criminalistics. *The Criminalist of the First Printing*, 21/2021, 12–26.

Ще один аспект є важливим в дослідженні означених питань – це проблеми та перспективи застосування штучного інтелекту у правоохоронній діяльності. На сьогоднішній день застосування та впровадження технологій штучного інтелекту у правоохоронну діяльність багато в чому обумовлено необхідністю протистояти злочинному світу, який дедалі бере на озброєння найсучасніші інноваційні технології. Злочинці достатньо активно використовують останні досягнення четвертої промислової революції: технології блокчейну, дрони, робототехніку, штучний інтелект. Тому використання можливостей штучного інтелекту у роботі правоохоронних органів є на сьогодні достатньо актуальними та затребуваними практикою¹.

Сьогодні правоохоронні органи України активно використовують технології штучного інтелекту за різними напрямками, які суттєво підвищують ефективність цієї роботи, оптимізують вирішення завдань протидії злочинності, зокрема, серед основним слід виокремити: 1) розпізнавання обличчя та ідентифікація російських військових-окупантів у соціальних мережах та камерах відеозапису²; 2) забезпечення безпеки на дорогах, виявлення та фіксація порушень правил дорожнього руху³; 3) використання безпілотників для протидії незаконному обгігу вогнепальної зброї, наркозлочинності⁴, проведення

¹ Шевчук В. М. Можливості та перспективи використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи, засоби та технології в криміналістиці та судовій експертизі* : наук.-практ. посібник : електрон. наук. вид. ; за ред. В. Ю. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Х.: Право, 2023. С. 105–115.

² Kryvoruchko, O., Bebesko, B., Khorolska, K., Desiatko, A., & Kotenko, N. Artificial intelligence face recognition for authentication = Використання системи розпізнавання обличчя для авторизації на основі штучного інтелекту=. *Технічні науки та технології*, 2020. (2(20)), 139–148. <http://tst.stu.cn.ua/article/view/215780>

³ Мисливий В. А. Штучний інтелект як фактор запобігання дорожньо-транспортної злочинності. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листопада 2020 р.). Харків : Право, 2020. С. 55–60.

⁴ Мовчан А. В., Мовчан М. А. Використання безпілотних літальних апаратів у діяльності правоохоронних органів. *Соціально-правові студії*. 2020. Випуск 3 (9). С. 104–110. URL: [http://www.sls.lvduvs.edu.ua/documents_pdf/arhiv/sps_3\(9\)_2020/16.pdf](http://www.sls.lvduvs.edu.ua/documents_pdf/arhiv/sps_3(9)_2020/16.pdf)

військових операцій¹ та збирання доказової інформації умовах війни і ведення активних бойових дій з метою фіксації воєнних злочинів; 4) попередження кримінальних правопорушень з використанням інтелектуальних систем безпеки з різними пристроями (датчиками) збору інформації²; 5) прогнозування кримінальних правопорушень методом картографування злочинності³, за допомогою якого формуються прогнози щодо місцевої злочинності та індивідуальної злочинної поведінки.

Так, наприклад, завдяки технологій штучного інтелекту можуть створюватися обґрунтовані прогнози щодо темпоральних, територіальних і якісних показників злочинності. Ці прогнози покликані сприяти правоохоронним органам в оптимізації використання наявних ресурсів та виконання поліцейських функцій⁴. Крім цього, за допомогою технологій штучного інтелекту здійснюється ідентифікація російських військових-окупантів у соціальних мережах та камерах відеозапису⁵. За інформацією Міністерства цифрової трансформації України, технології штучного інтелекту цього відомство вже зчитували обличчя, коли громадяни України підписувались в мобільному додатку «Дія». У сучасних реаліях за цим же алгоритмом штучний інтелект розвінчує міфи про так звану «спецоперацію» з «невмирущими» солдатами. Такі технології розпізнають обличчя трупів оку-

¹ Мосов С. П. Хорошилова С. Й. Особливості застосування стратегічної безпілотної розвідувальної авіації у воєнних конфліктах ХХІ століття. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. К., 2018. № 3. С. 97–102.

² Бугера О. І. Використання штучного інтелекту для запобігання злочинності. *Вчені записки ТНУ імені В. І. Вернадського*. 2021. № 6 (71). С. 82–86. doi: 10.32838/TNU-2707-0581/2021.6/13.

³ Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів. *Право і безпека. Право и безопасность – Law and Safety*. 2020. № 4 (79). С. 66–72. DOI: <https://doi.org/10.32631/pb.2020.4.10>.

⁴ 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 (м. Харків, 5 листоп. 2020 р.). Х. : Право, 2020. С. 99–104.

⁵ Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistikairteismo ekspertologija : mokslas, studijos, praktika: XVIII*, 2022. Т. 18. С. 32.

пантів та знаходять їх в соцмережах, а автодозвони повідомляють родичів про їхню смерть. Міноборони України також розпочало використовувати технологію розпізнавання обличчя «Clearview AI», щоб розпізнавати російських нападників, боротися з дезінформацією, ідентифікувати загиблих та воєнних злочинців-окупантів¹. У воєнних реаліях повномасштабної військової агресії РФ на території України інструменти цифрової криміналістики значно допомагають у виявленні, розкритті та розслідуванні воєнних злочинів².

Отже, використання штучного інтелекту у правоохоронній діяльності є важливим інструментом підвищення ефективності роботи органів правопорядку за допомогою розробки і впровадження новітніх цифрових технологій за такими головними спрямуваннями:

1) *інформаційно-аналітичне забезпечення правоохоронної діяльності*, зокрема, як приклад можна назвати інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», яка призначена для обробки відомостей, що утворюються у процесі діяльності НП України та її інформаційно-аналітичного забезпечення³;

2) *інформаційно-довідкове забезпечення правоохоронної діяльності*, як напрямок формування інформаційної системи, пов'язаний з появою геоінформаційних систем, які надають інформацію про просторове розміщення об'єктів з використанням карт або планів;

3) створення спеціалізованих інформаційних інтелектуальних систем оперативно-розшукового призначення, зокрема розробка та впровадження автоматизованої системи проведення ОРЗ та НСРД у телекомунікаційних мережах загального користування за аналогією

¹ Федоров М. Технології з розпізнавання облич та штучний інтелект дозволяють знайти кожного – SUNDRIES URL: <https://sundries.com.ua/tekhnolohii-z-rozpiznavannia-oblych-ta-shtuchnyi-intelekt-dozvoliaut-znaity>

² Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі?: URL: <https://nv.ua/ukr/opinion/viy-na-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochyni-rf-v-ukrajini-novini-ukrajini-50248411.html>

³ Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ МВС України від 03.08.2017 No 676 / *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/z1059-17>

до американських «Eshelon» та «DCS-1000» («Carnivore»), європейської системи «RES»;

4) *формування та розвиток інтелектуальних систем відеоспостереження*, які функціонально поділяються на дві групи: а) розпізнавання та класифікація об'єктів відеоспостереження; б) відстеження шляху об'єкта відеоспостереження;

5) *охорона об'єктів*, до яких можна віднести системи централізованої охорони об'єктів «Орлан», «Кронос», «АІ-Грифон» тощо, які, по суті, представляють комплекс технічних засобів і програмного забезпечення для централізованого спостереження за станом пристроїв охоронної та пожежної сигналізації;

6) *створення відомчих спеціалізованих інтелектуальних інформаційних систем*, наприклад, для поліції – автоматизовані дактилоскопічні інформаційні системи (АДІС «Сонда», «Дакто-2000», «Морфо» – Франція, «Принтрак» – США, «NEX» – Японія тощо); для прикордонної служби – інтегровані інформаційно-телекомунікаційні системи «Аркан» та «Гарт»; для митників – багатофункціональна комплексна інформаційна система «Електронна митниця»;

7) *впровадження та розроблення інтелектуальних інформаційних освітніх систем*, зокрема: моделювання знань, комунікації, інтерпретації, самовдосконалення; взаємодії¹;

8) *запровадження інформаційно-телекомунікаційної системи досудового розслідування*², що є важливим кроком удосконалення слідчої (детективної) діяльності, а використання штучного інтелекту сприятиме значній економії часу, коштів, засобів ресурсів, зменшенню строків розгляду відповідних процесуальних документів, спрощенню доступу учасників у межах їх компетенції до відповідних

¹ Ковтун В., Рвачов О. М. Огляд та перспективи використання технологій штучного інтелекту в правоохоронній діяльності. *Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару* (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 46–47.

² Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування: Закон України від 1 червня 2021 р. No 1498-IX. URL : <https://zakon.rada.gov.ua/laws/show/1498-20#Text>

матеріалів кримінального провадження, цифровізації документообігу тощо¹.

Крім цього, 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 України, зокрема технологій штучного інтелекту. 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. Штучний інтелект як останнє наукове досягнення потребує нових криміналістичних ідей і методів, пов'язаних із його використанням у боротьбі зі злочинністю², у тому числі й у забезпеченні безпеки та обороноздатності України.

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

¹ Глобенко Г. І. Інформаційно-телекомунікаційна система досудового розслідування: міжнародний досвід і шляхи запровадження. *Вісник Харківського національного університету внутрішніх справ*. 2021. №4 (95). С. 188–198. DOI: <https://doi.org/10.32631/v.2021.4.16>

² Jackson C. Artificial Intelligence Changing the World of Forensics Science. EasyChair Preprint. 2021. No. 5815. 3 p. URL: <https://easychair.org/publications/preprint/1Fmk>

кордону та правопорядку на всіх рівнях і всіма органами держави та певними службовими особами¹.

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 часу².

Правоохоронні органи України, суттєво підвищуючи ефективність своєї роботи й оптимізуючи розв'язання завдань із протидії злочинності, активно послуговуються різноманітними 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 ; 3) використання безпілотників для протидії незаконному обігу вогнепальної зброї й наркотиків³, для проведення військових операцій і збирання доказової інформації в умовах війни й ведення активних бойових дій із метою фіксування воєнних злочинів⁴; 4) попередження кримінальних правопорушень із використанням інтелектуальних систем без-

¹ Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки і обороноздатності України. *Юридичний науковий електронний журнал*. № 6. 2024. С. 356–361. URL: http://www.lsej.org.ua/6_2024/90.pdf

² Шевчук В. М. Проблеми застосування штучного інтелекту у правоохоронній діяльності в сучасних реаліях війни. *Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності* : матеріали постійно діючої Міжн. наук.-практ. конф. (м. Кропивницький, 24 березня 2023 р.) ; Кіровоградський НДЕКЦ МВС України. Кропивницький : ТОВ «Центрально-Українське видавництво», 2023. С. 141–145.

³ Мовчан А. В., Мовчан М. А. Використання безпілотних літальних апаратів у діяльності правоохоронних органів. *Соціально-правові студії*. 2020. Вип. 3 (9). С. 104–110.

⁴ Шевчук В. М. Проблеми використання цифрової інформації при розслідуванні порушення законів та звичаїв війни. *Актуальні аспекти криміналістичного та психологічного забезпечення правоохоронної діяльності*. Матеріали Всеукр. наук.-практ. конф. (м. Одеса, 6 жовтня 2023 р.). Одеса: ОДУВС, 2023. С. 184–189.

пеки з різними пристроями (датчиками) збирання інформації¹; 5) прогнозування кримінальних правопорушень методом картографування злочинності (за допомогою якого прогнозують місцеву злочинність та індивідуальну злочинну поведінку)².

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 функцій³. Крім того, за допомогою технологій штучного інтелекту можна ідентифікувати російських військових за соціальними мережами й записами камер відеоспостереження. Штучний інтелект руйнує міфи про нібито немирущих солдатів так званої спецоперації, розпізнаючи обличчя трупів окупантів, відшукуючи їх у соціальних мережах і за допомогою автодозвонів повідомляючи родичів про їхню смерть. Міністерство оборони України застосовує технологію розпізнавання обличчя *Clearview AI* для боротьби з дезінформацією, розпізнавання й ідентифікації загиблих і воєнних злочинців⁴.

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

¹ 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.

² Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів. *Право і безпека*. 2020. №4 (79). С. 66–72.

³ 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.

⁴ Федоров М. Технології з розпізнавання облич та штучний інтелект дозволяють знайти кожного / SUNDRIES. 09.04.2022. URL: <https://sundries.com.ua/tekhnolohii-z-rozpiznavannia-oblych-ta-shtuchnyi-intelekt-dozvoliaut-znaity>.

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 України¹.

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 політику².

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 штучного інтелекту у роботі правоохоронних органів є актуальними та затребуваними практикою.

¹ Шевчук В. М. Проблеми застосування штучного інтелекту у правоохоронній діяльності в контексті російсько-української війни. *Підготовка правоохоронців зі спеціальності 262 «Правоохоронна діяльність» нової формації: напрями освітнього та наукового забезпечення* : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 4 березня – 14 квітня 2024 року. Львів – Торунь : Liha-Pres, 2024. С.134–138.

² Правоохоронні та спеціалізовані інституції сектору безпеки і оборони України: навчально-методичний посібник / за заг. ред. О. Ю. Бусол. Київ: Юрінком Інтер, 2024. 492 с. С. 6–8.

Штучний інтелект відіграє важливу роль у забезпеченні безпеки та обороноздатності України. Забезпечення 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 цілому¹. Тому забезпечення національної безпеки та оборони України має стати головним пріоритетом діяльності України та військово-політичного керівництва держави².

Важливо зауважити, що розроблення правового регулювання застосування технологій штучного інтелекту наразі відбувається вкрай повільно стосовно стрімкого розвитку технологій ШІ, які одночасно охоплюють усі сфери суспільних відносин. Тому контроль за створенням та використанням штучного інтелекту 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 законодавства³. Більше того, що триваюча російська військова агресія змушує по-новому осмислити місію і завдання національного ОПК в сучасних реаліях. Відтворення тенденцій розвитку озброєнь 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 країни⁴.

¹ Matulienė, S., Shevchuk, V., & Baltrūnienė, J. Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics*, 2023, 29(4). Pp. 12–46.

² Шевчук В. М. Роль криміналістики та технологій штучного інтелекту у протидії злочинності й забезпеченні національної безпеки та оборони України. *Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни* : матеріали міжнародної науково-практичної конференції (м. Кропивницький, 19 квітня 2024 р.). Кропивницький: ДонДУВС, 2024. С. 652–660.

³ 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.

⁴ Павленко Т. А. Технології штучного інтелекту в забезпеченні національної безпеки та обороноздатності України. *Перспективи стратегії розвитку* : збірник

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

Вбачається, що контроль за створенням та використанням штучного інтелекту 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 реаліях¹. 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 штучного інтелекту у сфері забезпечення національної безпеки та обороноздатності України в умовах воєнного стану та повоєнний період.

Позитивним є, зокрема: а) підвищення ефективності – штучний інтелект 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 –

наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «ПРАВО». Вип. 38. 2023. С. 41–47.

¹ Шевчук В. М. Вплив технологій штучного інтелекту на методику викладання криміналістики в сучасних реаліях війни. *Sound legal education as a guarantee of fair justice: scientific and pedagogical internship*, December 4 – January 14, 2024. Riga, the Republic of Latvia: «Baltija Publishing», 2024. С. 89–95.

застосування ШІ може допомогти у попередженні катастроф та мінімізації ризиків для військового персоналу, що забезпечує безпеку та захист держави; в) забезпечення безпеки – ШІ 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 – ШІ може допомогти в автоматизації багатьох процесів у сфері оборони, що зменшує ризик помилок та підвищує ефективність; д) удосконалення озброєння – ШІ може бути використаний для розроблення та вдосконалення зброї, що забезпечує перевагу військам на полі бою. ШІ може бути використаний для створення систем розвідки та контролю, які можуть виявляти загрози національній безпеці та вживати заходів для їх запобігання ¹.

Визначаючи переваги використання штучного інтелекту для розвитку обороноздатності країн світу, необхідно враховувати, що надмірна залежність від систем ШІ призведе до появи нових значних загроз і невирішених питань для подальших досліджень. Крім цього, значний вплив на формування та розвиток військового потенціалу матиме ШІ, 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. ШІ 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 ².

¹ 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.

² 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.

Одночасно, вбачається, що разом з перевагами, ШІ може становити загрозу національній безпеці та обороноздатності нашої країні, оскільки країна-агресор може використовувати ШІ для вчинення воєнних злочинів, кібератак, що можуть негативно впливати на національну безпеку. В сучасних реаліях існує також ризик, що й інші держави можуть використовувати ШІ для проведення кібершпигунства та кібератак на інфраструктуру країни. Більше того, ШІ може порушувати етичні принципи та права людини, а використання автономної зброї, керованої ШІ, 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 штучного інтелекту 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 оборону¹. Необхідно забезпечити належний рівень кібербезпеки, захистити критичну інфраструктуру та розробити відповідні алгоритми та процедури для виявлення і запобігання загрозам.

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 між-

¹ 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.

народній 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.

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'язані 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 світової цивілізації¹.

Значною проблемою від використання технологій штучного інтелекту сьогодні є порушення прав людини у сфері захисту конфіденційності особистих даних в Інтернеті та проблеми втручання в приватне життя. Тому важливо не перебільшувати можливості та переваги штучного інтелекту, враховуючи і певні недоліки. Вбачається, що застосування штучного інтелекту у судочинстві та правоохороній діяльності є можливим із обов'язковим врахуванням принципів верховенства права, дотримання основних прав людини, поваги до честі і гідності, рівності перед законом і судом, пропорційності, змагальності сторін, прозорості, неупередженості та справедливості тощо. Водночас, неможливо на сьогодні повністю замінити суддю при здійсненні судочинства на штучний інтелект, однак, ніщо не забороняє оптимізувати роботу судді та суду шляхом залучення таких технологій. Головна роль штучного інтелекту має бути визначена не як заміна судді при здійсненні судочинства, а як своєрідна допомога для здійснення правосуддя суддею.

З огляду на викладене, необхідно створити глобальне (обов'язкове) міжнародне законодавство щодо розробки та впровадження штучно-

¹ Шевчук В. М. Розвиток криміналістики та судової експертизи в сучасних умовах воєнного стану війни. *Актуальні питання судової експертизи і криміналістики* : зб. мат-лів міжнар. наук.-практ. конф. з нагоди 100-річчя від дня народження М. С. Романова (Харків, 17. 05.2024). Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2024. С. 283–285.

го інтелекту, зокрема для запобігання його нелегальному, тобто нецивілізаційному використанню. Крім того, уряди та компанії повинні знати про недосконалість даних, на яких базується технологія штучного інтелекту, і подбати про запобігання дискримінації та порушенням прав людини. Перспективи подальших досліджень мають бути спрямовані на розроблення питань, що стосуються розвитку та використання штучного інтелекту як складової інформаційних технологій у правоохоронній діяльності та правосудді з врахуванням міжнародного досвіду та сучасної практики.

Отже, за таких обставин у воєнних реаліях сьогодення нині гостро постає питання про підвищення ефективності розслідування воєнних злочинів та кримінальних правопорушень, пов'язаних із війною, за допомогою активізації використання технологій штучного інтелекту, як важливого напрямку удосконалення криміналістичного забезпечення розслідування цієї категорії кримінальних проявів. У свою чергу це обумовлює потребу у подальших наукових дослідженнях цієї проблематики, як стратегічного напрямку розвитку сучасної криміналістики.

2.6. Проблеми забезпечення охорони прав і свобод людини в епоху штучного інтелекту (Г. Авдєєва)

Пріоритетним завданням будь-якої сучасної держави є захист і охорона прав і свобод людини. Основні принципи такої охорони містяться в Загальній декларації прав людини 1948 р., Міжнародних пактах «Про громадянські і політичні права», «Про економічні, соціальні і культурні права» 1966 р., Декларації прав дитини 1989 р., Хартії Європейського Союзу про основні права 2000 р. та ін. Професор М. І. Панов вірно зазначає, що «кожна країна, яка взяла на себе обов'язок виконувати міжнародні конвенції з прав людини, повинна керуватися їхніми принципами і нормами у своєму внутрішньому законодавстві, створювати умови для здійснення і захисту прав і сво-