

**РОЛЬ ІННОВАЦІЙ І ЦИФРОВИХ ТЕХНОЛОГІЙ  
В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ  
У ЗАБЕЗПЕЧЕННІ СТАЛОГО РОЗВИТКУ  
ТА ЕКОНОМІЧНОГО ПРОЦВІТАННЯ УКРАЇНИ**

**Негребецький В. В.**

**ВСТУП**

Указом Президента України від 11 травня 2023 року № 273/2023 було схвалено Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки<sup>1</sup>. «Кожен елемент державної системи – органи правопорядку передусім – мають працювати так, щоб люди реально відчували безпеку й захищеність, щоб люди реально відчували справедливість, щоб гарантувалося на рівні інституцій, на рівні повсякденної роботи тих, по кому люди судять про державу. Довіра в державі, довіра до держави формуються з довіри до тих, хто діє від імені держави. Правоохоронці, система прокуратури – ключові в цьому. Звичайно, разом з усіма іншими, хто працює в державному апараті», – наголосив Президент Володимир Зеленський<sup>2</sup>.

Документ було спільно розроблено міжвідомчою групою, до складу якої входили очільники Офісу Генпрокурора, МВС, Міністерства юстиції, СБУ, ДБР, Національної поліції, Державної прикордонної служби, БЕБ, Державної митної служби, а також представники Офісу Президента України, Кабінету Міністрів України, міжнародні експерти від Офісу Ради Європи в Україні, КМЕС, проекту ЄС “PRAVO-JUSTICE”, відділу з правоохоронних питань Посольства США в Україні, Міжнародної організації права розвитку (IDLO). Основною метою розробників Плану було поставити у центр уваги сектору правопорядку, сектору безпеки і оборони людину, її життя, здоров’я, честь і гідність, права і охоронювані законом інтереси. Кожен

---

<sup>1</sup> Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: <https://www.president.gov.ua/documents/2732023-46733>

<sup>2</sup> Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: <https://www.gp.gov.ua/ua/posts/prezident-ukrayinii-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku>.

українець має бути впевнений, що живе у безпеці, має свободу і може розраховувати на механізми справедливості.

План визначає шість стратегічних пріоритетів, які дозволять модернізувати сектор безпеки й привести у відповідність до стандартів, яких має досягти Україна на шляху до членства у ЄС, до яких належать:

1. Дієвість і ефективність органів правопорядку та прокуратури як невід'ємної складової сектору безпеки і оборони, в межах якого вони забезпечують національну безпеку України, у тому числі громадські безпеку й порядок, протидіють злочинності з урахуванням стратегічних цілей та відповідно до стандартів прав людини і основоположних свобод, у тому числі із забезпеченням гендерної рівності.

2. Послідовна кримінальна політика, пріоритетом у якій є запобігання злочинності, невідворотність відповідальності, захист особи, суспільства та держави від кримінальних правопорушень, забезпечення інтересів потерпілого.

3. Оперативність кримінального провадження з дотриманням міжнародних стандартів та принципу верховенства права.

4. Система управління, орієнтована на результат відповідно до встановлених пріоритетів.

5. Комплексна цифрова трансформація.

6. Відкритість, прозорість, підзвітність і незалежність.

Цим документом передбачено комплексну цифрову трансформацію, зокрема:

1. Здійснення консолідованої поетапної цифрової трансформації органів правопорядку та прокуратури на основі інструментів стратегічного менеджменту, які відповідають найкращим практикам ЄС.

2. Подальше впровадження в діяльність органів правопорядку та прокуратури інноваційних технологічних досягнень, що забезпечують гнучкість операційних процесів, IT-рішення, цифрову спроможність оперативно реагувати на події та зміни й здобувати результат, орієнтований на інтереси суспільства.

3. Поетапне впровадження електронної системи управління кримінальними провадженнями шляхом комплексної заміни та модернізації обладнання, забезпечення сумісності IT-систем, безперервності роботи, доступу усіх учасників кримінального провадження та інтероперабельності.

4. Підвищення ефективності діяльності органів правопорядку та прокуратури через забезпечення більшої доступності й повноти інформації, розроблення і впровадження сервісів на Єдиному державному вебпорталі електронних послуг.

5. Впровадження заходів безпеки і захисту персональних даних відповідно до стандартів ЄС.

6. Удосконалення та впровадження більш безпечних, гнучких, спроможних і доступних систем зв'язку між усіма органами правопорядку та іншими екстреними службами (включаючи цифрове радіо: голосовий зв'язок і широкосмугове передавання даних).

7. Запровадження в усіх органах правопорядку та прокуратури уніфікованої системи особистої автентифікації та системи біометричного зіставлення із поступовим забезпеченням її сумісності з європейськими системами. Широке використання під час здійснення досудового розслідування, а також для обробки даних та аналітичної діяльності органів правопорядку і прокуратури штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень.

8. Оновлення операційних процесів за допомогою ІТ-систем, придатних для обміну даними з інституціями ЄС відповідно до стандартів ЄС.

9. Надання органам правопорядку та прокуратури для забезпечення виконання покладених на них функцій права на безпосередній спільний доступ до автоматизованих інформаційних і довідкових систем, реєстрів і баз даних, держателем (адміністратором) яких є інші державні органи.

21 сторіччя характеризується стрімким розвитком інноваційних цифрових технологій, метою яких є підвищення ефективності діяльності людини, покращення комфорту і результатів праці. Сучасні інформаційні цифрові системи і мережі, доступ до яких є у більш ніж однієї людини, як правило, мають систему захисту. Вона необхідна для забезпечення схоронності інформації, надійної працездатності й запобігання несанкціонованого доступу в систему. Для виконання покладених функцій система безпеки виконує ідентифікацію користувачів, перевіряє особу й визначає їхні повноваження.

Питанням використання інформаційних технологій та інновацій в розслідуванні кримінальних правопорушень були присвячені роботи таких вчених-юристів, як Г. К. Авдеева, Т. Я. Гнідець, Ю. І. Дмитрик, К. В. Дубонос, Н. М. Дяченко, В. А. Журавель, В. П. Захаров, А. О. Ігнатович, Р. С. Козьяков, В. О. Коновалова, Т. М. Лемеха, А. М. Лисенко, О. С. Мельник, А. О. Мороз, І. В. Олешко, Ю. В. Осадча, О. В. Рибальський, В. І. Рудешко, В. І. Соловійов, Л. І. Сопільник, І. О. Супрун, В. В. Топчій, А. О. Фесенко, В. Г. Хахановський, Л. М. Хмельничий, Р. Ю. Царьов, В. А. Швець, В. Ю. Шепітько, та інших<sup>3</sup>. Зокрема питання щодо зменшення

---

<sup>3</sup> Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності*: матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків: Право, 2020. С. 6–10. URL: <https://dspace.nlu.edu.ua/bits.../123456789/18957/1/6-10.pdf>

можливостей вчинення злочинів за допомогою, зокрема, використання сучасних інформаційних технологій було предметом окремого наукового дослідження на рівні розробки стратегії<sup>4</sup>. Головним призначенням цифрових технологій є підвищення комфортності життя людини: починаючи від побутової техніки і закінчуючи цифровою інфраструктурою міст. Протягом останніх років застосування цифрових технологій у державному секторі (сфера послуг, правоохоронна діяльність тощо) в Україні набуває все більше популярності. Smart-технології є зв'язуючим компонентом між різними сферами життя, наприклад, населеного пункту. Так, використання сучасних технологій запроваджує новий рівень координації діяльності оперативних, чергових, диспетчерських та муніципальних служб, відповідальних за громадську безпеку та повсякденну життєдіяльність місцевих громад, а також забезпечує механізми швидкого реагування відповідних служб із метою усунення наслідків правопорушень та надзвичайних ситуацій<sup>5</sup>.

Зокрема, стратегія зменшення можливостей вчинення злочинів первинно була задумана її розробниками як соціальний метод містобудування, архітектурного і дизайнерського убезпечення промислових підприємств, житлових приміщень, освітлення, банків, бізнесу, магазинів, маркування товарів, цінних предметів, використання систем контролю, створення більш ефективних фізичних перепон, бар'єрів на шляху злочинних проявів, патрулювання поліції разом із громадськістю та ін. У модернізованому вигляді цю стратегію можна представити як стратегію «захисного простору і фізичних бар'єрів для злочинності»<sup>6</sup>.

Слід відзначити, що в літературних джерелах в основному розглядалися окремі аспекти використання сучасних інноваційних цифрових технологій в створенні умов для безпечного від злочинів і інших правопорушень середовища. Разом із тим, не всі існуючі на даний час технології були предметом дослідження в цьому контексті, тому питання використання інформаційних технологій в правоохоронній

---

<sup>4</sup> Зменшення можливостей вчинення злочинів: стратегічний підхід: монографія / за заг. ред. В. В. Голіни. Харків : Право, 2020. 287 с. URL: [https://ivpz.kh.ua/wp-content/uploads/2021/09//моно\\_Стратегія-зменшення-можливостей.pdf](https://ivpz.kh.ua/wp-content/uploads/2021/09//моно_Стратегія-зменшення-можливостей.pdf)

<sup>5</sup> Денисова Т. А., Шеремет О. С. Запобіжні заходи в межах інфраструктурного, технологічного та соціального розвитку сучасних міст: завдання та рішення. *Кримінальні загрози в секторі безпеки: практики ефективного реагування* : матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право», м. Харків, 26 верес. 2019 р. Харків : Право, 2019. С. 27.

<sup>6</sup> Зменшення можливостей вчинення злочинів: стратегічний підхід: монографія / за заг. ред. В. В. Голіни. Харків : Право, 2020. 287 с. URL: [https://ivpz.kh.ua/wp-content/uploads/2021/09//моно\\_Стратегія-зменшення-можливостей.pdf](https://ivpz.kh.ua/wp-content/uploads/2021/09//моно_Стратегія-зменшення-можливостей.pdf)

діяльності потребує подальшого дослідження. Також у зв'язку з війною в Україні вкрай актуальним постає питання використання цифрових доказів в розслідуванні воєнних злочинів, оскільки на відміну від традиційних «не цифрових» доказів, всі ці документи утворюються цифровими засобами і зберігаються на цифрових платформах. У зв'язку з тим, що війна проти України з самого початку мала «гібридний» характер, тобто одночасно використовувались інформаційні атаки та диверсії в комунікативних мережах, вельми актуальним є дослідження питання інформаційної безпеки.

Метою цієї статті є з'ясування можливостей використання цифрових технологій і інновацій в правоохоронній діяльності в системі механізмів забезпечення сталого розвитку та економічного процвітання України, а також розробка на цій основі практичних рекомендацій правоохоронним органам<sup>7</sup>.

### **1. Технології боротьби з поширенням неправдивих новин**

Початок військової агресії проти України в 2022 році був тісно пов'язаний з сильним інформаційним впливом ворога на наше суспільство через технології гібридних війн. Це сталося можливим завдяки активному використанню інформаційних технологій, та впливу інноваційних інструментів обміну та передачі інформації в різноманітних інформаційних ресурсах. Але на жаль не всі технології інформаційного пошуку однаково рівноцінні і безпечні. В 2023 році компанія Google впровадила технологію Search Generative Experience (SGE)<sup>8</sup>. Цей пошуковий сервіс ретельно розроблений та навчений виявляти й представляти користувачеві високоякісні результати, які відповідають інформації у видачі та підтримують її. Об'єднавши найсучасніші поєднання мовних моделей і цілеспрямовані методики навчання, компанія Google створила пошукову систему, яка надає надійну і підтверджену інформацію. Google прагне запобігати демонстрації шкідливого, образливого або відвертого контенту у своїх системах ранжування. Технологія Search Generative Experience (SGE), на якій ґрунтуються пошук, створена саме для цього. Основна увага приділяється створенню інформативних відповідей, підтверджених

---

<sup>7</sup> Примітка. Стаття написана у межах розробки фундаментальної теми «Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі», яка досліджується фахівцями НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України.

<sup>8</sup> Новий алгоритм пошуку Google на основі AI: чого очікувати (29.10.2023). URL: <https://livepage.ua/blog/the-new-ai-powered-google-search-what-to-expect.html>.

надійними джерелами, щоб користувачі отримували правдиву і перевірену інформацію. У випадках, коли системи Google мають меншу довіру до джерела або стикаються з інформаційними прогалинами, мета полягає в тому, щоб уникнути надання знімків, згенерованих штучним інтелектом. Крім того, відверті або небезпечні теми навмисно уникаються, щоб підтримувати відповідальне та безпечне середовище пошуку.

Безумовно технології персоніфікованого підбору відомостей мають велике майбутнє, надають багато переваг особам, що навчаються або підвищують свій професійний рівень. Але нажаль будь-який інструмент в руках правопорушника може перетворитись на зло. І якщо йдеться про інформаційні технології, то сила цього лиха збільшується у багато разів. Так, месенжери, а також соціальні мережі, доступ до яких має майже кожний, надають найбільше можливостей для поширення практично будь-якої інформації. Є можливість не просто одноразово поширити новину, а запустити «ланцюжкову реакцію», коли новина багаторазово пересилається користувачами соц. мережі від однієї особи до цілої групи осіб, або навіть до інших соц. мереж.

Нажаль не всі пошукові сервіси та інформаційні ресурси здатні виявляти ненадійні джерела інформації. Новини та повідомлення можуть не відповідати дійсності<sup>9</sup>. Фейк у перекладі з англійської “fake” означає – «фальшивка», «підробка», «обман». Таким чином, фейк – це завідомо неправдива інформація. Дезінформація – відомості, що розраховані на введення особи в оману<sup>10</sup>.

Особливого значення набуває питання про відповідальність за поширення інформації, яка загрожує Національній безпеці України, а саме спрямованої на заподіяння шкоди суверенітетові, територіальній цілісності та недоторканості, обороноздатності, державній, економічній чи інформаційній безпеці держави. Таким чином, ворог намагається методично і послідовно підірвати авторитет держави і органів влади, і послабити обороноздатність країни. В пояснювальній записці до законопроекту № 9223 від 19 квітня 2023 р. «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України» повідомляється, що «російськими спецслужбами в інтересах країни-агресора наращуються зусилля із

---

<sup>9</sup> Аналітичний звіт «російський інформаційний вплив в Африці». URL: <https://срd.gov.ua/reports/analitychnyj-zvit-rosijskyj-informacijnyj-vplyv-v-afrycz/>.

<sup>10</sup> Велика українська юридична енциклопедія: У 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків : Право, 2018. 952 с.

використання такого інструменту інформаційної війни як створення на платформах соціальних мереж Facebook, Instagram і Twitter мереж облікових записів (акаунтів) (так званих бот-мереж), які містять недостовірні дані щодо користувачів, діяльність яких є координованою ззовні та об'єднана єдиною метою, зокрема такою як проведення акцій інформаційного впливу проти державних інтересів України. До таких дій вдаються і громадяни України. Так, Службою безпеки України виявлено та припинено функціонування за 2022 рік – 45 ботоферм, загальною потужністю понад 4 млн. ботів, діяльність яких поширювалась на багатомільйонні аудиторії користувачів соціальних мереж у різних регіонах України (і не лише). Разом з тим, вжитими заходами було викрито та заблоковано близько 11 тис. облікових записів, що використовувались на користь російських окупантів. Непоодинокими стали і випадки, коли користувачі облікових записів (акаунтів) видають себе за інших осіб, зокрема за представників влади, інших публічних осіб, до яких прикута особлива увага, і від імені цих осіб розміщують і поширюють в соцмережах та на інших інтернет-платформах різну неправдиву, маніпулятивну інформацію. На жаль, соціальні мережі не дуже реагують на повідомлення про фейкові профілі і сторінки, які причетні до інформаційних атак»<sup>11</sup>. Тому існує необхідність підвищити контроль з боку правоохоронців. Якщо інформація розміщена у вільному доступі, є можливість використовувати методику збирання й аналізу інформації з відкритих джерел (*Open source intelligence, OSINT*).

Центр протидії дезінформації є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106<sup>12</sup>. Центр підпорядкований Раді національної безпеки і оборони України<sup>13</sup>. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки

---

<sup>11</sup> Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України : Законопроект України від 19.04.2023 № 9223 / База даних «Законодавство України / ВР України. URL: [itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk\\_RIKKEZHmqd699\\_G6ZH0h9ZmxxhEwLZ\\_ZpXM61T0/](https://itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk_RIKKEZHmqd699_G6ZH0h9ZmxxhEwLZ_ZpXM61T0/).

<sup>12</sup> Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» : Указ Президента України від 19.03.2021 р. № 106/2021. URL: <https://www.president.gov.ua/documents/1062021-37421>.

<sup>13</sup> Центр протидії дезінформації. URL: <https://cpd.gov.ua/>

України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Зокрема, до завдань Центру належать:

виявлення та протидія дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі.

Інформаційний імунітет – це здатність ідентифікувати маніпуляцію, фейк, оцінити рівень їх небезпеки і як їм можна запобігти. Для протидії дезінформації необхідно виробити у суспільства інформаційний імунітет.

Для повноцінної боротьби з поширенням фейків і інформації, що загрожує національній безпеці країни необхідно вдосконалити законодавство. В цьому аспекті корисним є вивчення досвіду інших країн. Відомо, що з проблемою інформаційної безпеки в еру активного розвитку соціальних мереж свого часу зіткнулася провідна європейська країна – Німеччина.

Німеччина є однією з перших країн, яка запровадила санкції на рівні законодавства за поширення неправдивої інформації. Парламентом Німеччини 30 червня 2017 р. був прийнятий Закон «Про вдосконалення правозастосування в соціальних мережах» (Net Enforcement Act (NetzDG)<sup>14</sup>. Це також називається законом Про Facebook. Закон спрямований на боротьбу з дифамацією (поширення про особу неправдивої інформації, яка принижує її честь та гідність, завдає шкоди діловій репутації) і розпалюванням ненависті в Інтернеті. Закон зобов'язує платформи соціальних мереж з більш ніж 2 мільйонами користувачів встановити прозору процедуру розгляду скарг на незаконний контент і зобов'язує надавати звітність і документацію. Провайдери повинні видаляти «явно незаконний» контент протягом 24 годин, а весь незаконний контент – протягом 7 днів з моменту його публікації, в іншому випадку їм загрожує адміністративний штраф у максимальному розмірі 50 мільйонів євро. Подавачі скарг та користувачі повинні бути негайно проінформовані про прийняті рішення. Віддалений вміст

---

<sup>14</sup> Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 01.09.2017 (Закон про поліпшення правозастосування в соціальних мережах). URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>



повинен зберігатися щонайменше десять тижнів як доказ, а платформи повинні подавати звіти про прозорість роботи з нелегальним вмістом кожні шість місяців.

## **2. Проблеми використання цифрових доказів в процесі доказування воєнних злочинів і фактів агресії проти України**

Війна в Україні призвела до потреби в розслідуванні і документуванні численних фактів причетності держави-агресора до терористичної діяльності та порушення норм міжнародного права. Станом на 10 жовтня 2023 року Офісом Генеральної прокуратури зареєстровано понад 109 000 випадків воєнних злочинів широкомасштабної агресії російської федерації проти України<sup>15</sup>. Зафіксовані чисельні випадки руйнувань житлової інфраструктури, вбивств мирних жителів, мародерства та насильства.

У зв'язку з цими трагічними обставинами слід необхідно згадати роль криміналістики та судової експертизи в міжнародному співробітництві в розслідуванні злочинів<sup>16</sup>. Так, члени Литовського товариства криміналістів, Польського товариства криміналістів та Міжнародного конгресу криміналістів (Україна), 04.03.2022 р. звернулись до мирової наукової спільноти для об'єднання зусиль європейських вчених і практиків для забезпечення безпеки та миру Європейського континенту<sup>17</sup>. Вони закликають колег докласти всіх зусиль, щоб зупинити агресію проти України як найближчої сусідньої держави, допомогти нашим братам і сестрам в Україні подолати труднощі війни, показати, як важливо бути справжніми друзями, бути зараз разом. За нашу і вашу свободу, за наше спільне майбутнє в ЄС, за наші спільні плани та прагнення. В Україні атакують і бомбардують не лише військові частини, але й варварськи руйнують критичну інфраструктуру, зокрема житлові квартали, гинуть мирні жителі та навіть діти. Порушуються основні принципи міжнародного співробітництва та норми міжнародного права. Український народ захищає не лише свою країну, націю, а й незалежність інших європейських держав, а також фундаментальні принципи міжнародного права: демократію, права і свободи людини,

---

<sup>15</sup> Злочини, вчинені в період повномасштабного вторгнення рф станом на 30.11.23. URL: <https://www.gp.gov.ua/>

<sup>16</sup> Shepitko, V. Y., Shepitko, M. V. (2021) The role of forensic science and forensic examination in international cooperation in the investigation of crimes. *Journal of the National Academy of Legal Sciences of Ukraine*. № 28 (1). P. 179–186 (in English).

<sup>17</sup> Звернення. (04.03.2022). URL: <https://crimcongress.com/news/звернення/>

верховенство права та нашу спільну безпеку на даний момент і назавжди, майбутнє всього людства.

На сьогодні одним із головних завдань держави України є відсіч збройної агресії РФ та поновлення порушених прав і свобод українських громадян, а також забезпечення принципу невідворотності відповідальності винних осіб у вчиненні злочинів, пов'язаних із вторгненням російських загарбників на терени нашої країни. 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, доведення невідворотності покарання усіх воєнних злочинців, а також відшкодування шкоди, відновлення верховенства права та справедливості<sup>18</sup>.

Сучасними завданнями цифрової криміналістики є пошук і аналіз цифрових слідів, аналіз даних, збирання доказової інформації у цифровому середовищі. Під цифровими доказами необхідно розуміти фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення. В Україні створено цифрових платформ, призначених для збирання доказів воєнних злочинів в Україні, зокрема:

Застосунок eyeWitness to Atrocities від Міжнародної асоціації юристів (IBA);

Платформа WarCrimes (warcrimes.gov.ua) на базі Офісу Генерального прокурора України;

War Crime Bot – для документування доказів порушень міжнародного гуманітарного права, прав людини і злочинів;

TRIBUNAL UA – чатбот для фіксації фото-і відеодоказів вбивств, насильства, пограбувань цивільних або військових окупантами;

SaveEcoBot – чатбот для повідомлень про злочини проти навколишнього середовища, що здійснюються на території України;

Портал «Доказ» (dokaz.gov.ua);

Портал «Культурні злочини» (culturecrimes.mkp.gov.ua) для збору доказів руйнування російською армією історичних та культурних пам'яток.

Так, на єдиній загальнодержавній платформі <https://warcrimes.gov.ua/> здійснюється збирання та документування доказів про воєнні злочини

---

<sup>18</sup> Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1>

держави – агресора. Таким чином, на базі Офісу Генерального прокурора України фактично було створено сучасну платформу для документування воєнних злочинів на Україні з можливістю надання документів, фото та відео.

Найбільш відповідним для потреб збору доказів воєнних злочинів є додаток від Міжнародної асоціації юристів “eyeWitness to Atrocities”. Додаток розроблено за ініціативи Міжнародної асоціації юристів (IBA) в 2011 році. Користувачі програми завантажують свої кадри на захищений сервер для верифікації та безпечного зберігання. Фотографії та відео, зроблені за допомогою програми “eyeWitness to Atrocities”, можна легко перевірити на предмет використання в якості доказів. Крім того, eyeWitness поцікуватиметься, щоб надані користувачем фото або відео були надані компетентним органам<sup>19</sup>.

Офіс Верховного комісара ООН із прав людини та Центр з прав людини Каліфорнійського університету в Берклі у 2020 р. представили «практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права», який містить стандарти й методологічні підходи до «збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах»<sup>20</sup>. Нажаль, норми Кримінального процесуального кодексу України не передбачають окремої категорії цифрових доказів. У КПК відсутнє визначення терміна «цифрові докази», не наведено докладного порядку їх вилучення, огляду, фіксування та зберігання. Однак у слідчих і суддів часто виникають труднощі у збиранні й оцінюванні цифрових доказів через відсутність у законодавстві України їх визначення, порядку фіксування й оцінки. Це може спричинити помилки в роботі із цифровою інформацією й невизнання її допустимим і достовірним доказом у суді.

---

<sup>19</sup> Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. URL: <https://khriife-journal.org/index.php/journal/article/download/564/633>

<sup>20</sup> Гладкий Д. В. Особливості використання програми “eyeWitness to Atrocities” в Україні для фіксації воєнних злочинів рф. *Державна безпека України в умовах російської агресії: актуальні питання експертно-криміналістичного та науково-технічного забезпечення* : збірник матеріалів Всеукраїнської науково-практичної конференції, 22 серпня 2023 р.: Т. 2. Київ : ІСТЕ СБУ, 2023. С. 29–31.

### 3. Використання систем відеоспостереження і смарт-технологій

Системи відеоспостереження розповсюджені й широко використовуються в різних сферах життя людини. Відеоспостереження – це процес спостереження, що реалізується із застосуванням оптико-електронних пристроїв, призначених для візуального контролю та автоматичного аналізу<sup>21</sup>. Для контролю навколишнього середовища з метою безпеки життєдіяльності в даний час широко використовуються системи відеоспостереження – комплекс обладнання та програмного забезпечення, призначений для моніторингу поведінки, дій або інформації з метою збирання інформації, впливу, управління та координації. Завдяки автоматизації та швидкості роботи, використання біометрії для розпізнавання особи, такі технології є дуже корисними в будь-якій галузі діяльності людини, де необхідно перевірити і підтвердити особу за її біометричними характеристиками. Це може бути безпека, оборона, міграційні процеси, банківська сфера та моніторинг, та ін. Причому дати вичерпний перелік сфер застосування біометричних технологій на сьогодні вже є неможливим, оскільки сама ідея перевірки й підтвердження особи людини вже більше і більше стає привабливою і асоціюється з безпекою.

Столичне комунальне підприємство «Інформатика» впроваджено новий аналітичний модуль відеоспостереження в рамках проекту «Безпечне місто» (Kyiv Smart Safe City)<sup>22</sup>. Унікальний модуль дозволяє шукати злочинців не тільки завдяки спеціалізованим камерам розпізнавання особи. Він фіксує зображення з будь-якої камери, установленої в рамках мережі й порівнює їх з наявною базою правопорушників. Якщо система виявляє подібність, оператор відразу одержує тривожний сигнал. Отже, правоохоронці зможуть швидше відслідковувати небезпечних злочинців. До складу нового аналітичного модуля розпізнавання осіб входить аналітична система й база даних, що полягає зі списку розшукуваних людей.

В Україні проект Smart City активно впроваджується містах: Київ, Харків, Львів, Дніпро, Вінниця, Маріуполь, Чернігів та ін. Особливим видом такого проекту є “Smart Safe City” – інформаційно-аналітична програма нового покоління, що здійснює розпізнавання потенційних

---

<sup>21</sup> Рувінська В. М., Девятков В. В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні*. 2021. Т. 11. № 4. С. 331–342. URL: [http://immm.op.edu.ua/files/archive/n4\\_v11\\_2021/2021\\_4\(9\).pdf](http://immm.op.edu.ua/files/archive/n4_v11_2021/2021_4(9).pdf)

<sup>22</sup> У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. URL: [https://kyivcity.gov.ua/news/u\\_ramkakh\\_proektu\\_bezpechne\\_misto\\_zapuscheno\\_noviy\\_analitichniy\\_modul\\_videospos\\_terezhennya\\_scho\\_priskorit\\_poshuk\\_prapovorushnikov/](https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videospos_terezhennya_scho_priskorit_poshuk_prapovorushnikov/)

небезпек, аналіз ситуації в реальному часі та передачу вже опрацьованих даних про виявлені загрози терористичного, кримінального, техногенного характеру у місцях масового перебування громадян, на об'єктах критичної інфраструктури, транспортних розв'язках, операторам екстрених служб для швидкого реагування на надзвичайні події.

Про ефективність впровадження системи “Smart Safe City” можна деякою мірою зробити висновки, проаналізувавши показники вуличної злочинності в Україні. Так, останніми роками, у період поступового запровадження проекту (протягом 2017–2019 рр.) рівень злочинів, що вчиняються на вулицях, різко знизився. Для порівняння: якщо у 2013 р. було обліковано 66 971 кримінальних правопорушення, вчинених на вулицях, у 2014 р. – 66 255, у 2015 р. – 61 718, у 2016 р. – 62 064, то у 2017 р. кількість таких правопорушень склала 45 707, у 2018 р. – 42 465, а у 2019 р. – 38 139 кримінальних правопорушень<sup>23</sup>.

#### **4. Цифрові технології в діяльності Державної прикордонної служби: боротьба нелегальною міграцією**

Питання нелегальної міграції для будь-якої країни світу є проблемою державного рівня. Так, 3 18 листопада 2023 року уряд Фінляндії вирішив закрити частину східного кордону країни – прикордонні пункти пропуску Ваалімаа, Нуйямаа, Іматра та Нійрала. Фінська прикордонна служба повідомила про постійне збільшення кількості шукачів притулку, які протягом останніх днів прибувають до пунктів перетину кордону на південному сході країни<sup>24</sup>.

Цифрові технології з використанням біометричних ознак людини успішно використовуються в діяльності міграційних служб майже у всіх країнах світу. Ідея перевірки й підтвердження особи людини при перетинанні державного кордону вже більше і більше стає привабливою і асоціюється з безпекою.

Біометричні паспорти набувають все більшого поширення у світі<sup>25</sup>. Відповідно до інформації всесвітньої організації цивільної авіації (ICAO) більше 90 країн з 193 держав-членів ООН в даний час видають

---

<sup>23</sup> Зменшення можливостей вчинення злочинів: стратегічний підхід: монографія / за заг. ред. В.В. Голіни. Харків: Право, 2020. С.191. URL: [https://ivpz.kh.ua/wp-content/uploads/2021/09//моно\\_Стратегія-зменшення-можливостей.pdf](https://ivpz.kh.ua/wp-content/uploads/2021/09//моно_Стратегія-зменшення-можливостей.pdf)

<sup>24</sup> Фінляндія закриває частину пунктів пропуску на кордоні з рф через наплив біженців (16.11.2023). URL: [https://lb.ua/society/2023/11/16/584592\\_finlyandiya\\_zakriye\\_chastinu\\_punktiv.html](https://lb.ua/society/2023/11/16/584592_finlyandiya_zakriye_chastinu_punktiv.html)

<sup>25</sup> Держприкордонслужба презентувала систему фіксації біометричних даних іноземців та осіб без громадянства. URL: <https://dpsu.gov.ua/ua/news/Derzhprikorдонsluzhba-prezentuvala-sistemu-fiksacii-biometrichnih-danih-inozemciv-ta-osib-bez-gromadyanstva/>

такі документи, при цьому ще більше двадцяти держав готові до впровадження таких документів в найближчі роки.

Близько 45 країн з числа тих, які видають біометричні документи, зберігають на документах одночасно і відбитки пальців, і зображення особи, в той же час більше 30 країн використовують лише оцифроване фото власника документа. Решта країн в даний час використовують тільки зображення обличчя, але найближчим часом планують використовувати і дані дактилоскопії.

За даними ІСАО, більше 15 країн в даний час використовують автоматизовані контрольно-пропускні системи для власників електронних паспортів. Для того, щоб пройти процедуру паспортного контролю, мандрівник може скористатися «електронними воротами», які в автоматичному режимі звіряють його біометричні дані з інформацією, що зберігається на чипі документа. Серед країн, які читають (сканують) е-паспорта в аеропортах і на кордонах США, Великобританія, Сінгапур, Португалія, Нова Зеландія, Японія, Індонезія і Німеччина.

Ініціатором впровадження біометричних паспортів на державному рівні були США: в 2002 р. Конгрес США прийняв Закон про безпеку державних кордонів, відповідно до якого громадяни країн, які мали угоди зі США про безвізовий режим, могли безперешкодно в'їжджати на територію США строком до 90 днів тільки за умови наявності в них біометричних документів<sup>26</sup>.

З 2004 р. у США розпочато програму US-Visit, що передбачала введення системи зняття відбитків пальців і фотографування всіх, що прибувають в Америку іноземців (115 аеропортів, 14 морських портів, 104 контрольно-пропускних пункти, біометрична база даних більш ніж на 5 млн осіб). Більш 80 країн миру (включаючи Афганістан, Бахрейн, Кувейт, Оман, Катар, Саудівську Аравію й ОАЕ) використовують програми електронних ID-card, у яких утримуються біометричні дані<sup>27</sup>.

Найбільшою у світі системою біометричної ідентифікації в цей час є Aadhaar (Індія). Aadhaar-це індійський онлайн-сервіс ідентифікації, що надається державним агентством UIDAI. Станом на кінець жовтня 2023 р., у системі зареєстроване більш 1,3 млрд людей, що становить більше 94 % громадян Індії<sup>28</sup>.

---

<sup>26</sup> Homeland Security Act of 2002. URL: <https://www.govinfo.gov/link/plaw/107/public/296?link-type=html>

<sup>27</sup> United States Visitor and Immigrant Status Indicator Technology (US-VISIT). URL: <https://www.epic.org/privacy/us-visit/>

<sup>28</sup> Unique Identification Authority Of India. URL: <https://uidai.gov.in> (дата доступу 30.11.23).

3 березня 2018 року посольство Саудівської Аравії в Україні запровадило обов'язкову процедуру зняття відбитків пальців у всіх бажаючих отримати візу до країни<sup>29</sup>. Процедура проводиться після подачі документів в попередньо призначений день і час.

На Україні 20.11.2012 р. було прийнято Закон «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» № 5492-VI, відповідно до якого передбачено введення документів з електронним носієм, на якому передбачається розміщення біометричних даних про особу<sup>30</sup>. В 2017 році Уряд України затвердив Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства<sup>31</sup>. Документом визначено, що це автоматизована система, створена в інтересах національної безпеки, економічного добробуту та прав людини, за допомогою якої забезпечується встановлення особи іноземця та особи без громадянства, які в'їжджають в Україну, виїжджають з України, здійснення контролю за додержанням ними правил перебування на території нашої держави.

Державна прикордонна служба у грудні 2017 р. презентувала систему фіксації біометричних даних іноземців та осіб без громадянства<sup>32</sup>. Демонстрація роботи системи відбулася в столичному аеропорту «Київ». Ця система фіксації біометричних даних іноземців та осіб без громадянства розгортається прикордонним відомством на виконання Указу Президента України від 30 серпня 2017 року № 256 «Про рішення Ради національної безпеки та оборони України від 10 липня 2017 року «Про посилення контролю за в'їздом в Україну, виїздом з України іноземців та осіб без громадянства, додержання ними правил перебування на території України». Вона є однією з підсистем відомчої автоматизованої системи прикордонного контролю. Держприкордонслужба активно працює над вдосконаленням безпекової складової на кордонах України. Сьогодні технічні засоби Держприкордонслужби

---

<sup>29</sup> Візу до Саудівської Аравії українцям необхідно отримати перед поїздкою. URL: <https://tourpoint.com.ua/ua/vizy/asia/saudi-arabia>

<sup>30</sup> Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 № 5492-VI . URL: <https://zakon.rada.gov.ua/go/5492-17>

<sup>31</sup> Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства : Постанова КМУ від 27.12.2017 № 1073. URL: <https://zakon.rada.gov.ua/laws/show/1073-2017-п#Text>

<sup>32</sup> Держприкордонслужба презентувала систему фіксації біометричних даних іноземців та осіб без громадянства. URL: <https://dpsu.gov.ua/ua/news/Derzhprikorдонsluzhba-prezentuvala-sistemu-fiksacii-biometrichnih-danih-inozemciv-ta-osib-bez-gromadyanstva/>

дозволяють зчитувати виготовлені за міжнародними стандартами ІКАО закордонні паспорти, в тому числі з вбудованим чіпом, ID-картки та водійські посвідчення. При цьому постійно вивчається досвід передових країн світу, європейських та американських партнерів щодо побудови систем автоматизації паспортного контролю. Кращі зразки обладнання впроваджуються у відомчу інформаційно-телекомунікаційну систему. 157 діючих пунктів пропуску обладнано засобами для зчитування інформації з біометричних документів, а 126 пунктів пропуску підключено до баз даних Інтерполу. З серпня 2017 року інформаційна система прикордонного відомства автоматично підраховує кількість дозволених діб перебування іноземців в Україні.

Запуск системи фіксації біометричних даних Держприкордонслужби – це ще один крок щодо покращення безпекової складової при перетинанні кордону та вдосконалення системи прикордонного контролю. під час паспортного контролю інспектори Держприкордонслужби здійснюватимуть перевірку паспортних документів іноземців, в тому числі за базами Інтерполу. Також відбуватиметься зчитування інформації (відбитки пальців) за допомогою рідерів, яка надходитиме до підсистеми обробки біометричних даних відомства. Крім того, через міжвідомчу інформаційно-телекомунікаційну систему «Аркан» вона надходитиме до Національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства Державної міграційної служби. При повторному перетині особою кордону здійснюватиметься процес ідентифікації особи. При цьому інспектор бачитиме чи здавала людина свої біометричні дані і здійснюватиме їх перевірку. У разі не співпадіння даних особу буде направлено на додатковий контроль для з'ясування обставин.

Отже, використання біометричних технологій в діяльності Держприкордонслужби, Державної міграційної служби України є вельми необхідним для контролю за міграційними процесами.

## **5. Використання цифрових технологій в розслідуванні кримінальних правопорушень**

Експертна служба Міністерства внутрішніх справ України є системою державних спеціалізованих установ судової експертизи. Експертна служба МВС є найбільшою мережею судово-експертних установ в Україні та налічує 24 адміністративно – лабораторних комплекси. У дев'яти обласних центрах було створено та забезпечено сучасним обладнанням повнопрофільні адміністративні лабораторні комплекси судової експертизи (ДНДЕКЦ МВС, Київський, Харківський, Вінницький, Волинський, Запорізький, Івано-Франківський, Львівський, та Миколаївський). «Експертна служба МВС України



виконує 79 видів експертних досліджень та нараховує значну кількість підготовлених фахівців по 79 експертних спеціальностях<sup>33</sup>.

При провадженні судових експертиз з метою ідентифікації причетних осіб використовуються цифрові технології біометричної ідентифікації. Яскравим прикладом використання біометричної технології в діяльності судового експерта є генотипоскопічна експертиза, або ДНК-аналіз, тобто дослідження мікрослідів на клітинному рівні. Це дозволяє ідентифікувати злочинця по слідах біологічного походження: крові, слини, (сперми), клітинах епітелію, частинах тканин і органів людини, волосся. Істотною особливістю є тісна інтеграція криміналістичних обліків та інформаційних біометричних систем. Так, актуальним аспектом використання судової генетики в системі кримінального правосуддя є створення та розширення централізованих національних баз даних. Такі бази містять генетичні профілі, які встановлюються і зберігаються відповідно до критеріїв, визначених у законодавстві кожної країни використання криміналістичних обліків генетичних ознак людини з інформаційно-пошуковими автоматизованими системами<sup>34</sup>. Автоматизовані криміналістичні обліки призначені для накопичування та зберігання отриманих в процесі дослідження даних, з метою подальшої перевірки шляхом порівняння їх з тими даними, що вже зберігаються в базі. Автоматизований облік генетичних ознак людини функціонує на центральному та обласних рівнях. Створення криміналістичних обліків генетичних ознак людини сприяло проведенню генетичного аналізу отриманих на місці злочину біологічних зразків, що багато в чому спростило роботу слідчих. Вони отримали надійний інструмент, що дозволяє ідентифікувати злочинця або його жертву, добувати незаперечні докази і розкривати злочини.

Судова молекулярно-генетична експертиза розв'язує завдання ідентифікації особи методом ДНК-аналізу, в т.ч.: встановлення приналежності об'єктів біологічного походження (кров, сперма, слина, волосся, м'язова та кісткова тканини) певній особі, встановлення слідів біологічного походження конкретної особи у змішаних слідах, встановлення ідентичності останків у випадках розчленування трупа та ідентифікації жертв катастроф, коли живі близькі родичі, визначення спадковості певних генетичних ознак людини (біологічна

---

<sup>33</sup> Про Експертну службу МВС. URL: <https://dndekc.mvs.gov.ua/про-експертну-службу-мвс/>

<sup>34</sup> Ірина Єпринцева Актуальні питання криміналістичних обліків генетичних ознак людини. *Молодий вчений*. № 9 (85) (2020). URL: <https://molodyivchenyi.ua/index.php/journal/article/view/703/679>

спорідненість) – встановлення батьків дитини у випадках спірного батьківства, дітовбивства, крадіжки, підміни дітей<sup>35</sup>.

Ідентифікація за ДНК ґрунтується на унікальності послідовності дезоксирибонуклеїнової кислоти у кожної людини. Процес починається з підготовки зразка ДНК індивідуума (що звичайно називається «контрольним зразком»). Для відібрання зразків використовується щічний мазок, а також кров, слина, інші виділення організму людини, тканини. Контрольний зразок з використанням спеціальної біометричної технології і обладнання аналізується для створення ДНК-профілю людини. Такий профіль потім можна порівняти з іншим зразком, щоб визначити, чи є генетична тотожність. Процес отримання ДНК-профілю займає певний час. Тому сам метод для автоматичної ідентифікації особи в реальному часі ще не є придатним. Але для проведення судово-експертних досліджень метод ДНК-аналізу став поширеним. Метод використовується при провадженні судових експертиз, наприклад за кримінальними провадженнями при розслідуванні умисних вбивств<sup>36</sup>. Зокрема, в Харкові дослідження ДНК проводяться з 2014 року в лабораторії судово-біологічних досліджень Харківського НДЕКЦ МВС України. ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса» отримав мобільну ДНК лабораторію для експрес-аналізу ДНК. Досліджувати зразки почали у вересні 2023 – після отримання від французького уряду мобільної лабораторії<sup>37</sup>.

## ВИСНОВКИ

Використання цифрових технологій і інноваційних цифрових продуктів в правоохоронній діяльності є необхідною умовою для забезпечення сталого розвитку та економічного процвітання України, подолання наслідків війни і післявоєнного відновлення нашої країни.

Проведення дослідження дозволяє визначити напрями використання цифрових технологій і систем в правоохоронній діяльності:

1. В системі механізмів Національної безпеки і оборони України.

---

<sup>35</sup> Види судових експертиз, які проводяться у лабораторії біологічних досліджень та питання які вони вирішують : Інформаційний лист. НДЕКЦ МВС України, Київський НДЕКЦ МВС України, 2017. URL: [https://ndekc.kiev.ua/wp-content/uploads/2017/02/Інф.лист\\_ДНК-2017.pdf](https://ndekc.kiev.ua/wp-content/uploads/2017/02/Інф.лист_ДНК-2017.pdf)

<sup>36</sup> Вирок Хмельницький міськрайонний суд Хмельницької області від 22.12.2021 р. База даних «Єдиний реєстр судових рішень». URL: <https://reyestr.court.gov.ua/Review/102204614>.

<sup>37</sup> «Брат шукає зниклого безвісти брата». Як судові експерти ідентифікують вбитих на Харківщині (19.01.23). URL: <https://suspilne.media/361804-brat-sukae-zniklogo-bezvisti-brata-ak-sudovi-eksperti-identifikuut-vbitih-na-harkivsini/>

2. В системах контролю та запобігання кримінальним правопорушенням в зоні бойових дій;
3. В автоматизованих системах відеоспостереження й розшуку з технологією біометричної ідентифікації;
4. В автоматизованих системах, що забезпечують використання біометричних документів для посвідчення особи (наприклад, біометричний паспорт);
5. В автоматизованих криміналістичних обліках Експертної служби МВС;
6. В судово-експертній діяльності при проведенні окремих видів ідентифікаційних досліджень (ідентифікацію особи за звуко- та відеозаписом, ДНК-аналіз);
7. В системах контролю за поширенням неправдивої інформації (фейків) в соціальних мережах та інформаційному просторі.

Використання цифрових технологій дозволить розширити можливості своєчасного повідомлення правоохоронців про правопорушення, розшуку і ідентифікації злочинців, оптимізувати процес розслідування кримінальних правопорушень. Очищення інформаційного простору від фальшивих новин і фейків є обов'язковою умовою подолання війни і перемоги. Для ефективної боротьби з поширенням неправдивої інформації за допомогою інноваційних цифрових технологій необхідно використовувати досвід провідних європейських країн, підвищити роль цифрових інструментів виявлення і протидії дезінформації, в тому числі в роботі правоохоронних органів, із залученням профільних науково-дослідних установ та провідних фахівців в галузі кримінального права адаптувати чинне законодавство до вимог цифрової епохи.

## **АНОТАЦІЯ**

Стаття присвячена дослідженню можливостей використання цифрових технологій і інновацій в діяльності правоохоронних органів в системі механізмів забезпечення сталого розвитку та економічного процвітання України. Розглянуто можливості таких технологій в діяльності як в процесі превентивної діяльності правоохоронних органів, так і під час досудового розслідування кримінальних правопорушень. Передусім, завдяки цим технологіям розширяються можливості своєчасного повідомлення про правопорушення, розшуку і ідентифікації злочинців. На основі аналізу історії впровадження інформаційних технологій і систем безпеки в правоохоронну діяльність, прикладів впровадження новітніх цифрових технологій і систем, результатів профільних наукових досліджень щодо впровадження систем безпеки (стратегія «захисного простору і фізичних бар'єрів для злочинності») запропоновано системний підхід до впровадження інновацій і цифрових

технологій в екосистемі міст. В роботі приділяється увага проблемі дезінформації в соціальних мережах та інформаційному просторі. Автор дійшов висновку, що для ефективної боротьби з поширенням неправдивої інформації за допомогою інноваційних цифрових технологій необхідно використовувати досвід провідних європейських країн, підвищити роль цифрових інструментів виявлення і протидії дезінформації, в тому числі в роботі правоохоронних органів, із залученням профільних науково-дослідних установ та провідних фахівців в галузі кримінального права адаптувати чинне законодавство до вимог цифрової епохи.

### Література

1. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки : Указ Президента України від 11.05.2023 № 273/2023. URL: <https://www.president.gov.ua/documents/2732023-46733>.

2. Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: <https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku>.

3. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 6–10. URL: <https://dspace.nlu.edu.ua/bits.../123456789/18957/1/6-10.pdf>

4. Shepitko, V. Y., Shepitko, M. V. (2021) The role of forensic science and forensic examination in international cooperation in the investigation of crimes. *Journal of the National Academy of Legal Sciences of Ukraine*. № 28 (1). P. 179–186.

5. Шевчук В. М. Проблеми цифровізації криміналістики в умовах російсько-української війни. *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, Від. дослідж. Проблем крим. проц. та судоустрою. Харків : Право, 2022. С. 127–140. URL: [https://drive.google.com/file/d/1xeu-J0LA\\_70FtmwPPeqrjI8Oml6H34Ou/view/](https://drive.google.com/file/d/1xeu-J0LA_70FtmwPPeqrjI8Oml6H34Ou/view/)

6. Shevchuk, Viktor M. Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*. 2020. № 27 (2). P. 170–183.

7. Zhuravel, Volodymyr A. Reliability evaluation of a forensic expert's opinion: World practices and Ukrainian realities / Zhuravel, V. A., Kono-

valova, V. E., Avdeyeva, G. K. *Journal of the National Academy of Legal Sciences of Ukraine*. 2021. № 28 (2). P. 252–261.

8. Зменшення можливостей вчинення злочинів: стратегічний підхід: монографія / за заг. ред. В. В. Голіни. Харків : Право, 2020. 287 с. URL: [https://ivpz.kh.ua/wp-content/uploads/2021/09//моно\\_Стратегія-зменшення-можливостей.pdf](https://ivpz.kh.ua/wp-content/uploads/2021/09//моно_Стратегія-зменшення-можливостей.pdf)

9. Денисова Т. А., Шеремет О. С. Запобіжні заходи в межах інфраструктурного, технологічного та соціального розвитку сучасних міст: завдання та рішення. *Кримінальні загрози в секторі безпеки: практики ефективного реагування* : матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право», м. Харків, 26 верес. 2019 р. Харків : Право, 2019. С. 25–29.

10. Новий алгоритм пошуку Google на основі AI: чого очікувати (29.10.2023). URL: <https://livepage.ua/blog/the-new-ai-powered-google-search-what-to-expect.html>.

11. Аналітичний звіт «російський інформаційний вплив в Африці». URL: <https://cpd.gov.ua/reports/analitychnyj-zvit-rosijskyj-informacijnyj-vplyv-v-afryczji/>.

12. Велика українська юридична енциклопедія: У 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків : Право, 2018. 952 с.

13. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України: Законопроект України від 19.04.2023 № 9223 / База даних «Законодавство України / ВР України. URL: [https://itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk\\_RIKKEZHmqd699\\_G6ZH0h9ZmxhEwLZ\\_ZpXM61T0/](https://itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk_RIKKEZHmqd699_G6ZH0h9ZmxhEwLZ_ZpXM61T0/)

14. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» : Указ Президента України від 19.03.2021 р. № 106/2021. URL: <https://www.president.gov.ua/documents/1062021-37421>.

15. Центр протидії дезінформації. URL: <https://cpd.gov.ua/>.

16. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 01.09.2017 (Закон про поліпшення правозастосування в соціальних мережах). URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>.

17. Злочини, вчинені в період повномасштабного вторгнення рф станом на 30.11.23. URL: <https://www.gp.gov.ua/>

18. Звернення. (04.03.2022). URL: <https://crimcongress.com/news/звернення/>.

19. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. URL:

<http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1>.

20. Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. URL: <https://khrife-journal.org/index.php/journal/article/download/564/633>.

21. Гладкий Д. В. Особливості використання програми “eyeWitness to Atrocities” в Україні для фіксації воєнних злочинів рф. *Державна безпека України в умовах російської агресії: актуальні питання експертно-криміналістичного та науково-технічного забезпечення* : збірник матеріалів Всеукраїнської науково-практичної конференції, 22 серпня 2023 р.: Т. 2. Київ : ІСТЕ СБУ, 2023. С. 29–31.

22. Рувінська В. М., Девятков В. В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні*. 2021. Т. 11, № 4. С. 331–342. URL: [http://immm.op.edu.ua/files/archive/n4\\_v11\\_2021/2021\\_4\(9\).pdf](http://immm.op.edu.ua/files/archive/n4_v11_2021/2021_4(9).pdf)

23. Швець В. А., Фесенко А. А. Основні біометричні характеристики, сучасні системи і технології біометричної аутентифікації. *Безпека інформації (Ukrainian Scientific Journal of Information Security)*. 2013. № 2. С. 99–111.

24. Biometrics Research Group. URL: <https://biometrics.cse.msu.edu>.

25. Biometrics Institute. URL: <https://biometricsinstitute.org>.

26. Biometrics. URL: <https://biometrics.com/>.

27. У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. URL: [https://kyivcity.gov.ua/news/u\\_ramkakh\\_proektu\\_bezpechne\\_misto\\_zapuscheno\\_noviy\\_analitichniy\\_modul\\_videosposterezheniya\\_scho\\_priskorit\\_poshuk\\_pravoporushnikov/](https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezheniya_scho_priskorit_poshuk_pravoporushnikov/).

28. Фінляндія закриває частину пунктів пропуску на кордоні з РФ через наплив біженців (16.11.2023). URL: [https://lb.ua/society/2023/11/16/584592\\_finlyandiya\\_zakriie\\_chastinu\\_punktiv.html](https://lb.ua/society/2023/11/16/584592_finlyandiya_zakriie_chastinu_punktiv.html).

29. Держприкордонслужба презентувала систему фіксації біометричних даних іноземців та осіб без громадянства. URL: <https://dpsu.gov.ua/ua/news/Derzhprikordonsluzhba-prezentovala-sistemu-fiksacii-biometrichnih-danih-inozemciv-ta-osib-bez-gromadyanstva/>.

30. Homeland Security Act of 2002. URL: <https://www.govinfo.gov/link/plaw/107/public/296?link-type=html>

31. United States Visitor and Immigrant Status Indicator Technology (US-VISIT). URL: <https://www.epic.org/privacy/us-visit/>.

32. Unique Identification Authority Of India. URL: <https://uidai.gov.in>.

33. Візу до Саудівської Аравії українцям необхідно отримати перед поїздкою. URL: <https://tourpoint.com.ua/ua/vizy/asia/saudi-arabia>.

34. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 № 5492-VI. URL: <https://zakon.rada.gov.ua/go/5492-17>.

35. Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства : Постанова КМУ від 27.12.2017 № 1073. URL: <https://zakon.rada.gov.ua/laws/show/1073-2017-п#Text>.

36. Про Експертну службу МВС. URL: <https://dnдекс.mvs.gov.ua/про-експертну-службу-мвс/>.

37. Осуховський Р. В., Кизименко С. Г. Використання технічних засобів дактилоскопіювання для ідентифікації осіб. *Використання досягнень сучасної науки й техніки в розкритті злочинів* : матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лютого 2021 р.). С. 174–179. URL: <https://www.nai.au.kiev.ua/files/kafedru/ord/2021/ks-250221.pdf>.

38. Ірина Спринцева Актуальні питання криміналістичних обліків генетичних ознак людини. *Молодий вчений*. № 9 (85) (2020). URL: <https://molodyivchenyi.ua/index.php/journal/article/view/703/679>; <https://doi.org/10.32839/2304-5809/2020-9-85-50>.

39. Види судових експертиз, які проводяться у лабораторії біологічних досліджень та питання які вони вирішують: Інформаційний лист. ДНДЕКЦ МВС України, Київський НДЕКЦ МВС України, 2017. URL: [https://ndекс.kiev.ua/wp-content/uploads/2017/02/Інф.лист\\_ДНК-2017.pdf](https://ndекс.kiev.ua/wp-content/uploads/2017/02/Інф.лист_ДНК-2017.pdf)

40. Вирок Хмельницький міськрайонний суд Хмельницької області від 22.12.2021 р. База даних «Єдиний реєстр судових рішень». URL: <https://reyestr.court.gov.ua/Review/102204614>.

41. «Брат шукає зниклого брата». Як судові експерти ідентифікують вбитих на Харківщині (19.01.23). URL: <https://suspilne.media/361804-brat-sukae-zniklogo-bezvisti-brata-ak-sudovi-eksperti-identifikuut-vbitih-na-harkivsini/>.

#### **Information about the author:**

**Nehrebetskyi Vladyslav Valerevych,**

Ph. D. in Law,

Researcher at Academician Stashis Scientific Research Institute  
for the Study of Crime Problems

National Academy of Law Sciences of Ukraine

49, Pushkinska str., Kharkiv, 61002, Ukraine,

Associate Professor at the Department of Criminalistics

Yaroslav Mudryi National Law University

77, Pushkinska str., Kharkiv, 61024, Ukraine