УДК 342.951
DOI https://doi.org/10.32782/2311-8040/2025-3-8

Здебський Дмитро Володимирович,
аспірант кафедри кібербезпеки та інформаційного забезпечення,
Одеський державний університет внутрішніх справ,
вулиця Успенська, 1, Одеса, 65000, Україна
ORCID: https://orcid.org/0009-0004-5279-1024

ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ БАЗ ДАНИХ ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОВЕДЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ

Анотація. *У статті здійснено комплексне науково-правове дослідження засад формування та функціонування баз даних поліграфологічних досліджень як інструменту цифровізації правоохоронних органів України. Досліджено правове регулювання порядку збирання, обробки, зберігання та використання інформації, отриманої за результатами проведення поліграфологічних досліджень у діяльності органів сектору безпеки і оборони України. Проаналізовано нормативні вимоги національного та міжнародного законодавства. Обґрунтовано доцільність розробки та функціонального розмежування двох типів інформаційних систем: відомчої бази даних, що накопичує великі масиви персоніфікованої інформації з метою забезпечення кадрової роботи правоохоронних органів із дотриманням принципів Big Data-аналітики, та спеціалізованої бази, інтегрованої до системи управління цифровими доказами (Digital Evidence Management System), для забезпечення проведення кримінального аналізу. Підкреслено важливість забезпечення достовірності, цілісності, збереження та захисту результатів поліграфологічних досліджень в умовах цифровізації сектору безпеки й оборони України. Обґрунтовано, що формування таких баз даних повинно супроводжуватися запровадженням спеціальних політик конфіденційності, технічних засобів захисту, чітким розподілом доступу та інституційними механізмами контролю за обробкою даних. У межах аналітично-розвідувального підходу до правоохоронної діяльності (Intelligence-Led Policing) запропонована модель формування баз даних поліграфологічних досліджень, здатна посилити ефективність кримінального аналізу шляхом своєчасного виявлення ризиків, формування поведінкових профілів і підтримки процесів ухвалення управлінських рішень на основі доказової та перевіреної інформації.*

Зроблено висновок, що формування баз даних поліграфологічних досліджень має ґрунтуватися на чітких правових засадах із дотриманням міжнародних та національних стандартів захисту персональних даних, що, своєю чергою, створює передумови для їх ефективного використання в кримінальному аналізі, оперативно-розшуковій та контррозвідувальній діяльності в структурі аналітичної моделі Intelligence-Led Policing.

Ключові слова: база даних, інформаційна безпека, кримінальний аналіз, персональні дані, поліграф, цифрова трансформація, Big Data, DEMS, ILP, GDPR.

Zdebskyi Dmytro. Legal framework for the formation of polygraph examination databases to support criminal analysis

Abstract. *The article presents a comprehensive legal and scholarly analysis of the foundations for the formation and functioning of polygraph examination databases as a tool for the digital transformation of Ukraine's law enforcement agencies. It explores the legal regulation of the collection, processing, storage, and use of information obtained from polygraph examinations within the activities of security and defense sector bodies. National and international legal standards are examined. The article substantiates the need to develop and functionally differentiate two types of information systems: (1) a departmental database that accumulates large volumes of personalized data for personnel-related purposes, based on Big Data analytics principles; and (2) a specialized database integrated into the Digital Evidence Management System (DEMS) to ensure support for criminal analysis. Emphasis is placed on the importance of ensuring the accuracy, integrity, preservation, and protection of polygraph data amid the digitalization of the security and defense sector. It is argued that the creation of such databases must be accompanied by the implementation of privacy policies, technical safeguards, regulated access control, and institutional mechanisms for data processing oversight. Within the framework of the Intelligence-Led Policing (ILP) model, the proposed approach to polygraph data management can enhance the effectiveness of criminal analysis by enabling timely threat detection, behavioral profiling, and informed decision-making based on verified and evidence-*

ISSN 2311-8040

based information. It is concluded that the formation of polygraph examination databases must be based on clear legal foundations and comply with international and national standards for personal data protection, thus creating the prerequisites for their legitimate and effective use in criminal analysis, operational, and counterintelligence activities within the ILP structure.

Key words: *database, information security, criminal analysis, personal data, polygraph, digital transformation, Big Data, DEMS, ILP, GDPR.*

Вступ. Цифровізація правоохоронних органів та спеціальних служб України в умовах правового режиму воєнного стану потребує оновлення підходів до збору, обробки, зберігання та використання спеціалізованих інформаційних масивів. Особливого значення набувають дані, сформовані за результатами поліграфологічних досліджень. Формування та функціонування відповідних баз даних – це нове комплексне явище на стику адміністративного, інформаційного та кримінального права, що потребує системного нормативно-правового врегулювання. Наразі в українському законодавстві відсутній цілісний підхід до правового регулювання використання результатів поліграфологічних досліджень як джерела інформації для аналітиків правоохоронних органів. Зокрема, не визначено правовий статус такої інформації, не встановлено порядок її обробки, критерії правомірного включення до відомчих інформаційних систем, а також умови її подальшого використання в кримінальному аналізі. З активним впровадженням поліграфологічних досліджень у практику добору персоналу, службових перевірок, забезпечення оперативно-розшукової та контррозвідувальної діяльності виникає нагальна потреба у нормативному врегулюванні механізмів інтеграції відповідних даних до цілісних цифрових систем управління доказами та аналітичними процесами. Із запровадженням кримінального аналізу як складника інформаційно-аналітичної підтримки діяльності правоохоронних органів та спеціальних служб, орієнтованих на модель Intelligence-Led Policing (далі – ILP), актуалізується залучення нових джерел структурованих та неструктурованих даних. Перспективним напрямом є інтеграція результатів поліграфологічних досліджень до інформаційного простору аналітичних систем правоохоронних органів в умовах роботи з великими даними (Big Data), зокрема в системи управління цифровими доказами (Digital Evidence Management Systems, далі – DEMS). Така інформація, поєднана з результатами оперативного обліку, цифровими слідами, відкритими джерелами (OSINT) та іншими масивами, може використовуватись для проведення кримінального аналізу, прогнозування ризиків, аналізу поведінкових тенденцій та верифікації аналітичних гіпотез. Правове забезпечення використання даних поліграфологічних досліджень у кримінальному аналізі потребує врахування низки принципових вимог: законності, пропорційності, мінімізації обсягу оброблюваних персональних даних, цільового призначення та забезпечення інформаційної безпеки. З огляду на це, виникає потреба у гармонізації національного законодавства із загальноєвропейськими стандартами у сфері захисту персональних даних, зокрема Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [1], який встановлює єдині вимоги до обробки персональних даних у межах Європейського Союзу та Директиви (ЄС) 2016/680 від 27 квітня 2016 року щодо обробки персональних даних правоохоронними органами [2]. Актуальним є створення спеціальних нормативно-правових актів, що визначатимуть статус, режим зберігання, доступ, захист та аналітичне використання інформації, отриманої за результатами поліграфологічних досліджень.

Метою статті є теоретико-правове обґрунтування необхідності формування цілісного нормативно-правового механізму зберігання, обробки та використання даних результатів поліграфологічних досліджень правоохоронними органами та спеціальними службами з

метою забезпечення ефективного проведення кримінального аналізу в умовах цифровізації сектору безпеки й оборони України та впровадження моделі ILP.

Матеріали та методи. Методологічною основою дослідження стала сукупність загальнонаукових, спеціально-юридичних та інформаційно-аналітичних методів, що застосовувалися у взаємозв'язку для всебічного аналізу правових засад формування баз даних поліграфологічних досліджень як інструменту кримінального аналізу. Використано діалектичний підхід до правового регулювання в контексті цифровізації та впровадження моделі Intelligence-Led Policing. Застосовано аналіз нормативно-правових актів (національних і міжнародних), порівняльно-правовий метод (для зіставлення з іноземним досвідом), контент-аналіз наукових джерел, інтерпретацію правових норм і системний підхід до вивчення взаємозв'язків між правовими, технічними та організаційними чинниками. Практична цінність дослідження підкріплюється авторським досвідом поліграфолога в умовах воєнного стану, що дозволило врахувати ризики та вимоги до безпеки обробки даних.

Результати. Від початку повномасштабного вторгнення російських окупаційних військ застосування поліграфа в Україні суттєво активізувалося, зокрема в секторі безпеки і оборони, де він зарекомендував себе як ефективний інструмент виявлення колаборантів, корупціонерів, шпигунів тощо. Це зумовило створення спеціалізованих поліграфологічних підрозділів у секторі безпеки і оборони України, що привело до збільшення документообігу в цій сфері. Ця тенденція виявила нагальну потребу в цифровізації сфери документообігу поліграфологічних підрозділів та актуалізувала проблему відсутності чітко визначеного правового регулювання щодо обробки, зберігання й формування відповідних баз даних.

Указ Президента України від 11 травня 2023 року № 273/2023 (далі – Указ) «Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки» встановив стратегічну основу реформування органів правопорядку як складової частини сектору безпеки і оборони України [3]. Відповідно до Указу важливим складником реформ є посилення цифровізації та модернізації інформаційної інфраструктури органів правопорядку, що безпосередньо стосується формування та функціонування автоматизованих баз даних. Це створює правову та організаційну основу для впровадження сучасних інформаційних систем. Указ акцентує увагу на впровадженні ризик-орієнтованих підходів і розвитку інформаційно-аналітичної діяльності, що є ключовими елементами концепції ILP. Ефективне використання баз даних поліграфологічних досліджень у кримінальному аналізі сприяє формуванню точних профілів ризику, оперативному виявленню загроз та прийняттю обґрунтованих управлінських рішень на тактичному й оперативному рівнях. Автоматизовані бази даних у поєднанні з аналітичною платформою ILP підвищують прозорість, оперативність та результативність діяльності органів правопорядку, дозволяючи максимально ефективно розподіляти ресурси і формувати проактивні стратегії забезпечення безпеки. Указ створює комплексне нормативно-правове та організаційне підґрунтя для формування, захисту й ефективного використання баз даних поліграфологічних досліджень в Україні, що відповідає сучасним вимогам кримінального аналізу, міжнародним стандартам цифрової трансформації, захисту персональних даних та кібербезпеки, а також забезпечує інтеграцію цих ресурсів у системи аналітично-розвідувального управління в секторі безпеки і оборони відповідно до принципів ILP.

Нами проведено дослідження щодо перспективи створення та впровадження відомчих баз даних результатів поліграфологічних перевірок на базі одного з підрозділів спеціального призначення сектору безпеки і оборони України, на який покладаються обов'язки внутрішнього контроль військового формування. У цьому підрозділі з 2017 року запроваджено поліграфологічні дослідження за валідними методиками, які відповідають міжнародним стандартам. Зона відповідальності даного підрозділу поширюється на Вінницьку, Одеську,

Миколаївську, Херсонську та Запорізьку області. Поліграфологічні дослідження даним підрозділом проводились переважно за трьома напрямами:

1. Кадрове забезпечення – поліграфологічне дослідження спрямоване на сприяння у відборі, професійній підготовці, розподілі та просуванні по службі персоналу відомства;

2. Забезпечення внутрішньої безпеки – поліграфологічне дослідження спрямоване на виявлення, та припинення правопорушень, вчинюваних персоналом відомства, а також запобігання їм;

3. Забезпечення власної безпеки – поліграфологічне дослідження для забезпечення комплексу організаційних і правових заходів, спрямованих на захист персоналу відомства та їхніх близьких родичів від протиправних посягань, пов'язаних із виконанням службових обов'язків, зокрема загроз життю, здоров'ю, житлу та майну. У межах цього напряму поліграфологічне дослідження також проводиться для сприяння в проведенні контррозвідувальних заходів в інтересах забезпечення охорони державної таємниці, виявлення впливу іноземних спецслужб, запобігання витоку службової інформації та забезпечення стійкості відомства від зовнішнього втручання.

У своїй діяльності залежно від завдань та наявної інформації даний підрозділ використовує такі дослідження:

1. Діагностичні: в межах службового розслідування або для забезпечення оперативно-розшукових / контррозвідувальних заходів, щодо конкретної події (інциденту) або звинувачення, з метою встановлення участі особи в події, що досліджується, або достовірності свідчень щодо знання фактичних обставин [4, с. 15]. Переважно застосовуються методики: Федеральний двозонний тест «You Phase» та Федеральний тест порівняння зон «Federal ZCT».

2. Скринінгові: в межах службової або кадрової перевірки, у разі відсутності повідомлення щодо події (інциденту) або звинувачення [4, с. 15]. Переважно застосовуються методики: Модифікований тест основних запитань ВПС США «AFMGQT», Скринінговий тест із запитаннями спрямованого обману «DLST» та Британський однотемний скринінговий тест «BOST».

Оцінка результатів поліграфологічного дослідження в даному підрозділі здійснюється за «Емпіричною Системою Оцінки – Мультиноміальною» («ESS-M»). Дана система використовує Баєсовий довірчий інтервал для апостеріорних шансів правди за допомогою методу Клоперу-Пірсона та альфою, що дорівнює 5 % для правди та обману, а результати поліграфологічного дослідження розраховані з використанням апріорної ймовірності 50 %, для якої апріорні шанси правди були 1:1 [2]. Дана методика оцінки дає можливість у відсотковому або шансовому вигляді зробити науково обґрунтований висновок.

Відповідно до Мета-аналітичного дослідження критеріальної точності валідних поліграфологічних методик Американської поліграфологічної асоціації, точність методик, які використовуються даним підрозділом, така:

Діагностичні: точність у межах 90,4 – 92,1 % [5], невизначений результат (отримані фізіологічні дані не містять достатньої або узгодженої діагностичної інформації, на основі якої можна було би прийняти остаточне рішення [4, с. 21]) в межах 9,8–19,2 % [5], хибно негативна помилка (помилкове визначення поліграфологом неправдивої особи як правдивої [4, с. 26]) в межах 3,4–7,7 % [5], хибно позитивна помилка (помилкове визначення поліграфологом правдивої особи як неправдивої [4, с. 26]) сягає 6,4–13,8 % [5].

Скринінгові: точність у межах 85,8 – 87,5 % [5], невизначений результат в межах 9–17 % [5], хибно негативна помилка в межах 9,2–11,2 % [5], хибно позитивна помилка сягає 11,2–14,6 % [5].

Ми проаналізували застосування поліграфа в діяльності підрозділу протягом трьох років повномасштабного вторгнення російських окупаційних військ – з березня 2022 року по березень 2025 року. За цей період проведено 1487 поліграфологічних досліджень. Для порівняння: з моменту впровадження поліграфа в

підрозділі у 2017 році до 24 лютого 2022 року було здійснено менш ніж 300 досліджень. Таке зростання кількісних показників свідчить про зростання актуальності, практичної значущості та ефективності використання поліграфа в умовах дії правового режиму воєнного стану в Україні. У дослідженні висновки спеціаліста-поліграфолога ми поділили на три категорії, а саме:

1. Значущі реакції виявлено – фізіологічні реакції, що вказують на свідоме приховування інформації (обман) суб'єктом дослідження, тобто оманлива особа;

2. Значущі реакції не виявлено – не виявлено фізіологічних реакцій, які б вказували на свідоме приховування інформації (обман) суб'єктом дослідження, тобто правдива особа;

3. Невизначений результат – фізіологічні дані не містять достатньої або узгодженої діагностичної інформації, на основі якої можна було б прийняти остаточне рішення [4, с. 22]. Тобто спеціаліст-поліграфолог не може дійти висновку, оцінивши результати дослідження. До цієї категорії ми долучили результати ймовірної протидії суб'єктом дослідження процедурі тестування.

Результати нашого дослідження ми відобразили в таблиці 1.

Таблиця 1

Кількість та результати поліграфологічних тестувань у досліджуваному підрозділі

№ з/п	Висновок поліграфолога	Кількість досліджень	Відсоток
03.2022-03.2023			
1	Значущі реакції не виявлено	280	75,2%
2	Значущі реакції виявлено	75	20,1%
3	Невизначений результат	17	4,7%
4	Всього	372	100 %
03.2023-03.2024			
1	Значущі реакції не виявлено	300	73,5%
2	Значущі реакції виявлено	84	20,5%
3	Невизначений результат	24	6%
4	Всього	408	100 %
03.2024-03.2025			
1	Значущі реакції не виявлено	502	71%
2	Значущі реакції виявлено	156	22%
3	Невизначений результат	49	7%
4	Всього	707	100 %
03.2022-03.2025			
1	Значущі реакції не виявлено	1082	72,7%
2	Значущі реакції виявлено	315	21,2%
3	Невизначений результат	90	6,1%
4	Всього	1487	100 %

За результатами проведеного аналізу ми дійшли висновку, що з кожним роком повномасштабного вторгнення російських окупаційних військ кількість поліграфологічних перевірок лише збільшується. Так, за перший рік війни кількість поліграфологічних досліджень перевищила результати досліджень попередніх п'яти років. На третьому році війни кількість проведених досліджень майже в два рази збільшилась порівняно з першим роком. Із загальної кількості поліграфологічних досліджень за три роки аналізу отримано 315 випадків приховування інформації, що з вірогідністю від 85,8 до 92,1 % може вказувати на наявні ризики для відомства в питаннях кадрової, внутрішньої та власної безпеки. Саме ця категорія висновків може створювати значну небезпеку та має бути врахована і належним чином облікована.

В умовах цифровізації сектору безпеки і оборони України, а також запровадження поліграфа практично в усіх його сферах потреба у формуванні відомчих баз даних є актуальною. У нашому попередньому дослідженні щодо правового регулювання захисту персональних даних суб'єктів опитування із застосуванням поліграфа ми дійшли висновку, що:

– у більшості керівних документів складників сектору безпеки і оборони України відсутня норма, що регламентує порядок ведення та обробки персональних даних в електронному вигляді. Така норма міститься лише в «Порядку проведення психофізіологічного дослідження із застосуванням поліграфа в Управлінні державної охорони України»;

– ведення електронних баз поліграфологічних досліджень без нормативного врегулювання призводить до порушення права на захист персональних даних суб'єктів поліграфологічних досліджень;

ISSN 2311-8040

– відсутність регулюючих норм щодо баз даних поліграфологічних досліджень унеможливлює їх використання у законний спосіб, а в разі їх незаконного ведення вони підлягають знищенню [7, с. 80].

Формування відомчих баз даних поліграфологічних досліджень потребує комплексного нормативного врегулювання, яке має забезпечувати правомірність збору, зберігання, обробки та використання відповідної інформації з урахуванням вимог законодавства України у сфері захисту персональних даних, державної таємниці, оперативно-розшукової та контррозвідувальної діяльності і кримінального аналізу. Змістове наповнення такої бази даних доцільно структурувати за такими категоріями:

– ідентифікаційні відомості про ініціатора дослідження, поліграфолога та досліджувану особу (прізвище, ім'я, по батькові; звання; посада; тощо);

– тематика й тип дослідження (виявлення причетності до протиправної діяльності; державної зради; корупції тощо);

– застосовані методики тестування;

– поліграфологічні матеріали (аудіо – та відеозаписи; поліграми (графічне відображення психофізіологічних реакцій досліджуваної особи); інформована згода; установки; аналітичні довідки тощо);

– додатково отримана інформація під час дослідження;

– висновок поліграфолога;

– службові примітки (реалізація отриманої інформації; обґрунтування висновків; результати подальших перевірок) [8, с. 35].

На курсах підвищення кваліфікації поліграфологів у Національній академії внутрішніх справ у жовтні 2024 року керівник поліграфологічного підрозділу державного банку, виступаючи, зазначив, що в практиці банку, де поліграфологічні перевірки вже інтегровані у процедури службових розслідувань, одним із найбільших викликів стало забезпечення належного зберігання великих обсягів відеоданих, отриманих у ході досліджень [8, с. 36]. Тому у проєктуванні таких баз необхідно враховувати серверну інфраструктуру, розподілене зберігання, шифрування та доступ з урахуванням службових повноважень.

Значення електронної бази даних не обмежується лише забезпеченням кримінального аналізу. Вона також може використовуватись:

– кадровими службами під час прийняття управлінських рішень;

– для оцінювання ефективності діяльності поліграфологів (контроль якості);

– з науковими цілями (порівняльна ефективність методик, статистична валідизація, типологізація підходів тощо).

У міжнародній практиці (зокрема, у правоохоронних органах Великої Британії) результати поліграфологічних досліджень інтегруються до загальнодоступної для уповноважених суб'єктів інформаційної системи, що підвищує прозорість процедур та забезпечує стандартизацію якості [8, с. 36].

Важливо врегулювати строки зберігання інформації таких баз. На нашу думку, найбільш доцільно застосовувати такі строки:

– для осіб, щодо яких встановлено ознаки причетності до кримінального правопорушення, – зберігати дані відповідно до строків давності, визначених Кримінальним кодексом України;

– для осіб, стосовно яких не встановлено інформацію про причетність до кримінальних правопорушень, – передбачити автоматизовану процедуру деперсоналізації даних після трьох років. Саме більшість внутрішньовідомчих наказів складників сектору безпеки і оборони України визначають три роки для зберігання довідок за результатами поліграфологічних досліджень. Цю норму було запозичено із Закону США від 1988 року «Про захист працівників від поліграфа» (Employe e Polygraph Protection Act) [9].

Формування баз даних результатів поліграфологічних досліджень обов'язково має бути з дотриманням захисту персональних даних суб'єктів поліграфологічного дослідження, навіть у разі обмежень прав громадян в умовах правового режиму воєнного стану. Професор М. В. Корнієнко обґрунтовано зазначає, що воєнний стан доцільно розглядати як засіб відновлення умов, за яких людина може

ефективно реалізувати свої права та свободи [10, с. 30]. При цьому низка прав не може бути обмежена, а обмеження інших прав не може знищувати їхню сутність [10, с. 30]. На нашу думку, ця позиція є особливо релевантною у контексті формування баз даних поліграфологічних досліджень під час воєнного стану: навіть за умов посилених безпекових вимог держава зобов'язана забезпечити дотримання принципів законності, пропорційності та збереження сутнісного змісту права на приватність, зокрема, шляхом запровадження чітких гарантій захисту персональних даних.

Захист персональних даних під час формування та використання баз поліграфологічних досліджень у кримінальному аналізі регламентується міжнародним і національним правом. Базовими актами, ратифікованими Україною, є Конвенція про захист прав людини і основоположних свобод 1950 р. та Конвенція Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних [11]. Національне правове регулювання здійснюється відповідно до Закону України «Про захист персональних даних» [6], на виконання якого наглядовим органом у сфері захисту персональних даних є Уповноважений Верховної Ради України з прав людини. Наказом від 8 січня 2014 року № 1/02-14 було затверджено підзаконні акти у сфері захисту персональних даних:

– Типовий порядок обробки персональних даних;

– Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних;

– Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації [12].

У сфері захисту інформації значення мають також Закон України «Про доступ до публічної інформації» та Закон України «Про інформацію». Водночас наявна нормативна база потребує оновлення з урахуванням стандартів ЄС, зокрема положень Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, General Data Protection Regulation, далі – GDPR) [13], який встановлює єдині вимоги до обробки персональних даних у межах Європейського Союзу, та Директиви (ЄС) 2016/680 від 27 квітня 2016 року щодо обробки персональних даних правоохоронними органами [1]. Доцент К. Ю. Ісмайлов наголошує на необхідності оновлення українського законодавства про персональні дані з урахуванням вимог «Пакету про захист даних» ЄС, зокрема Регламенту (ЄС) 2016/679 (GDPR) та пов'язаних директив, з метою гармонізації з міжнародно-правовими стандартами й адаптації до сучасних викликів обробки інформації [14].

Правове регулювання формування та використання баз даних результатів поліграфологічних досліджень у кримінальному аналізі вимагає чіткого розмежування між загальними підходами до обробки персональних даних, які закріплені в GDPR, та спеціальними нормами, що містяться в Директиві (ЄС) 2016/680. GDPR регламентує обробку даних у межах Big Data-аналітики, яка застосовується для моніторингових, управлінських і профілактичних цілей, а Директива (ЄС) 2016/680 – обробку даних компетентними органами в межах правоохоронної діяльності, зокрема в системах DEMS, де така інформація набуває статусу доказової або оперативно вагомої. Відповідно до обох актів передбачено спільні фундаментальні принципи, а саме: законність, пропорційність, обмеження мети, мінімізація, точність, обмеження строків зберігання, безпека, псевдонімізація, а також гарантії захисту прав суб'єктів персональних даних.

Особливої уваги потребує регулювання обробки спеціальних категорій персональних даних – біометричних або тих, що стосуються здоров'я, які нерозривно пов'язані з результатами поліграфологічного дослідження.

Стаття 23 GDPR [13] передбачає допустимість встановлення державами обґрунтованих обмежень для обробки таких даних у разі необхідності забезпечення національної безпеки, громадського порядку чи запобігання кримінальним правопорушенням, що створює нормативну підставу для функціонування відомчих баз даних результатів поліграфологічних досліджень, у форматі Big Data.

Положення Директиви (ЄС) 2016/680 визначають концептуальну й техніко-юридичну основу інтеграції результатів поліграфологічних досліджень до DEMS шляхом встановлення конкретних вимог до категоризації суб'єктів (наприклад, підозрювані, обвинувачені, свідки), ведення журналів доступу, обмеження кола уповноважених осіб, призначення посадової особи з питань захисту даних, а також забезпечення шифрування і псевдонімізації даних. Таке диференційоване регулювання забезпечує баланс між суспільним інтересом та фундаментальними правами особи, а також підвищує доказову надійність та легітимність поліграфологічної інформації в кримінальному аналізі. Аналогічний підхід простежується й у правовій системі США, де з 1988 року діє Закон «Про захист працівників від поліграфа» (Employee Polygraph Protection Act, далі – EPPA) [9], який суворо обмежує розкриття результатів поліграфологічного дослідження: дозволяється їх повідомлення лише самому досліджуваному (або його представнику), ініціатору перевірки та за ухвалою суду. EPPA передбачає, що розкриття інформації державним органам можливе лише за наявності ознак протиправної поведінки особи, що надає підстави для подальшої правової кваліфікації. Така модель цільового, пропорційного та контрольованого доступу до поліграфологічних даних цілком корелює з обмежувальним режимом, передбаченим статтею 23 GDPR [13], і підтримує загальну логіку Директиви (ЄС) 2016/680 щодо правомірного обмеження прав на захист персональних даних в умовах кримінального провадження [1].

Отже, інтеграція результатів поліграфологічних досліджень до кримінального аналізу, зокрема цифрових систем DEMS, повинна здійснюватися з урахуванням як вимог Директиви (ЄС) 2016/680, так і узагальнених міжнародних стандартів на кшталт EPPA, що забезпечує не лише юридичну відповідність, але й етичну виправданість такої практики в умовах зростання значущості Big Data у сфері безпеки.

Висновки. Актуальність формування баз даних поліграфологічних досліджень в умовах воєнного стану зумовлена різким зростанням кількості досліджень у секторі безпеки і оборони України з початком повномасштабного вторгнення російських окупаційних військ. Поліграф довів свою ефективність у забезпеченні внутрішньої та власної безпеки та кадровій політиці правоохоронних органів України. Стратегічне нормативне підґрунтя створення таких баз забезпечує Указ Президента України № 273/2023 [3], який передбачає цифрову трансформацію органів правопорядку з модернізацією інформаційної інфраструктури та ризик-орієнтованим управлінням. Водночас правова невизначеність ведення баз даних результатів поліграфологічних досліджень, через відсутність чітких норм у відомчих актах створює ризики порушення законодавства про захист персональних даних і легітимність інформації.

Формування баз має відповідати Закону України «Про захист персональних даних», Конвенції № 108 Ради Європи, стандартам ЄС (GDPR, Директива 2016/680) та внутрішнім безпековим регламентам складників сектору безпеки і оборони України із застосуванням псевдонімізації, шифрування, обмеженого доступу, кіберзахисту, строкового зберігання та визначення відповідальних осіб.

У сучасних умовах цифровізації сектору безпеки і оборони України доцільно впроваджувати формування кількох типів баз даних поліграфологічних досліджень із дотриманням відповідних нормативно-правових стандартів, а саме:

1. Відомча база даних, у форматі Big Data. Функціонування цієї бази має ґрунтуватися на вимогах Регламенту (ЄС) 2016/679 (GDPR), який встановлює комплексні правила обробки персональних даних. У цій базі необхідно зберігати ідентифікаційні дані суб'єкта до-

слідження (ПІБ, звання, посаду тощо), ініціатора поліграфологічного дослідження, поліграфолога, а також сам факт проходження поліграфологічного дослідження без висновку поліграфолога. Особливістю такої бази має бути присвоєння унікального особистого номера суб'єкту дослідження, що забезпечує можливість подальшої деперсоналізації даних у спеціальній базі та захищає інформацію про особу під час подальшого використання. Такий підхід забезпечує баланс між прозорістю та захистом персональних даних, створюючи базу для аналітичної роботи без надмірного розголошення чутливої інформації.

2. База даних поліграфологічних досліджень підрозділу кримінального аналізу, у форматі DEMS. Формування і функціонування цієї бази регламентується Директивою (ЄС) 2016/680, яка визначає особливі вимоги до обробки персональних даних правоохоронними органами для забезпечення потреб кримінального аналізу. У межах цієї бази допускається використання лише унікального особистого номера суб'єкта поліграфологічного дослідження (присвоєного у відомчій базі) без розголошення його ідентифікаційних даних, що підвищує рівень захисту персональних даних. База має вміщувати деталі проведеного поліграфологічного дослідження: застосовані методики тестування, результати дослідження, аналітичні висновки, а також цифрові матеріали, зокрема поліграми (графіки психофізіологічних реакцій). Така структура забезпечує необхідний рівень конфіденційності, правомірності доступу та використання даних у межах кримінального аналізу й оперативно-розшукової діяльності.

3. Впровадження порядку обробки та зберігання відеозаписів і супутньої інформації. Особлива увага має бути приділена нормативному регулюванню процесів зберігання великих обсягів відео-, аудіоданих та інших матеріалів, що утворюються під час поліграфологічного дослідження. Розробка чіткого порядку зберігання повинна передбачати питання серверної інфраструктури, шифрування, кіберзахисту, розподіленого зберігання, а також контролю доступу відповідно до службових повноважень. Встановлення строків зберігання, умов архівування та процедури знищення інформації має ґрунтуватися на вимогах законодавства України про захист персональних даних, державну таємницю, а також відповідати принципам мінімізації зберігання даних. Забезпечення надійності та безпеки цих процесів є критичним складником комплексного захисту інформації та підтримки доказової сили даних у кримінальному аналізі.

Запропонований нами підхід дозволяє створити систему управління даними результатів поліграфологічних досліджень, що відповідає сучасним міжнародним стандартам, забезпечує права суб'єктів персональних даних та підвищує ефективність використання результатів поліграфологічних досліджень у секторі безпеки і оборони України. У межах концепції ILP така система може стати важливим компонентом тактичного й оперативного кримінального аналізу, забезпечуючи своєчасне виявлення загроз, формування профілів ризику, і прийняття рішень на основі доказової інформації. Інтеграція баз даних поліграфологічних досліджень до загальної аналітичної інфраструктури, відповідно до принципів ILP, сприятиме підвищенню ефективності ресурсного планування, забезпеченню внутрішньої та власної безпеки правоохоронних органів України.

Список використаних джерел:

1. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding processing of personal data by competent authorities. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680 (дата звернення: 23.06.2025).

2. Nelson et al. How To: A Step-by-Step Worksheet for the Multinomial ESS. *Polygraph & Forensic Credibility Assessment*. 2019. № 48 (1). P. 60–75.

3. 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://zakon.rada.gov.ua/laws/show/273/2023#Text (дата звернення: 23.06.2025).

4. Поліграфологія: основні терміни та поняття : словник / заг. ред. Л. Д. Удалова, С. С. Чернявський, Д. О. Алєксєєва-Процюк ; кол. авт. Київ : ТОВ «Альянт», 2022. 46 с.

5. Gordon N. et al. Meta-Analytic Survey of Criterion Accuracy of Validated Polygraph Techniques: Report Prepared For The American Polygraph Association. *Polygraph*. 2011. № 40(4). P. 193–305.

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 23.06.2025).

7. Здебський Д. В. Правове регулювання захисту персональних даних військовослужбовців, як суб'єктів опитування із застосування поліграфа. *Українська поліцеїстика: теорія, законодавство, практика.* 2024. № 1. С. 77–82. DOI: https://doi.org/10.32782/2709-9261-2024-1-9-15.

8. Здебський Д. В. Впровадження електронних баз даних поліграфологічних досліджень в кримінальному аналізі. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України :* матеріали науково-практичної конференції, 20 грудня 2024 р. Львів : ЛьвДУВС, 2025. С. 34–37.

9. Employee Polygraph Protection Act. URL: https://www.dol.gov/agencies/whd/polygraph (дата звернення: 23.06.2025).

10. Корнієнко М. В. Права людини в умовах воєнного стану: загальноправовий дискурс. *Південноукраїнський правничий часопис*. 2022. № 1–2. С. 27–31. DOI: https://doi.org/10.32850/sulj.2022.1-2.5.

11. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Страсбург, 28 січня 1981 р.) URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 23.06.2025).

12. Про затвердження документів у сфері захисту персональних даних : наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 23.06.2025).

13. Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.06.2025).

14. Ismailov K. To the issue of personal information circulation in the national police databases. *Fundamental and applied researches in practice of leading scientific schools*. 2020. № 38 (2). P. 41–45.

References:

1. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding processing of personal data by competent authorities. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680 [in English].

2. Nelson, R., et al. (2019). How To: A Step-by-Step Worksheet for the Multinomial ESS. *Polygraph & Forensic Credibility Assessment*. Vol. 48, vol. 1. Pp. 60–75 [in English].

3. President of Ukraine. (2023). Pro Kompleksnyi stratehichnyi plan reformuvannia orhaniv pravoporiadku yak chastyny sektoru bezpeky i oborony Ukrainy na 2023–2027 roky: Ukaz Prezydenta Ukrainy vid 11.05.2023 No. 273/2023 [On the Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defense Sector of Ukraine for 2023–2027: Presidential Decree No. 273/2023]. Retrieved from: https://zakon.rada.gov.ua/laws/show/273/2023#Text [in Ukrainian].

4. Udalova, L. D., Cherniavskyi, S. S., & Alekseeva-Protsiuk, D. O. (Eds.). (2022). *Polihrafolohiia: osnovni terminy ta poniattia: slovnyk [Polygraphology: basic terms and concepts: dictionary].* Kyiv: Al'iant. 46 p. [in Ukrainian].

5. Gordon, N., et al. (2011). Meta-Analytic Survey of Criterion Accuracy of Validated Polygraph Techniques: Report Prepared for the American Polygraph Association. *Polygraph.* Vol. 40, vol. 4. Pp. 193–305 [in English].

6. Verkhovna Rada of Ukraine. (2010). Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 No. 2297-VI [On personal data protection: Law of Ukraine No. 2297-VI dated June 1, 2010]. Vidomosti Verkhovnoi Rady Ukrainy. Vol. 34. Art. 481. Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

7. Zdebskyi, D. V. (2024). Pravove rehuliuvannia zakhystu personalnykh danykh viiskovosluzhbovtsiv, yak subiektiv opytuvannia iz zastosuvannia polihrafa [Legal regulation of personal data protection of servicemen as subjects of polygraph examinations]. *Ukrainska politseistyka: teoriia, zakonodavstvo, praktyka*. Vol. 1. Pp. 77–82. https://doi.org/10.32782/2709-9261-2024-1-9-15 [in Ukrainian].

8. Zdebskyi, D. V. (2025). Vprovadzhennia elektronnykh baz danykh polihrafolohichnykh doslidzhen v kryminalnomu analizi [Implementation of electronic databases of polygraph examinations in criminal analysis].

In: *Informatsiino-analitychne zabezpechennia diialnosti orhaniv sektoru bezpeky i oborony Ukrainy*: Proceedings of the Scientific-Practical Conference, December 20, 2024. Lviv: Lviv State University of Internal Affairs. Pp. 34–37 [in Ukrainian].

9. Employee Polygraph Protection Act. Retrieved from: https://www.dol.gov/agencies/whd/polygraph [in English].

10. Kornienko, M. V. (2022). Prava liudyny v umovakh voiennoho stanu: zahalnopravovyi dyskurs [Human rights under martial law: general legal discourse]. *Pivdennoukrainskyi pravnychyi chasopys.* Vol. 1–2. Pp. 27–31. https://doi.org/10.32850/sulj.2022.1-2.5 [in Ukrainian].

11. Konventsiya pro zakhyst osib u zv″yazku z avtomatyzovanoyu obrobkoyu personal′nykh danykh (Strasburh, 28 sichnya 1981 r.) [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, January 28, 1981)]. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_326#Text [in Ukrainian].

12. Ombudsman of Ukraine. (2014). Pro zatverdzhennia dokumentiv u sferi zakhystu personalnykh danykh: Nakaz vid 08.01.2014 No. 1/02-14 [On the approval of documents in the field of personal data protection: Order No. 1/02-14 dated January 8, 2014]. Retrieved from https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text [in Ukrainian].

13. Pro zakhyst fizychnykh osib u zv″yazku z obrobkoyu personal′nykh danykh i pro vil′nyy rukh takykh danykh, a takozh pro skasuvannya Dyrektyvy 95/46/YES (Zahal′nyy rehlament pro zakhyst danykh) : Rehlament (YES) 2016/679 Yevropeys′koho Parlamentu i Rady vid 27 kvitnya 2016 r. [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)]. Retrieved from https://zakon.rada.gov.ua/laws/show/984_008-16#Text [in Ukrainian].

14. Ismailov, K. (2020). To the issue of personal information circulation in the national police databases. Fundamental and applied researches in practice of leading scientific schools. Vol. 38, vol. 2. Pp. 41–45 [in English].

Дата надходження статті: 17.07.2025
Дата прийняття статті: 22.08.2025
Опубліковано: 27.10.2025