ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»

Кваліфікаційна наукова праця на правах рукопису

КІРІЄНКО ВІКТОР МИКОЛАЙОВИЧ

Прим. № ____

УДК 342.7:351.74:004.738

ДИСЕРТАЦІЯ
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

Спеціальність – 081 Право

Галузь знань – 08 Право

Подається на здобуття наукового ступеня доктора філософії. Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.М. Кірієнко

Науковий керівник – Корж Ігор Федорович доктор юридичних наук, старший науковий співробітник

Київ – 2026

АНОТАЦІЯ

Кірієнко В.М. Адміністративно-правове забезпечення захисту персональних даних у сфері охорони державного кордону України. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 Право – Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», м. Київ, 2026.

Дисертація є першим комплексним науковим дослідженням щодо адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України, у якому здійснено системний аналіз чинного законодавства, практики його застосування та міжнародних стандартів у сфері приватності. У дослідженні обґрунтовано концептуальні засади формування сучасної моделі захисту персональних даних із урахуванням процесів цифровізації, діджиталізації та гібрид загроз.

Наукова новизна одержаних результатів полягає, що внаслідок здійснення комплексного аналізу та наукового обґрунтування адміністративно-правових засад захисту персональних даних у сфері охорони державного кордону України, напрацьовано та удосконалено правові, організаційні і технічні механізми їх забезпечення, гармонізації національного законодавства з європейськими стандартами (GDPR, Конвенція 108), а також визначено роль та правовий статус Державної прикордонної служби України як ключового суб’єкта реалізації державної політики щодо захисту персональних даних при здійсненні пропуску через державний кордон осіб в умовах здійснюваної цифровізації, діджиталізації та протидії гібридним загрозам.

У дисертації уперше розроблено детальний шаблон оцінки впливу на захист даних (DPIA) адаптований для прикордонних інформаційних систем, який структуровано за ключовими розділами: опис операції обробки, правові підстави, пропорційність, карта потоків даних, оцінка ризиків, заходи зниження ризиків, залишковий ризик, доказова база. Це дозволяє системно оцінювати ризики для прав і свобод осіб, визначати технічні та організаційні заходи захисту

персональних даних, а також запроваджувати превентивні механізми управління ризиками у прикордонній сфері.

Автором напрацьовано пропозиції щодо внесення змін до Закону України «Про прикордонний контроль», які уможливлюють застосування наступних європейських принципів обробки персональних даних: законність, мінімізація, пропорційність, конфіденційність, підзвітність та які визначають обсяг даних, що можуть оброблятися, встановлюють правила інформування осіб про зазначене, регулюють використання автоматизованих і біометричних технологій, строки зберігання та процедури знищення/знеособлення даних, порядок доступу та передачі інформації, а також вводять обов'язкову оцінку впливу на захист даних перед запуском нових цифрових систем в Державній прикордонній службі України.

В роботі обґрунтовано доцільність та запропоновано запровадження інституту уповноваженої особи із захисту персональних даних у Державній прикордонній службі України, яка відповідатиме за дотримання законодавства, реагування на інциденти, що виникають на державному кордоні у процесі пропуску осіб та забезпечення прозорості обробки даних.

Дисертантом окреслено проблеми та напрацьовано пропозиції щодо необхідності запровадження комплексного підходу до гармонізації українського прикордонного законодавства з європейськими стандартами щодо захисту персональних даних, що включає в себе не лише загальні європейські принципи, а й конкретні процедурні та технічні механізми: журналювання доступу, аудит, людський контроль за автоматизованими рішеннями, обмеження транскордонної передачі даних.

Важливим є напрацювання пропозицій про розробку конкретних підзаконних актів, які мають регламентувати порядок інформування осіб у процесі їх пропуску через державний кордон, про застосування біометричних технологій, про проведення DPIA, щодо зберігання та передачі даних, а також приведення внутрішніх регламентів і інформаційних систем у відповідність із новими європейськими вимогами сьогодення.

Таким чином, окреслені авторські новації формують цілісну концепцію удосконалення адміністративно-правових механізмів захисту персональних даних у прикордонній сфері. Водночас, для забезпечення їхньої ефективності та практичної реалізації необхідним є врахування напрацьованих міжнародних стандартів і кращих практик у цій галузі.

Важливим елементом дослідження є аналіз міжнародного досвіду охорони персональних даних, а саме Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» та Загального Регламенту ЄС 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних» та можливості його адаптації до українського законодавства.

На основі здійсненого аналізу нинішнього стану системи захисту персональних даних та міжнародного досвіду у даній сфері, сформульовано напрями удосконалення правового регулювання охорони персональних даних у сфері захисту державного кордону України, включаючи гармонізацію із європейськими стандартами та впровадження принципів – «Приватність за задумом» (Privacy by Design) та «Приватність за замовчуванням» (Privacy by Default), а також розвиток інтегрованих інформаційних систем, таких як – «Цифрова біометрична система контролю в'їзду та виїзду на зовнішніх кордонах Європейського Союзу та Шенгенської зони» (EES) та «Державна електронна система онлайн-бронювання місця в черзі для перетину державного кордону України автомобілями (вантажівками, автобусами)» (єЧерга).

Визначено основні принципи адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України, якими є наступні з них: принципи верховенства права, законності, демократизму, дотримання прав і свобод, доцільності, раціональності. Досліджено теоретичні засади принципів адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України.

Обґрунтовано, що адміністративно-правовим забезпеченням захисту персональних даних у сфері охорони державного кордону України є система

нормативно-правових актів, організаційно-правових механізмів спрямованих на регулювання збору, обробки, зберігання, використання та захисту персональних даних під час здійснення прикордонного контролю, оперативно-службової діяльності та інформаційної взаємодії суб'єктів інтегрованого управління кордонами.

Практичне значення одержаних результатів полягає у тому, що вони становлять як науково-теоретичний, так і практичний інтерес і можуть бути використані у: *науково-дослідній сфері* – основні положення та висновки дисертації можуть бути основою для подальшого розвитку концепції та моделі реформи системи охорони державного кордону України що стосується захисту персональних даних у сфері прикордонної безпеки та за умов цифровізації та застосування штучного інтелекту; *сфері правотворчості та правозастосовної діяльності* – висновки, пропозиції та рекомендації, сформульовані у дисертації, можуть бути використані: у процесі наукової та правової експертизи відповідності існуючих нормативно-правових актів вимогам законодавству з питань охорони державного кордону, діяльності Державної прикордонної служби України, захисту персональних даних у процесі пропуску через державний кордон осіб, забезпечення національної безпеки; *навчальному процесі* – матеріали дисертації доцільно використовувати при підготовці підручників та посібників з дисциплін адміністративно-правового та інформаційно-правового циклів та викладанні навчальних дисциплін «Конституційне право», «Адміністративне право», «Інформаційне право», «Безпекове право» та ін.

Ключові слова: адміністративно-правове забезпечення, публічне адміністрування, інформаційне право, захист персональних даних, персональні дані, право на приватність, інформаційна безпека, національна безпека, воєнна безпека, охорона державного кордону України, прикордонний контроль, прикордонна безпека, Державна прикордонна служба України, цифровізація, інформаційні системи, інформаційні технології, штучний інтелект, правоохоронні органи, адміністративно-правовий режим, публічне управління.

SUMMARY

Kiriienko V.M. Administrative and legal protection of personal data in the sphere of protection of the state border of Ukraine. Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the specialty 081 Law - State scientific institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine", Kyiv, 2026.

The dissertation is the first comprehensive scientific study on the administrative and legal protection of personal data in the sphere of protection of the state border of Ukraine, in which a systematic analysis of the current legislation, the practice of its application and international standards in the field of privacy was carried out. The research substantiates the conceptual foundations of the formation of a modern model of personal data protection, taking into account the processes of digitization, digitization and hybrid threats.

The scientific novelty of the obtained results is that as a result of the comprehensive analysis and scientific substantiation of the administrative and legal basis for the protection of personal data in the field of protection of the state border of Ukraine, legal, organizational and technical mechanisms for their provision, harmonization of national legislation with European standards (GDPR, Convention 108) have been developed and improved, and the role and legal status of the State Border Guard Service of Ukraine as a key subject of the implementation of the state policy on the protection of personal data in the event of a crossing has been determined. across the state border of individuals in the conditions of digitization, digitization and countering hybrid threats.

The dissertation first developed a detailed data protection impact assessment template (DPIA) adapted for border information systems, which is structured according to key sections: description of the processing operation, legal basis, proportionality, data flow map, risk assessment, risk reduction measures, residual risk, evidence base. This makes it possible to systematically assess risks for the rights and freedoms of individuals, to determine technical and organizational measures for the protection of

personal data, as well as to introduce preventive risk management mechanisms in the border area.

The author has developed proposals for amendments to the Law of Ukraine "On Border Control", which enable the application of the following European principles of personal data processing: legality, minimization, proportionality, confidentiality, accountability and which determine the amount of data that can be processed, establish rules for informing individuals about the above, regulate the use of automated and biometric technologies, storage periods and procedures for destruction/depersonalization of data, the procedure for accessing and transferring information, and also introduce mandatory data protection impact assessment before launching new digital systems in the State Border Service of Ukraine.

The paper substantiates the expediency and proposes the introduction of the institute of the authorized person for the protection of personal data in the State Border Service of Ukraine, who will be responsible for compliance with the legislation, responding to incidents that occur at the state border in the process of passing persons and ensuring transparency of data processing.

The dissertation outlined the problems and developed proposals regarding the need to introduce a comprehensive approach to the harmonization of Ukrainian border legislation with European standards for the protection of personal data, which includes not only general European principles, but also specific procedural and technical mechanisms: access logging, auditing, human control over automated decisions, restrictions on cross-border data transfer.

It is important to develop proposals for the development of specific by-laws that should regulate the procedure for informing persons in the process of their passage across the state border, about the use of biometric technologies, about conducting DPIA, about data storage and transmission, as well as bringing internal regulations and information systems into compliance with the new European requirements of today.

Thus, the outlined author's innovations form a holistic concept of improving the administrative and legal mechanisms for the protection of personal data in the border area. At the same time, to ensure their effectiveness and practical implementation, it is

necessary to take into account the developed international standards and best practices in this field.

An important element of the research is the analysis of the international experience of personal data protection, namely the Convention of the Council of Europe No. 108 "On the Protection of Individuals in Connection with Automated Processing of Personal Data" and the General EU Regulation 2016/679 "On the Protection of Individuals in Connection with the Processing of Personal Data and on the Free Movement of Such Data" and the possibility of its adaptation to Ukrainian legislation.

Based on the analysis of the current state of the personal data protection system and international experience in this field, directions for improving the legal regulation of personal data protection in the field of protection of the state border of Ukraine, including harmonization with European standards, and the implementation of the principles - "Privacy by Design" (Privacy by Design) and "Privacy by Default" (Privacy by Default), as well as the development of integrated information systems, such as - "Digital biometric system of entry control and exit at the external borders of the European Union and the Schengen zone" (EES) and "State electronic system of online reservation of a place in the queue for crossing the state border of Ukraine by cars (trucks, buses)" (eCherga).

The main principles of administrative and legal protection of personal data in the sphere of protection of the state border of Ukraine are defined, which are the following: the principles of rule of law, legality, democracy, observance of rights and freedoms, expediency, rationality. The theoretical foundations of the principles of administrative and legal protection of personal data in the sphere of protection of the state border of Ukraine have been studied.

It is substantiated that the administrative-legal provision of personal data protection in the field of protection of the state border of Ukraine is a system of normative-legal acts, organizational-legal mechanisms aimed at regulating the collection, processing, storage, use and protection of personal data during border

control, operational-service activities and information interaction of subjects of integrated border management.

The practical significance of the obtained results lies in the fact that they are of both scientific-theoretical and practical interest and can be used in: the research field - the main provisions and conclusions of the dissertation can be the basis for the further development of the concept and model of the reform of the state border protection system of Ukraine regarding the protection of personal data in the field of border security and under the conditions of digitization and the use of artificial intelligence; in the field of law-making and law-enforcement activities - the conclusions, proposals and recommendations formulated in the dissertation can be used: in the process of scientific and legal examination of the compliance of existing normative legal acts with the requirements of the legislation on the protection of the state border, the activities of the State Border Guard Service of Ukraine, the protection of personal data in the process of passing people across the state border, ensuring national security; the educational process - it is advisable to use the dissertation materials in the preparation of textbooks and manuals for the disciplines of administrative-legal and informational-legal cycles and the teaching of the educational disciplines "Constitutional Law", "Administrative Law"; "Information Law", "Security Law", etc.

Keywords: administrative and legal support, public administration, information law, personal data protection, personal data, right to privacy, information security, national security, military security, protection of the State Border of Ukraine, border control, border security, the State Border Guard Service of Ukraine, digitalization, information systems, information technologies, artificial intelligence, law enforcement agencies, administrative and legal regime, public governance.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Корж І. Ф., Кірієнко В. М. Політико-правова аберація: нігілізм та зброя. *Інформація і право*. 2023. № 1 (44). С. 9–24. URL: https://doi.org/10.37750/2616-6798.2023.1(44)

2. Корж І. Ф., Кірієнко В. М. Дискреція обмеження прав і свобод людини в Україні. *Сучасні аспекти науки*. 2023. С. 77–98. URL: http://perspectives.pp.ua/public/site/mono/mono-31.pdf

3. Кірієнко В. М. Основи прикордонної безпеки України. Organizational and legal fundamentals for the formation of a security environment in Ukraine: Scientific monograph. Riga, Latvia: Baltija Publishing, 2023. 342 p. С. 64–74. http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/386 https://doi.org/10.30525/978-9934-26-363-7-4

4. Кірієнко В. М. Захист персональних даних як аспекту, національної безпеки, в умовах збройного конфлікту. *Юридичний науковий електронний журнал.* 2024. № 1. С. 398–400. URL: https://doi.org/10.32782/2524-0374/2024-1/90

5. Кірієнко В. М. Загрози прикордонній безпеці в умовах збройного конфлікту. *Юридичний науковий електронний журнал*. 2024. № 2. С. 272–274. URL: https://doi.org/10.32782/2524-0374/2024-2/65

які засвідчують апробацію матеріалів дисертації:

1. Корж І. Ф., Кірієнко В. М., Корж Т. І. Дискреція обмеження прав і свобод людини. *Актуальні питання сучасної юриспруденції :* матеріали міжнародної наукової конференції (м. Ченстохова, Республіка Польща, 05–06 квітня 2023 року). Рига : *Baltija Publishing*, 2023. С. 14–18.

2. Кірієнко В. М. Захист персональних даних в умовах воєнного стану. *Актуальні питання юридичної науки :* матеріали всеукраїнської науково-практичної конференції (м. Київ, 18 травня 2023 року). Одеса : Видавництво “Юридика”, 2023. С. 302–305.

3. Кірієнко В. М. Інформаційна безпека в умовах війни. *Проблеми інформаційно-правового забезпечення децентралізації державної влади та цифрової трансформації в Україні :* матеріали науково-практичної конференції (м. Вінниця, 15 червня 2023 року). Вінниця, 2023. Т.1. С. 88–91.

4. Кірієнко В. М. Охорона державного кордону – як складова сектору безпеки і оборони. *Науковий прогрес: інновації, досягнення та перспективи :* матеріали науково-практичної конференції (м. Мюнхен, Німеччина, 23–25 липня 2023 року). Німеччина : *MDCP Publishing,* 2023. С. 201–205.

5. Кірієнко В. М. Адміністративна відповідальність за порушення зберігання персональних даних. *Європейський науковий конгрес :* матеріали міжнародної науково-практичної конференції (м. Мадрид, Іспанія, 07–09 серпня 2023 року). Іспанія : *Barca Academy Publishing,* 2023. С. 170–175.

6. Кірієнко В. М. Захищеність персональних даних військовослужбовців Державної прикордонної служби України. *Європейський науковий конгрес :* матеріали міжнародної науково-практичної конференції (м. Мадрид, Іспанія, 04–09 вересня 2023 року). Іспанія : *Barca Academy Publishing,* 2023. С. 239–241.

7. Кірієнко В. М. Протидія інформаційній агресії та інформаційній пропаганді. *Нормативно-правова інформація і парламентський контроль :* матеріали науково-практичної конференції (м. Київ, 21 вересня 2023 року) / наук. керівник конф.: Д. В. Ланде; упоряд.: В. М. Фурашев, А. І. Нижник, С. О. Дорогих. Київ, 2023. С. 88–90.

8. Кірієнко В. М. Виклики та загрози прикордонній безпеці від впровадження в сучасне життя цифрових технологій. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання :* матеріали всеукраїнської науково-практичної конференції (м. Київ, 23 листопада 2023 року) / наук. керівник конф. О. А. Баранов; упоряд.: М. В. Дубняк, С. О. Дорогих. Київ, 2023. С. 108–111.

9. Кірієнко В. М. Протидія терористичним загрозам на державному кордоні України. *Актуальні проблеми протидії злочинності і корупції :*

матеріали всеукраїнської науково-практичної конференції (м. Харків, 22 грудня 2023 року). Харків : *Юрайт*, 2023. С. 70–72.

10. Кірієнко В. М. Правові аспекти регулювання прикордонної безпеки. *Теоретичні та практичні проблеми реалізації норм права :* матеріали міжнародно науково-практичної конференції (м. Львів, 22–23 грудня 2023 року). Львів – Торунь : *Liha-Pres,* 2023. С. 200–203.

11. Кірієнко В. М. Захист персональних даних як аспект українсько-європейської співпраці у сфері прикордонної безпеки. *Сучасні виклики науки та освіти :* матеріали міжнародної науково-практичної конференції (м. Берлін, Німеччина, 15–17 січня 2024 року). Німеччина : *MDCP Publishing,* 2024. С. 593–596.

12. Кірієнко В. М. Захист персональних даних військовослужбовців Державної прикордонної служби України*. Сучасні виклики науки та освіти : матеріали міжнародної науково-практичної конференції* (м. Берлін, Німеччина, 12–14 лютого 2024 року). Німеччина *: MDCP Publishing,* 2024. С. 492–496.

13. Кірієнко В. М. Вплив корупції на ефективність діяльності правоохоронних органів в умовах воєнного стану. *Актуальні проблеми протидії корупції в умовах воєнного стану :* матеріали міжнародної науково-практичної конференції (м. Львів, 15 лютого 2024 року). Львів – Торунь : *Liha-Pres,* 2024. С. 65–68.

14. Кірієнко В. М. Методологічні засади удосконалення службової діяльності Державної прикордонної служби України в умовах цифровізації. *Реформування правоохоронних органів в Україні : актуальні питання та перспективи :* матеріали міжнародної науково-практичної конференції (м. Львів, 05 лютого 2026 року). Львів – Торунь : *Liha-Pres,* 2026. С. 81–84.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АДПСУ – Адміністрація Державної прикордонної служби України

ВПС – відділ прикордонної служби

ВРУ – Верховна Рада України

ДБР – Державне бюро розслідувань

Дія – державний мобільний застосунок

ДКНПУ – Департамент кіберполіції Національної поліції України

ДПСУ – Державна прикордонна служба України

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації

ЄС – Європейський Союз

єЧерга – електронна черга перетину кордону

ЗСУ – Збройні сили України

ІІКС – інтегрована інформаційно-комунікаційна система

ІКС – інформаційно-комунікаційна система

ІС – інформаційні системи

ІТ – інформаційні технології

КМУ – Кабінет Міністрів України

КСУ – Конституційний Суд України

КУпАП – Кодекс України про адміністративні правопорушення

МВС – Міністерство внутрішніх справ України

МЗС – Міністерство закордонних справ України

Мінцифри – Міністерство цифрової трансформації України

МОУ – Міністерство Оборони України

Омбудсмен – Уповноважений Верховної Ради з прав людини

ОСД – оперативно-службова діяльність

ПТК – програмно-технічний комплекс

РФ – Російська Федерація

СБУ – Служба безпеки України

СЕД – система електронного документообігу

СІПС – спеціалізована інтегрована інформаційно-пошукова система

УВВБ – Управління внутрішньої та власної безпеки

ШІ – штучний інтелект

AI Act – Закон ЄС про штучний інтелект

CERT-UA – Національна команда реагування на кіберінциденти, кібератаки та кіберзагрози

DPIA – оцінка впливу на приватність

DPO – уповноважена особа із захисту даних

EES – цифрова біометрична система контролю в'їзду та виїзду на зовнішніх кордонах ЄС та Шенгенської зони

E-mail – електронна пошта

EU-LISA – Європейське агентство з оперативного управління ІТ-системами

GDPR – Регламент Європейського Парламенту і Ради

VIS – візова інформаційна система

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. У сучасних умовах інтенсивної цифровізації суспільства, активного впровадження технологій штучного інтелекту та процесів європейської інтеграції України, особливо з огляду на актуальні виклики національній безпеці, спричинені широкомасштабною агресією Російської Федерації, розвиток нашої держави неможливий без ефективного адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України.

В наш час проблема захисту персональних даних полягає не стільки у відсутності нормативно-правових актів, скільки у їх застарілості, фрагментарності та складності застосування, адже базовий нормативно-правовий акт, а саме Закон України «Про захист персональних даних», який був прийнятий у 2010 році, не враховує сучасні технології – «Big Data» (Великі дані), «AI» (Штучний інтелект) та хмарні сервіси, характеризується нечіткістю норм, фрагментарністю регулювання та слабким механізмами контролю і санкцій, а відсутність незалежного органу нагляду свідчить про його невідповідність сучасним цифровим викликам, а також вказує на актуальність та необхідність наукового дослідження даного предмету.

Європейський стандарт захисту персональних даних визначається Регламентом Європейського Парламенту і Ради «Про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних» – «GDPR», однак його імплементація в українське законодавство є неповною та супроводжується відсутністю належної консолідації між нормами ЄС і національним правом. Це, в свою чергу, зумовлює складність досягнення відповідності для бізнесу, проблеми практичного застосування – оцінка ризиків, оцінка впливу на захист даних (DPIA), контроль процесорів даних.

Додаткові колізії також виникають і у взаємодії Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації», а це створює конфлікт між правом на приватність і правом на доступ до інформації, а також відбуваються різні тлумачення правових норм. В умовах правового

режиму воєнного стану спостерігається розширення доступу держави до персональних даних, а це знижує рівень гарантій приватності та загострює конфлікт між безпекою інформаційних положень і правами особи на доступ до інформації.

Використання нових цифрових інструментів державних сервісів породжує ризики цифрової дискримінації, непрозорості обробки даних та недостатнього контролю за винятками для правоохоронних органів. Загальні проблеми законодавства мають нормативний характер – відсутність єдиного кодифікованого акту, прогалини у сфері AI та транскордонної передачі даних; інституційний характер – слабкий нагляд, низька ефективність відповідальності; практичний характер – низька обізнаність громадян, складність реалізації прав, формальний характер політик конфіденційності.

Поряд із загальними проблемами законодавчого, інституційного та практичного характеру, у сфері охорони державного кордону України виокремлюються й спеціальні проблеми адміністративно-правового забезпечення захисту персональних даних. Вони зумовлені специфікою прикордонної діяльності та функціонування інформаційних систем Державної прикордонної служби України й полягають у відсутності спеціалізованого нормативного регулювання прикордонних реєстрів, невизначеності механізмів транскордонного обміну даними, відсутності обов’язкових процедур оцінки впливу на приватність при впровадженні нових IT-рішень, слабкому інституційному контролі за прикордонними базами даних, низькому рівні цифрової грамотності персоналу та підвищеній вразливості прикордонних інформаційних систем до кіберзагроз.

Сьогодні проблема виникає не в кількості нормативно-правових актів, а в тому, що українська система захисту персональних даних не синхронізована з європейською «GDPR» та не адаптована до цифрової економіки, адже містить колізії між різними законами та має слабкі механізми контролю і відповідальності, що зумовлює необхідність вирішення наукового завдання

щодо удосконалення правового забезпечення охорони персональних даних у сфері захисту державного кордону України.

Дослідження адміністративно-правового регулювання захисту персональних даних у сфері охорони державного кордону України здійснено шляхом комплексного аналізу чинних нормативно-правових актів та міжнародних стандартів у сфері захисту персональних даних. Головним чинником у цьому контексті є висновок про необхідність гармонізації національного законодавства з правовими актами Європейського Союзу, зокрема із Загальним регламентом про захист даних – GDPR, який закріплює фундаментальні принципи обробки та збереження інформації.

Особливу увагу приділено специфіці діяльності Державної прикордонної служби України, підрозділи якої здійснюють контроль за переміщенням осіб і вантажів через державний кордон. Зазначена діяльність передбачає використання сучасних інформаційних систем, таких як «EES» (Система в'їзду та виїзду) та «єЧерга» (Електронна черга перетину кордону), а також функціонування баз даних і впровадження технологій штучного інтелекту, що зумовлює необхідність належного адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України.

Проблематика дослідження персональних даних та діяльності Державної прикордонної служби України не є новою для науки. Зокрема, різні аспекти персональних даних досліджували такі вчені як: Баранов О. А., Брижко В. М., Виноградова Г. М., Гусаров С. М., Дзьобань О. П., Доронін І. М., Заярний О. А., Касперський І. П., Корж І. Ф., Ланде Д. В., Мельник С. М., Пилипчук В. Г., Радзієвська О. Г., Різак М. В., Саєнко М. І., Самойленко Ю. С., Ткачук Т. Ю., Тунік А. В., Фурашев В. М., Цвірюк Д. В., Чанишев Р. І., Чернобай А. М. та ін.

У наукових дослідженнях, присвячених діяльності Державної прикордонної служби України, зокрема прикордонній безпеці, вагомий внесок зробили: Басараб О. Т., Корж І. Ф., Ксензюк А. Я., Курилюк Ю. Б., Литвин М. М., Мельников О. Г., Назаренко В. О., Нікіфоренко В. С., Олексієнко Б. М.,

Сердюк С. І., Цевєльов О. Є., а інформаційній складовій прикордонної безпеки – Кушнір І. П. та ін.

Водночас, попри значну увагу науковців, системне дослідження адміністративно-правового забезпечення захисту персональних даних, зокрема у сфері охорони державного кордону України на монографічному рівні не здійснювалося, що зумовлює доцільність проведення такого дослідження, визначає його актуальність та необхідність вирішення наукового завдання щодо правового забезпечення збереження персональних даних осіб, які перетинають державний кордон.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконана відповідно до науково-дослідної роботи «Правові засади протидії інформаційній агресії та розвитку системи забезпечення інформаційної безпеки України», зареєстрованої в УкрІНТЕІ РК № 0123U100415 від 21.01.2023 р., підставами для виконання якої є: рішення Вченої ради ДНУ ІІБП НАПрН України – протокол № 3 від 22.03.2022 р.; Тематичний план, затверджений Постановою Бюро Президії Національної академії правових наук України № 206/1-Б від 26.08.2022 р., експертний висновок Експертної ради НАН України від 01.12.2022 р. № 121/56, Стратегія розвитку Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» на 2021-2025 роки, затверджена постановою Бюро Президії НАПрН України від 12 серпня 2021 р. № 192/2-Б.

У дисертації узагальнено теоретико-методологічні засади та обґрунтовано необхідність удосконалення адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України, що передбачає гармонізацію національного законодавства з європейськими стандартами в умовах цифровізації суспільства та усунення спеціальних проблем прикордонної сфери, пов'язаних із нормативною неврегульованістю інформаційних систем, транскордонним обміном даними, слабким інституційним контролем і підвищеною вразливістю баз даних до кіберзагроз.

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає у комплексному аналізі та науковому обґрунтуванні адміністративно-правових засад захисту персональних даних у сфері охорони державного кордону України, розробці та удосконаленні правових, організаційних і технічних механізмів їх забезпечення, гармонізації національного законодавства з європейськими стандартами (GDPR, Конвенція 108), а також визначенні ролі та правового статусу Державної прикордонної служби України як ключового суб'єкта реалізації державної політики у сфері прикордонної безпеки в умовах цифровізації, діджиталізації та гібридних загроз.

Досягнення поставленої мети передбачає розв'язання таких *завдань:*

- здійснити комплексний аналіз сучасного стану адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України з виявленням прогалин у законодавстві, суперечностей між нормами та практикою їх застосування, а також оцінкою ефективності існуючих механізмів контролю;

- уточнити понятійно-категорійний апарат шляхом розмежування понять «охорона» (превентивний, статистичний характер) та «захист» (відновлювальний, активний характер) персональних даних, що дозволить сформувати цілісну систему термінів для законодавчого використання;

- визначити правовий статус Державної прикордонної служби України як ключового суб'єкта забезпечення прикордонної безпеки, поєднуючи її функції військового формування та правоохоронного органу спеціального призначення, що забезпечує обробку та захист захисту персональних даних;

- дослідити особливості обробки та захисту персональних даних у прикордонній сфері з акцентом на надмірність збору, нечіткість строків зберігання, широке коло доступу та недостатню прозорість для громадян;

- обґрунтувати напрями гармонізації національного законодавства з європейськими стандартами (GDPR, Конвенція 108), включно з принципами законності, пропорційності, мінімізації та конфіденційності;

- проаналізувати вплив цифровізації та гібридних загроз на адміністративно-правові механізми захисту персональних даних, визначивши нові ризики та потребу у створенні комплексних гарантій приватності;

- оцінити функціонування інтегрованих інформаційних систем «ГАРТ» та «Аркан» з точки зору їхньої інформаційної безпеки та розробити пропозиції щодо впровадження персоніфікованої ідентифікації, журналювання доступу та регулярного аудиту;

- визначити адміністративно-правові механізми запобігання порушенням у сфері захисту персональних даних в умовах гібридного конфлікту та кібератак, зокрема превентивні заходи та інституційні гарантії стабільності прикордонних систем;

- узагальнити міжнародний досвід у сфері захисту персональних даних та адаптувати його до національного законодавства, враховуючи потребу у незалежних органах нагляду та співпраці держави, приватного сектору та громадянського суспільства;

- розробити комплекс практичних пропозицій щодо удосконалення правового регулювання, організаційних та технічних механізмів захисту персональних даних, включно із впровадженням DPIA, інституту DPO, чітких строків зберігання та посилення парламентського та громадського контролю.

Об'єктом дослідження є суспільні відносини пов'язані зі збиранням, обробкою, використанням та захистом персональних даних у сфері охорони державного кордону України.

Предметом дослідження є адміністративно-правове забезпечення захисту персональних даних у сфері охорони державного кордону України.

Методи дослідження. Використання у процесі дослідження наукових підходів: аксіологічного, діяльнісного, міждисциплінарного, праксеологічного та системного надало можливість здійснити комплексну характеристику адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України.

Методологічну основу наукової роботи складають такі методи: діалектичний, методи аналізу і синтезу, описовий метод, порівняльний метод, формально-логічний метод.

Діалектичний метод дозволив дослідити правове забезпечення охорони персональних даних у його розвитку, взаємозв'язку та взаємозумовленості із суспільними процесами, зокрема в умовах трансформації безпекового середовища та цифровізації (підрозділи 2.1., 3.1).

Методи аналізу і синтезу використано для виокремлення структурних елементів механізму правового забезпечення захисту персональних даних та їх подальшого узагальнення у цілісну концептуальну модель.

Описовий метод сприяв систематизації наукових підходів, нормативно-правових актів і практики застосування у сфері захисту державного кордону України.

Порівняльний метод застосовано з метою зіставлення національного законодавства із міжнародними та європейськими стандартами у сфері захисту персональних даних, що дало змогу окреслити напрями його вдосконалення.

Формально-логічний метод забезпечив уточнення понятійно-категорійного апарату дослідження, формулювання наукових висновків і пропозицій.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим комплексним науковим дослідженням адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України, і яка вирішує проблемне наукове завдання щодо удосконалення нормативно-правового забезпечення приватності відповідно до європейських стандартів у процесі переміщенням осіб і вантажів через державний кордон.

У процесі здійснення дослідження одержано низку нових наукових результатів, які мають важливе теоретичне і практичне значення, зокрема:

уперше:

- розроблено детальний шаблон оцінки впливу на захист даних (DPIA) адаптований для прикордонних інформаційних систем, який структуровано за

ключовими розділами: опис операції обробки, правові підстави, пропорційність, карта потоків даних, оцінка ризиків, заходи зниження ризиків, залишковий ризик, доказова база. Це дозволяє системно оцінювати ризики для прав і свобод осіб, визначати технічні та організаційні заходи захисту персональних даних, а також запроваджувати превентивні механізми управління ризиками у прикордонній сфері;

- напрацьовано пропозиції щодо внесення змін до Закону України «Про прикордонний контроль», які уможливлюють застосування наступних європейських принципів обробки персональних даних: законність, мінімізація, пропорційність, конфіденційність, підзвітність та які визначають обсяг даних, що можуть оброблятися, встановлюють правила інформування осіб про зазначене, регулюють використання автоматизованих і біометричних технологій, строки зберігання та процедури знищення/знеособлення даних, порядок доступу та передачі інформації, а також вводять обов'язкову оцінку впливу на захист даних перед запуском нових цифрових систем в Державній прикордонній службі України;

- обґрунтовано доцільність та запропоновано запровадження інституту уповноваженої особи із захисту персональних даних у Державній прикордонній службі України, яка відповідатиме за дотримання законодавства, реагування на інциденти, що виникають на державному кордоні у процесі пропуску осіб, та забезпечення прозорості обробки даних;

- окреслено проблеми та напрацьовано пропозиції щодо необхідності запровадження комплексного підходу до гармонізації українського прикордонного законодавства з європейськими стандартами щодо захисту персональних даних, що включає в себе не лише загальні європейські принципи, а й конкретні процедурні та технічні механізми: журналювання доступу, аудит, людський контроль за автоматизованими рішеннями, обмеження транскордонної передачі даних;

- напрацьовано пропозиції для Кабінету Міністрів України та Державної прикордонної служби України про напрацювання конкретних підзаконних актів,

які мають регламентувати порядок інформування осіб у процесі їх пропуску через державний кордон, про застосування біометричних технологій, про проведення DPIA, щодо зберігання та передачі даних, а також приведення внутрішніх регламентів і інформаційних систем у відповідність із новими європейськими вимогами сьогодення.

удосконалено:

- положення Закону України «Про прикордонний контроль», в яких пропонується закріпити європейські принципи обробки персональних даних: законність, мінімізація, пропорційність, конфіденційність, підзвітність, а також якими визначаються строки зберігання та процедури знищення/знеособлення даних, встановлюють правила доступу й передачі інформації, а також запроваджують обов'язкову оцінку впливу на захист даних перед запуском нових цифрових систем;

- положення внутрішніх актів Служби в частині функціонування спеціальних актів та інструкцій Державної прикордонної служби України, які регламентують порядок інформування осіб на державному кордоні, застосування біометричних технологій при здійсненні пропуску через державний кордон осіб, проведення DPIA, зберігання та передачі даних, що забезпечує єдину практику в Службі та усуває прогалини в чинних актах законодавства;

- існуючі механізми забезпечення інформаційної безпеки прикордонних систем «ГАРТ» та «Аркан» шляхом запровадження персоніфікованої авторизації, журналювання доступу, регулярного аудиту та інтеграції з іншими державними реєстрами, а також проведення DPIA як превентивного інструменту управління ризиками.

набули подальшого розвитку:

- підходи та бачення щодо напрямів та механізмів посилення парламентського й громадянського контролю за діяльністю Державної прикордонної служби України; в частині належного забезпечення захисту

персональних даних осіб, щодо яких здійснюються заходи збору інформації в інтересах охорони державного кордону;

- організаційно-процедурні основи щодо напрямів та механізмів удосконалення цифрової грамотності персоналу Державної прикордонної служби України як комплексу базових знань шляхом: проведення регулярних тренінгів з кібербезпеки; формування у нього сучасної культури захисту персональних даних; навчання прикордонників протидії фішингу, соціальній інженерії та правилам поводження з носіями інформації; застосування штучного інтелекту; проведення незалежних кібераудитів та стрес-тестів систем бази даних кордону (наприклад, Державною службою спецзв'язку або міжнародними експертами); здійснення менеджменту інцидентів, тобто створення чітких протоколів швидкого реагування на випадок кібератак або компрометації даних пасажирів;

- напрацювання щодо доцільності удосконалення здійснення контролю за правоохоронним запитом: встановлення та запровадження жорстких судових або адміністративних фільтрів для передачі прикордонних даних іншим відомствам;

- напрями, механізми та засоби удосконалення механізму здійснення прикордонного контролю, які мають базуватися на впроваджених стандартах GDPR, тобто на адаптованих до українських умов процедурах здійснення прикордонного контролю відповідно до вимог Регламенту ЄС про захист даних;

Практичне значення одержаних результатів. Сформульовані в дисертації висновки та пропозиції можуть бути використані:

- *у науково-дослідній діяльності* – для подальших науково-теоретичних досліджень адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України;

- *у правотворчій діяльності* – з метою удосконалення адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України;

- *у правозастосовній сфері* – як напрацьований базис;

- *у навчальному процесі* – під час підготовки підручників і навчальних посібників, методичних матеріалів, проведенні занять з дисциплін «Інформаційне право», «Охорона та захист державного кордону України», «Прикордонна безпека», а також при викладанні правових та суміжних дисциплін.

Особистий внесок дисертанта. Дисертація є самостійно виконаним, завершеним науковим дослідженням. Сформульовані в роботі положення та наукові висновки є результатом особистого дослідження та обґрунтуванням автора на основі аналізу наукових джерел та нормативно-правових актів.

Апробація матеріалів дисертації. Основні положення та результати дисертаційної роботи було оприлюднено на науково-практичних конференціях: «Актуальні питання сучасної юриспруденції» (м. Ченстохова, 05–06 квітня 2023 р.); «Актуальні питання юридичної науки» (м. Одеса, 18 травня 2023 р.); «Проблеми інформаційно-правового забезпечення децентралізації державної влади та цифрової трансформації в Україні» (м. Вінниця, 15 червня 2023 р.); «Науковий прогрес: інновації, досягнення та перспективи» (м. Мюнхен, 23–25 липня 2023 р.); «Європейський науковий конгрес» (м. Мадрид, 07–09 серпня 2023 р.); «Європейський науковий конгрес» (м. Мадрид, 04–09 вересня 2023 р.); «Нормативно-правова інформація і парламентський контроль» (м. Київ, 21 вересня 2023 р.); «Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання» (м. Київ, 23 листопада 2023 р.); «Актуальні проблеми протидії злочинності і корупції» (м. Харків, 22 грудня 2023 р.); «Теоретичні та практичні проблеми реалізації норм права» (м. Львів, 22–23 грудня 2023 р.); «Сучасні виклики науки та освіти» (м. Берлін, 15–17 січня 2024 р.); «Сучасні виклики науки та освіти» (м. Берлін, 12–14 лютого 2024 р.); «Актуальні проблеми протидії корупції в умовах воєнного стану» (м. Львів, 15 лютого 2024 р.); «Реформування правоохоронних органів в Україні» (м. Львів, 05 лютого 2026 р.).

Публікації. Основні наукові результати дисертації опубліковано в дев’ятнадцяти наукових працях, серед яких: п’ять статей, із них дві у

співавторстві, у наукових фахових виданнях України та за кордоном, чотирнадцять тез, із них одна у співавторстві, що опубліковані у збірниках матеріалів науково-практичних конференцій.

У статті «Політико-правова аберація: нігілізм та зброя», опублікованій у співавторстві, особистий внесок здобувача полягає у пошуку, аналізі наукової літератури, формулюванні теоретичних положень, підготовці окремих висновків. У розділі колективної монографії «Дискреція обмеження прав і свобод людини в Україні», опублікованій у співавторстві, особистий внесок здобувача полягає у пошуку, аналізі наукової літератури, підготовці окремих висновків та пропозицій. У тезах «Дискреція обмеження прав і свобод людини» особистий внесок здобувача полягає у пошуку, аналізі наукової літератури, формулюванні теоретичних положень, узагальнені результатів дослідження.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, які об’єднують дев’ять підрозділів, висновку, списків використаних джерел і додатків. Загальний обсяг дисертації становить 225 сторінок, з них основного тексту – 8,09 аркушів. Список використаних джерел містить 247 найменування, які викладено на 30 сторінках, а додатки – на 10 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО–МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

1.1. Концептуальні підходи до розуміння захисту персональних даних в сучасних умовах

У XXI сторіччі, у зв'язку зі стрімким технологічним розвитком, цифровізацією державних послуг, використанням технологій штучного інтелекту та здійсненням відеоспостереження [1, С. 210], питання захисту персональних даних у сфері охорони державного кордону України стає надзвичайно актуальним.

Зберігання персональних даних осіб, відповідно до ст. 33 Конституції України (надалі – Конституція) [2], котрим гарантується свобода пересування та право вільно залишати територію України, за винятком обмежень, які встановлюються законом, здійснюється задля перевірки в необхідному обсязі з метою визначення наявності законних підстав для перетинання державного кордону особами та з метою протидії незаконному переміщенню осіб через державний кордон, незаконній міграції, а також незаконному переміщенню зброї, наркотичних засобів, психотропних речовин, боєприпасів та матеріалів і предметів, заборонених до переміщення через державний кордон [3, ст. 2] та з метою забезпечення прикордонної безпеки в інформаційній сфері.

Термін «персональні дані» все частіше вживається не лише у практичній юридичній діяльності, а й у наукових працях та у повсякденних відносинах юридичних і фізичних осіб, що вказує на важливість їх зберігання і не розголошення в інтересах людини.

Поряд з цим терміном вживаються й інші близькі до нього, терміни – «особиста інформація», «ідентифікаційні дані», «конфіденційна інформація», «приватні дані», «чутлива інформація», «біометричні дані», «контактні дані», «фінансові», «професійні дані» та «дані про місце знаходження». Велика кількість цих термінів, можуть бути використані в різних контекстах, залежно від того, яку інформацію потрібно обробити або захистити та позитивно впливає

як на розвиток наукової думки у сфері інформаційної безпеки, так і на практичне застосування законодавства у сфері персональних даних.

Зважаючи на вищевикладене, необхідно зазначити, що захист персональних даних є найбільш актуальною та нагальною потребою в сучасному розвиненому інформаційному світі. Концептуальні підходи до розуміння захисту персональних даних в сучасних умовах відображають низку теоретичних та практичних аспектів, що визначаються правовими, етичними, соціальними та технічними факторами.

У зв'язку із зазначеним, важливого значення набуває необхідність уточненням та конкретизація поняття «персональні дані», також більш точне визначення його місця серед багатьох інших понять, які визначають аналогічні або суміжні явища правової дійсності та вироблення раціональної й ефективної системи правових норм, які регламентують форми, методи, засоби та способи ефективного захисту персональних даних. Доцільно зазначити, що на сьогодні є 28 різних законодавчих визначень цього терміну [4].

Виходячи з вищезазначеного, з його мети, на виконання завдань даного дослідження, в даному розділі розкривається зміст поняття «персональні дані» та конкретизуються такі поняття як «захист» та «охорона», що в свою чергу визначить розуміння поняття «захист персональних даних», адже, в контексті забезпечення безпеки державного кордону України, захист персональних даних є важливим аспектом забезпечення національної безпеки.

В сучасному динамічному світі, котрий стрімко розвивається та змінюється, дедалі частіше суспільство використовує інформацію про фізичну особу, людину в цілому, громадянина держави тощо, в інтересах свого подальшого розвитку. В процесі взаємодії людини з навколишнім світом відбувається обмін інформацією, що породжує використання та обробку індивідуальних даних про особу, зокрема про її ім'я та по батькові, місце проживання, стан здоров'я, номер мобільного телефону, кредитну історію, страхування. Особисті майнові та немайнові права дозволяють нам виділити та ідентифікувати конкретного індивіда серед інших [5, С. 51]. Таким чином, у

сучасному світі, що швидко змінюється та розвивається, використання та обробка інформації про фізичну особу набуває надзвичайної важливості для забезпечення ефективної комунікації у різних сферах людської діяльності.

На нашу думку, головним критерієм ефективної комунікації в сучасному інформаційному суспільстві, є убезпечення інформації про фізичну особу від незаконного поширення, обробки та використання, адже певна інформація може бути використана для маніпуляцій, шахрайства, або інших незаконних дій, що може мати серйозні негативні наслідки для приватності та безпеки певної особи.

Для прикладу, Уповноважений Верховної Ради України з прав людини (надалі – Уповноважений), який відповідно до статті 101 Конституції України здійснює парламентський контроль за додержанням конституційних прав і свобод людини і громадянина [2] та здійснює контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбаченим Законом [6, ст. 22], зазначає, що під час парламентського контролю за додержанням законодавства про захист персональних даних було виявлено неправомірне поширення персональних даних близько 100 осіб шляхом їх розголошення на запит адвоката.

Так, на запит адвоката, який був адресований володільцю та який стосувався лише отримання персональних даних про свого клієнта, було отримано персональні дані не тільки його клієнта, але й інших осіб, які містились у документі.

Уповноважений звертає увагу, що у цьому разі, надаючи копії документів, які містять персональні дані, необхідно було знеособити персональні дані інших осіб, тобто вилучити відомості, які дають змогу прямо чи опосередковано ідентифікувати їх та обмежитись наданням персональних даних про одну особу (клієнта адвоката), адже з метою дотримання законодавства персональні дані інших осіб підлягають закриттю або ретушуванню у спосіб, що не дасть змоги їх відтворити та прочитати.

Відповідною посадовою особою Секретаріату Уповноваженого було складено протокол про адміністративне правопорушення, передбаченого

частиною четвертою статті 188-39 Кодексу України про адміністративні правопорушення (надалі – КУпАП), а саме: недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них [7]. Зазначений протокол направлено до місцевого загального суду.

З огляду на зазначену подію, Уповноважений закликає володільців персональних даних забезпечити захист персональних даних від незаконного поширення [8] та незаконного використання.

На сьогодні можна говорити про те, що через низький рівень правової обізнаності та правової свідомості громадян часто проявляються проблеми, пов'язані із захистом персональних даних. Звичайна людина, яка виступає учасником інформаційних відносин, підписуючи різного роду документи або переглядаючи сайти в мережі Інтернет, може потрапляти у своєрідну залежність якогось «товариства»: організації, супермаркета, банка, тощо.

Необізнана особа навіть не уявляє ким і задля чого її персональні дані можуть бути використані, залишаючи їх в обмін на послуги «товариств». Незліченні факти шахрайства, організована злочинність на державному кордоні України надзвичайно загострили проблему правового захисту прав фізичних осіб, через високу активність користувачів соціальних мереж у формуванні баз персональних даних [9]. На нашу думку, низький рівень правової обізнаності та правової свідомості громадян, щодо захисту персональних даних, може призвести до випадків шахрайства з метою заволодіння чужим майном, дискредитації особи або громадянина з метою нанесення шкоди професійній репутації, або інших незаконних дій з боку зловмисників.

Уповноваженим та його представниками, протягом 2022 року, для представників Національної школи суддів України (надалі – НШСУ), Національного агентства України з питань державної служби (надалі – НАДС), працівників Міністерства внутрішніх справ (надалі – МВС) України та працівників підрозділів системи МВС України, правових інспекторів праці Федерації профспілок України та її членських організацій проводилися лекції,

тренінги, навчання та круглі столи в онлайн-режимі, з питань захисту персональних даних [10, С. 6–7], а також проводилася та проводиться просвітницька робота серед суспільства щодо поглиблення знань про додержання права на захист персональних даних.

Одним із перших учених в сучасній, незалежній Україні, хто розпочав наукове дослідження в сфері персональних даних на нашу думку, є В. М. Брижко, який у своїй науковій роботі «Організаційно-правові питання захисту персональних даних», «підкреслюючи значення та важливість захисту персональних даних, цілком доречно визначає персональні дані як найбільш чуттєву, делікатну і важливу для людини інформацію та як особливий вид приватної власності, яка юридично виступає у формі виключного права власності і монополія на яку обмежується законом в інтересах дотримання прав та основних свобод інших осіб, а також в інтересах дотримання балансу прав людини, суспільства і держави, що посідає особливе місце в суспільних інформаційних відносинах» [11, С. 15].

Отже, інформація визначена як особливий вид приватної власності, має вирішальне значення для дотримання прав та основноположних свобод людини, а також збалансованого співвідношення між правами особи, суспільства і держави.

Розуміння важливості і необхідності ефективного захисту персональних даних є ключем до забезпечення спокою та благополуччя як окремої особи, так і всієї держави в цілому, адже це вимагає ефективних механізмів захисту приватності та збереження довіри громадськості до обробки їхніх особистих даних.

Науковці надають різні визначення терміну «персональні дані». Зокрема, як зазначає А. М. Чернобай, «під персональними даними працівника слід розуміти будь-яку інформацію, яка стосується конкретного працівника та необхідна роботодавцю у зв'язку із використанням праці цього працівника на підставі трудового договору. Це може бути тільки така інформація, яка необхідна роботодавцю у зв’язку з трудовими правовідносинами. Відповідно, поняття

персональних даних працівника вужче за поняття персональних даних про особу, оскільки йдеться не про всі відомості (факти, події, обставини життя фізичної особи), а тільки про такі обставини, що можуть характеризувати фізичну особу як працівника.

Тому працівникам і кандидатам на посаду необхідно гарантувати свободу самостійно вирішувати, чи потрібно надавати роботодавцю дані особистого характеру, тобто контролювати інформацію про себе. Цю свободу можна обмежити лише законними інтересами роботодавців, держави, третіх осіб» [12, С. 18–19].

Відповідно до Конвенції Ради Європи [13] «дані особистого характеру» визначаються як будь-яка інформація, що стосується певної або такої, що піддається ідентифікації особи, тобто дані особистого характеру – це будь-які відомості, які можуть бути використані для ідентифікації людини, такі як ім’я, адреса, номер телефону, ідентифікаційний номер тощо.

Таким чином, персональні дані працівника містять тільки ті відомості котрі необхідні роботодавцю для трудових відносин, а працівник повинен мати свободу щоб вирішувати, яку саме інформацію особистого характеру надавати, з обмеженням цієї свободи лише законними інтересами роботодавців, держави та третіх осіб.

Робота будь-якої організації безпосередньо пов’язана з підбором персоналу, накопиченням, обробкою, зберіганням і використанням даних про працівників. Непоодинокі факти, коли співробітники кадрових відділів часто не мають належних навичок роботи з персональними даними працівників, але щодня обробляють їх, і це найчастіше призводить до неправомірного поширення персональних даних. В основному це пов’язано з нерозумінням працівниками, які мають доступ до такої інформації, важливості її конфіденційності і настання відповідальності за її розголошення [14, С. 49], а також з відсутністю належного рівня знань щодо захисту персональних даних та відповідних процедур їх обробки. Важливо розуміти, що захист персональних даних є не лише вимогою Закону, але й етичним обов’язком кожного співробітника кадрового підрозділу.

Науковці М. В. Сокол та А. В. Тимощук вважають, що персональні дані працівника – це відомості про факти, події і обставини життя найманого працівника, що безпосередньо пов’язані з діловими якостями, які мають безпосереднє відношення до виконуваної ними трудової функції, та надаються роботодавцю з метою забезпечення дотримання законів та інших нормативно правових актів, сприяння працівникові в працевлаштуванні, навчанні, підвищенні кваліфікації та перекваліфікації, забезпечені охорони праці, контролю за кількістю і якістю виконуваної роботи [14, С. 53]. Тобто персональні дані працівника – це інформація про його життєві обставини, яка стосується його професійних якостей та надається роботодавцю для дотримання законодавства, допомоги у працевлаштуванні, навчанні, підвищенні кваліфікації, охороні праці та контролю за виконанням роботи.

На думку С. М. Гусарова та К. Ю. Мельника, персональні дані працівника – це будь-яка інформація, яка стосується конкретної фізичної особи, що працює на підставі трудового договору, надана роботодавцю або зібрана ним відповідно до законодавства [15, С. 141], а саме будь-які інші дані, що прямо чи опосередковано стосуються цієї особи, такі як: ім’я, прізвище та по-батькові, дата та місце народження, адреса проживання, контактні дані (телефон, електронна пошта), ідентифікаційний номер (ІПН), освіта та професійна кваліфікація, інформація про сімейний стан та склад родини, медична інформація, інформація про трудовий стаж та попередні місця роботи.

Дослідник Р. І. Чанишев вважає, що персональні дані працівника варто визначити як інформацію, необхідну роботодавцю у зв’язку з трудовими відносинами, що стосується конкретного працівника і пов’язана з його професійною кваліфікацією, діловими, професійними якостями. Ця інформація стосується також вимог, що можуть бути висунуті до працівника у зв’язку з характером роботи [16, С. 97], яку він виконує.

Таким чином до персональних даних працівника можуть належати відомості про його освіту, професійний досвід, кваліфікаційні характеристики, результати атестацій та інших оцінювань, відомості про стан здоров'я, необхідні

для виконання конкретних трудових функцій, а також інша інформація, що стосується виконання трудових обов'язків та забезпечення трудової дисципліни.

На нашу думку, запропоновані дослідниками визначеннями персональних даних працівника, є дискусійними, адже якщо певна інформація дає змогу володільцю виділити із групи людей конкретну особу, то цю інформацію можна вважати персональними даними, а «дані, які самі по собі не є персональними даними, за певних обставин (коли вони дають змогу ідентифікувати особу) ними стають» [17]. Варто зазначити, що вичерпними відомостями про працівника може служити будь-яка окрема характеристика (номер паспорта або дата видачі диплома про здобуту освіту, або місце і дата народження), яка дасть змогу ідентифікувати його серед інших працівників. Таке визначення не досить точне, оскільки створюється враження, що йдеться виключно про ідентифікацію раніше невідомої особи, в той час як інформація може збиратися і про вже відому особу. Тому персональні дані працівника необхідно розглядати з урахуванням специфіки, цілей і завдань трудового права і законодавства про працю [14, С. 52], що мають захищати не лише конфіденційність, а й права працівників на вільне здобуття інформації про себе, а також контролювати обробку їх персональних даних в робочих цілях.

В контексті сучасного розвинутого інформаційного середовища, де збільшується об’єм обробки, аналізу та обміну персональними даними, забезпечення захисту цих даних стає надзвичайно важливим завданням. Принцип свободи вибору працівників щодо надання роботодавцю особистої інформації є ключовим для забезпечення конфіденційності та приватності в робочому середовищі.

Науковиця А. В. Тунік прийшла до висновку, що персональні дані є предметом дослідження багатьох юридичних наук – теорії держави та права, інформаційного права, адміністративного права, кримінального права, цивільного права та інших.

Але відсутній єдиний уніфікований понятійно-категоріальний апарат в зазначеній сфері, оскільки здебільшого у дослідженнях використовуються як

синонімічні поняття без чіткої аргументації такі категорії: «персональні дані», «особиста інформація», «приватна інформація про фізичну особу», «приватна інформація», «персональна інформація», «конфіденційна особиста інформація», «персоніфікована інформація» тощо.

На думку А. В. Тунік поняття «персональні дані» та «інформація про особу» є змістовно ідентичними. Не всі персональні дані є інформацією з обмеженим доступом. Винятки охоплюють знеособлені персональні дані та персональні дані певних категорій громадян, зокрема персональні дані фізичної особи, яка претендує зайняти чи займає виборну посаду (у представницьких органах) або посаду державного службовця першої категорії. Саме тому поняття «персональні дані» та «конфіденційна інформація про особу» співвідносяться між собою як загальне та часткове, тобто саме конфіденційна інформація про особу є завжди інформацією з обмеженим доступом, а її поширення без згоди цієї особи можливе лише у чітко визначених випадках: у інтересах національної безпеки, економічного добробуту та прав людини. Конфіденційна інформація про особу охоплює поряд з іншими відомостями і інформацію про особисте та сімейне життя особи [18, С. 29–30].

Таким чином поняття «персональні дані» та «конфіденційна інформація про особу» взаємопов’язані, адже конфіденційна інформація завжди є частиною персональних даних і завжди вимагає обмеженого доступу, за винятком чітко визначених ситуацій, таких як національна безпека, економічний добробут та права людини.

Зокрема, Д. В. Цвірюк класифікує персональні дані за рахунок уведення ним нових критеріїв: характер даних про особу, здатність змінюватися у часі та джерело походження даних про особу, що дозволило визначити їх сутність, охарактеризувати окремі особливості виникнення та існування, а також розкрити особливості створення й функціонування баз персональних даних та підстав для обробки персональних даних в них. Окремо вчений наголошує на необхідності правильного співвідношення й розмежування понять «персональні дані» і «конфіденційна інформація», оскільки ці поняття не є тотожними, адже

незважаючи на наявність спільних ознак, персональні дані – це лише різновид конфіденційної інформації, яка містить виключно відомості про фізичну особу [19, С. 4–5]. Таким чином вчений зауважує, що класифікація персональних даних за новими критеріями підкреслює їх важливість і вимагає правильного розмежування від поняття «конфіденційна інформація», наголошуючи на їх відмінностях і значущості для забезпечення конфіденційності особистих відомостей.

Розглянутий вище процес класифікації персональних даних за допомогою встановлення нових критеріїв, таких як характер даних, їх змінюваність у часі та джерело походження. Зазначене допоможе визначити сутність персональних даних, висвітлити особливості їх виникнення та функціонування. Особлива увага має приділятися розмежуванню понять «персональні дані» та «конфіденційна інформація», що підкреслюється їх відмінністю та необхідністю правильного їх розуміння. Персональні дані розглядаються як окремий вид конфіденційної інформації, що містить відомості про фізичну особу.

Як наголошує М. В. Різак, зміст який вкладається законодавством у поняття «персональні дані», а саме – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [6, ст. 2], є дуже широким, що підтверджується відкритістю переліку відомостей, віднесених до числа цих даних. Відтак, зважаючи на саму природу персональних даних, повністю їх перерахувати досить складно. Це обумовило формування окремих положень, згідно з якими суб’єкт має право частково самостійно формувати свій «інформаційний портрет», вирішуючи, які з характеристик, що його ідентифікують, слід віднести до числа персональних даних, а які ні.

Зокрема, акцентується увага на тому, що законодавством також не встановлено чіткої класифікації персональних даних. Проведений дослідником аналіз дозволив зробити висновок про наявність основних категорій персональних даних: звичайні, спеціальні (вразливі) та біометричні. Водночас для зменшення надмірного регулювання у сфері персональних даних та покращення комунікації в суспільстві, яке відбувається під стрімким розвитком

та інтеграцією інформаційно-комунікаційних систем, запропоновано закріпити на законодавчому рівні таку класифікацію персональних даних: загальні персональні дані, спеціальні персональні дані та вразливі персональні дані [20, С. 15].

Таким чином, науковцями визначено широкий спектр персональних даних, що підкріплюється потребою суб'єктів визначати самостійно, які характеристики, що їх ідентифікують, вони вважатимуть за персональні, що свідчить про необхідність ясної класифікації цих даних у правовому полі.

На думку М. І. Саєнка, під поняттям «персональні дані» варто розуміти дані про живу людину, котра ідентифікована, або може бути ідентифікована на основі цих даних, чи на основі додаткової інформації, що може потрапити до особи, яка контролює дані, що містять вираження становлення до цієї людини й указівку на певну мету, або план стосовно цієї людини з боку особи, яка контролює дані, або іншої особи [21, С. 103], яка здійснює обробку даних.

Науковець Г. В. Виноградова зазначає, що персональні дані – це сукупність документованих або публічного оголошених відомостей про фізичну особу [22, С. 176], які дозволяють її ідентифікувати. У свою чергу О. Дяковський розуміє персональні дані як відомості чи сукупність відомостей про живу фізичну особу, яка ідентифікована або може бути конкретно ідентифікована з урахуванням встановленого законом поділу персональних даних [5, С. 57], що містять таку інформацію, яка дозволяє ідентифікувати особу, а саме: ім'я, адресу, номер мобільного телефону, електронну пошту, номер та серію паспорта, генетичні та біометричні дані тощо.

Як відмічає В. М. Брижко, поняття «персональні дані» охоплює об'єктивні та суб'єктивні відомості про особисте, сімейне чи публічне життя фізичної особи, що виражені у формі літер, чисел, графіки, фото, звуку чи відео, символів, якщо вони дозволяють ідентифікувати таку особу. Для визнання відомостей персональними даними обов'язковою є наявність зв'язку між такими відомостями та конкретною особою [23, С. 59]. Таким чином поняття «персональні дані» охоплює об'єктивні та суб'єктивні відомості про особисте,

сімейне чи публічне життя фізичної особи, виражені у різних формах, які дозволяють ідентифікувати цю особу.

Можна зробити висновок, що в існуючих визначеннях поняття «персональні дані» в основу покладений термін «ідентифікація». У загальному значенні ідентифікація (від лат. Identifico – «ототожнюю») означає визначення відповідності предмета, біологічного організму, особи (юридичної, фізичної), певним, конкретним, лише їм властивим ознакам. Ідентифікація особи – визначення за допомогою спеціальних методів тотожності суб'єкта, конкретній особі [24, С. 488]. Таким чином визначення поняття «персональні дані» базується на концепції ідентифікації, що передбачає встановлення відповідності між суб'єктами та конкретною особою за допомогою унікальних ознак.

Отже, наукові погляди щодо персональних даних відзначаються великою широтою та складністю, оскільки відкритість переліку інформації, що вважається персональними даними, дає можливість індивідуально визначати обсяг цих даних. Аналіз показує наявність основних категорій персональних даних: звичайні, спеціальні (вразливі) та біометричні. З метою спрощення регулювання і покращення комунікації у суспільстві, пропонується закріпити таку класифікацію на законодавчому рівні: загальні, спеціальні та вразливі персональні дані. Це допоможе уникнути надмірного регулювання та встановити зрозумілі рамки для збору, обробки та захисту персональних даних у світі стрімкого розвитку інформаційних технологій.

В той же час, попри значну увагу науковців, аналіз останніх публікацій свідчить, про те, що питання захисту персональних даних переважно розглядалися у загальнотеоретичному аспекті, не торкаючись до розмежувань таких понять як «захист» та «охорона».

З погляду теорії права, необхідне ретельне вивчення та чітке визначення юридичних термінів і понять, оскільки теорія права виконує роль інтерпретатора, який сприяє розкриттю сутності різних юридичних термінів та державно-правових явищ, і робить це через ретельне аналізування їх значення та надання відповідних пояснень для загального розуміння [25, С. 610–616].

Таким чином побудова правової держави вимагає систематичних змін, серед яких ключове значення має уніфікація правової системи України та сфери законодавства. Однак, також важливо усунути існуючі колізії у сфері законодавства та забезпечити точність і вивіреність юридичних термінів. Це є фундаментальними аспектами для побудови системи ефективного вітчизняного законодавства. Реформування юридичної термінології відіграє ключову роль у цьому процесі, оскільки воно спрямоване на створення унормованої мови всіх галузей права на сучасних методологічних засадах.

Зазначимо, що проблема співвідношення понять «захист» і «охорона» у правовій літературі стоїть досить гостро, і не є новою. Дослідженню цій проблемі приділяли увагу такі вчені, як: Галунько В. В. [29], Гіда Є. О. [30], Назаров В.В. [32] Обущак О. О. [31], Ромовська З. В. [33] та інші.

Відповідно до Великого тлумачного словника сучасної української мови, слово «охорона» означає оберігання кого/чого-небудь, вартування, сторожування, а слово «захист» – заступництво, охорона, підтримка [26, С. 870], виступаючи таким чином як захисник. За юридичною енциклопедією «охорона» означає захист, забезпечення, а «захист» означає забезпечення, охорона [27, С. 432] прав та інтересів, вжиття заходів задля попередження загроз, або усунення шкоди, що може бути завдана державі.

Отже, з вищевикладеного випливає, що в обох випадках вказані терміни мають практично однаковий зміст. Тому один з підходів до визначення понять «охорона» і «захист», що обговорюється серед юридичних науковців, ґрунтується на їх збігу та взаємозамінності.

На думку В. О. Попелюшко, терміни «захист» та «охорона» означають діяльність держави, її органів, громадських та інших недержавних організацій, особи, спрямовані на запобігання, подолання справжньої чи уявної протиправної шкоди, що загрожує, або вже спричиненої правам, свободам, законним інтересам особи, суспільства, держави [28, С. 66], в умовах забезпечення прикордонної безпеки, як аспекту національної безпеки, що містить контроль, профілактику і реагування на загрози, пов'язані з нелегальною міграцією, контрабандою,

терористичними та іншими протиправними діями, які можуть порушити суверенітет і цілісність держави.

До науковців, які розмежовують терміни «охорона» та «захист», належать Гіда Є. О. та Галунько В. В., котрий вважає охорону вищим поняттям порівняно із захистом зазначаючи, що охорона – це стан, спрямований на запобігання правопорушенням, усунення перешкод, а захист він розуміє як дії спрямовані на відновлення порушених прав, свобод та законних інтересів фізичних і юридичних осіб, усунення перешкод щодо їх здійснення засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності [29, С. 247].

Є. О. Гіда вважає, що охорона включає заходи, які застосовуються до моменту порушення прав людини, а захист – після вчинення правопорушення [30, С. 759], з метою відновлення порушених прав. Таким чином охорона прав людини включає в себе заходи, спрямовані на запобігання порушенням прав заздалегідь. Ці заходи включають у себе правове регулювання, освіту, просвітництво та систему моніторингу. Захист прав, у свою чергу, активується після факту правопорушення з метою відновлення порушених прав та компенсації завданих збитків. Отже, в комплексі охорона та захист прав людини створюють цілісну систему забезпечення правової безпеки та справедливості. На нашу думку слід погодитися з науковцями, адже дійсно захист відбувається лише у випадку загрози, а охорона здійснюється постійно.

На наш погляд, для забезпечення ефективного захисту прав необхідно створити механізми, які би дозволяли уповноваженим особам реалізувати свої права безпосередньо. Це може бути здійснено через різноманітні механізми, такі як медіація, арбітраж або альтернативні форми конфліктного врегулювання, які дозволяють сторонам досягти взаємовигідних угод без необхідності втручання публічних органів. Це сприятиме ефективнішому врегулюванню конфліктів та забезпечить більш широкий доступ до справедливості для всіх громадян.

Науковець О. О. Обущак зазначає, що охорона є більш широким поняттям, ніж захист. Вона являє собою сукупність заходів, спрямованих на забезпечення нормальної реалізації прав, а також на захист прав у випадку їх порушення або оспорювання через конкретні засоби державного впливу, які існують переважно в правовій формі і можуть проявлятися або через встановлення правових норм, або через їх, насамперед, позитивне застосування.

Якщо ж розглядати поняття «захист», то слід зазначити, що воно пов'язане не з стандартною реалізацією прав, а лише з конкретним правопорушенням або оспорюванням прав, тобто під «захистом» розуміється передбачена законодавством діяльність відповідних публічних органів щодо поновлення порушеного права, припинення таких порушень, а також створення необхідних умов для притягнення до юридичної відповідальності осіб, винних у вчиненні протиправних дій, внаслідок яких було завдано шкоди правам та законним інтересам суб'єктів. Таким чином, поняття «охорона» і «захист» співвідносяться, як ціле й частина [31, С. 75−86].

На думку В. В. Назарова поняття «охорона» та «захист» перебувають в одній площині, оскільки вони мають єдиний критерій виміру – права та свободи людини і громадянина [32, С. 385–391], а отже охорона стосується заходів, спрямованих на запобігання порушення цих прав і свобод, тоді як захист передбачає вжиття заходів у випадку їх порушення або загрози порушення.

Про взаємообумовленість категорій «охорона» та «захист» говорить З. В. Ромовська, проте повністю тотожними їх не вважає. На її думку, правова охорона містить в собі систему різноманітних юридичних заходів із метою вберегти право від можливого порушення. Таким чином, можливість захисту суб'єктивного права і конкретне здійснення захисту є одним із засобів правової охорони. Суть правового захисту полягає у тому, що він є реалізацією обраного правозастосовним органом заходом державного примусу. Своїм конкретним застосуванням примусові заходи припиняють порушення суб'єктивного права, забезпечують необхідні умови для його здійснення, поновлюють порушене право або тим чи іншим способом усувають наслідки його порушення [33, С. 11-

13]. Таким чином головною метою цих заходів є забезпечення реального і ефективного захисту прав громадян та інших суб'єктів права, підтримка законності і порядку в суспільстві.

Дослідивши наукові погляди, ми прийшли до висновку, що доцільним визначенням поняття «охорона», є визначення, котре відповідає вимогам сьогодення в умовах стрімкого технологічного розвитку суспільства, а саме «охорона» – це сукупність різноманітних організаційно-правових заходів спрямованих на запобігання можливого порушення правопорядку, забезпечення безпеки об’єктів, збереження майна і захисту громадян від протиправних дій.

Наразі вважаємо, що слід прийти до такого висновку, що думки науковців щодо визначення поняття терміну «персональні дані» різняться, але на нашу думку, слід погодитися із визначеннями, де «персональні дані» визначаються як: будь-яка інформація, що стосується конкретної фізичної особи, яка може бути ідентифікована на основі цієї інформації або додаткових даних.

Таким чином, захист персональних даних у сфері охорони державного кордону України – це сукупність різноманітних організаційно-правових заходів спрямованих на запобігання можливого порушення правопорядку, забезпечення безпеки об’єктів, збереження майна і захисту громадян від протиправних дій з інформацією, що стосується конкретної фізичної особи, яка може бути ідентифікована на основі цієї інформації або додаткових даних, з метою забезпечення прикордонної безпеки, як аспекту національної безпеки в цілому.

1.2. Персональні дані як предмет адміністративно-правового регулювання

Серед важливих характеристик держави, які істотно впливають на всі процеси соціально-економічного розвитку суспільства, є рівень інформаційного забезпечення системи органів державної влади. Забезпечення вільного доступу до інформації та її поширення, підвищення конкурентоспроможності економіки держави й розширення можливостей її інтеграції до європейської економічної системи, підвищення ефективності державного управління – всьому цьому сприяють інформаційно-комунікативні технології.

У зв’язку із зростанням фактів частих атак на сервери державних органів, на персональну інформацію про фізичних осіб, а також загроз корпоративної безпеки, а саме розкрадання з подальшим поширенням в мережі корпоративної інформації, тощо, ми спостерігаємо зростання не лише наукового, але і практичного інтересу до тематики даного дослідження [34, С. 70].

Це зумовлює необхідність глибшого аналізу існуючих загроз, розробки ефективних методів захисту інформації та впровадження сучасних технологій кібербезпеки для забезпечення стійкості як державних, так і корпоративних систем.

Питання захисту інформації, зокрема, що стосується персональних даних, наразі перебуває на етапі удосконалення як у національному, так і в міжнародному, політичному, правовому та науковому дискурсі. Адже захист персональних даних є не просто обов’язком держави й предметом державно-правового регулювання, а його необхідно розглядати в поєднанні із захистом прав людини [35, С. 75].

Науковий інтерес до проблематики правового регулювання та охорони суспільних відносин у сфері приватного життя фізичної особи завжди залишається дискусійним та динамічним [34, С. 70], оскільки охоплює широкий спектр питань, пов’язаних із визначенням меж приватності та необхідністю захисту персональних даних в умовах розвитку Інформаційних технологій (надалі – ІТ).

На думку Р. О. Стефанчука, сфера приватного життя є доволі специфічною, адже вона визначається поняттям особистої свободи фізичної особи та не може зазнавати безцеремонного втручання з боку законодавця, оскільки тісно співвідноситься із сферами людської життєдіяльності, які знаходяться за межами правового регулювання. Складність позитивного законодавчого врегулювання приватного життя людини полягає, перш за все, у визначенні та встановленні меж, які з точки зору моральних засад суспільства є допустимими і не будуть розглядатись як неправомірне втручання законодавця [36].

Таким чином, сфера приватного життя людини є надзвичайно делікатною та багатогранною. Її регулювання вимагає обережного підходу, що базується на принципах поваги до особистої свободи та моральних засад суспільства.

Забезпечення охорони та захисту персональних даних є одним із основоположних прав людини. Воно закріплено у фундаментальних документах України, які гарантують відповідні права і свободи людини.

Варто зауважити, що законодавство України у сфері захисту персональних даних базується на міжнародних правових актах, метою якого є захист основних прав і свобод, а особливо права на невтручання в особисте життя.

Як зазначають К. М. Врублевська-Місюна та В. П. Тичина, доволі тривалий час нормативним фундаментом розвитку законодавства у сфері захисту персональних даних була [37, С. 152] Директива 95/46/ЄС Європейського Парламенту і Ради (надалі – Директива 95/46/ЄС) [38], яка встановлювала детальні вимоги щодо організації системи захисту персональних даних.

У подальшому розвиток правового регулювання у сфері захисту персональних даних отримав своє відображення у Директиві 2002/58/ЄС Європейського Парламенту і Ради (надалі – Директива 2002/58/ЄС) [39], яка була ухвалена як спеціалізоване доповнення до Директиви 95/46/ЄС [38] та спрямована на врегулювання специфічних питань, пов’язаних із конфіденційністю комунікацій у телекомунікаційній та інформаційній сфері.

На заміну Директиві 95/46/ЄС був прийнятий Регламент Європейського Парламенту і Ради (ЄС) 2016/679 (надалі – Регламент 2016/679) [40], який встановлює нові європейські стандарти у сфері захисту приватності особи.

На національному рівні ключовими документами у сфері захисту персональних даних [41, С. 8], є Конституція України (надалі – Конституція) [2], Закон України «Про захист персональних даних» [6], документи у сфері захисту персональних даних, прийняті Уповноваженим Верховної Ради України з прав людини. Вагоме значення мають також низка інших законів, як наприклад, Закон України «Про доступ до публічної інформації» [42] та Закон України «Про інформацію» [43].

Так, в статті 32 Конституції [2] зазначено, що ніхто не може зазнавати втручання в його особисте та сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, а тому громадянам важливо розуміти і знати свої права щодо захисту своїх персональних даних і використовувати належні заходи безпеки та контролю щодо їх збереження.

Зважаючи на вищевикладене, варто відзначити, що у формуванні правового захисту персональних даних відправним є визначення змісту та обсягу істотних ознак термінів «персона» та «персональні дані» [44, С. 6], оскільки саме ці поняття є фундаментальними для побудови ефективної системи регулювання, яка забезпечує баланс між правами особи на приватність та потребами суспільства в обробці інформації.

Термін «персона» [44, С. 6] походить із давньогрецької мови, спочатку означав театральну маску, а з часом набув значення, пов’язаного із соціальною, юридичною та індивідуальною ідентичністю.

У творах Цицерона поняття «persona» вже включало юридичний і соціальний зміст, а також індивідуальні якості. Римське право розглядало особу як вільну людину, що протиставлялася речам і діям.

З поширенням християнства ідея рівності людей перед Богом сприяла формуванню поняття «права людини» і свободи. У середньовіччі Фома Аквінський використав термін «personalitas» для позначення людської індивідуальності.

Сьогодні поняття «особа» і «особистість» використовуються як синоніми, означаючи цілісність інтелектуальних, емоційних і соціально-культурних якостей людини [44, С. 6], які визначають її унікальність, індивідуальність і здатність до самовираження та взаємодії з суспільством.

З метою забезпечення реалізації прав, закріплених в Конституції України [2] та створення ефективних механізмів для їх застосування Верховною Радою

України було ухвалено Закон України «Про захист персональних даних» [6], який, відповідно до ст. 1 регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних та відповідно до ст. 2 якого «персональними даними» є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Виходячи з вищезазначеного, на нашу думку, варто також проаналізувати такі важливі поняття як: «людина», «громадянин» та «особа», які мають пріоритетне значення у нормотворчій та правозастосовній діяльності [45, С. 82], оскільки вони є ключовими для визначення правового статусу та забезпечення прав і свобод людини в інформаційній сфері прикордонної безпеки.

Відповідно до ст. ст. 3, 21, 28, 32, 34 Конституції [2] суб’єктами інформаційних відносин визначаються «людина», відповідно до ст. ст. «громадянин» ст. ст. 32, 41, 54, та «особа», ст. 32, які мають права та обов’язки щодо отримання, використання, поширення та зберігання інформації.

Людина – це узагальнююча назва для всіх представників людства, яка поєднує в собі відображення всіх спільних якостей людей (як біологічного, так і соціального змісту). Кожна людина народжується індивідом, формується в процесі життя як особистість та кристалізується в індивідуальність через реалізацію своїх природних, психічних, духовних та соціальних особливостей у соціально значущі якості протягом всього свого життя [46, С. 110].

Згідно тлумачного словника української мови, слово «людина» визначається як: будь-яка особа, кожний, людська постать та особа як втілення високих моральних та інтелектуальних якостей [46, С. 503]. Також термін «людина» вказує на біосоціальну істоту, форму земного життя, яка має здатність мислити, створювати й застосовувати для задоволення своїх потреб знаряддя праці, володіє мовою й розвивається за умови широкого та тісного спілкування із собі подібними [47, С 326].

В Українській юридичній енциклопедії [48, С. 640], поняття «громадянин» визначено як фізична особа, статус якої обумовлений належністю до громадянства певної країни. Громадяни є найчисельнішою категорією населення, володіють повнішим обсягом прав і свобод, ніж інші – іноземці та особи без громадянства. Громадянин є завжди людиною.

А з юридичної точки зору не кожна людина може бути громадянином. Звідси випливають певні відмінності у правовому статусі «людини» і «громадянина». Перебування людини у громадянстві країни обумовлює поширення на неї всього обсягу законодавчо гарантованих на території відповідної держави прав і свобод, зокрема пов'язаних з її участю в політичному житті, управлінні державними справами, що невластиве негромадянам, забезпеченням інформаційної безпеки тощо [48, С. 640].

Особа визначається як людина, яка знаходиться в системі суспільних зв'язків та відносин [49, С. 351] та володіє рисами та якостями, які визначають людину в суспільному значенні та містять її соціальну оцінку [50, С. 49].

Зміст поняття «особа» є значно ширший, ніж термін «громадянин», що означає лише осіб, які володіють громадянством України. З іншого боку, поняття «особа» в юридичному значенні вважається більш загальним, ніж «людина». Воно передбачає такого носія прав і свобод, який володіє не тільки отриманими від народження правами і основоположними свободами, що властиво для статусу людини, а й набутим у процесі життя відповідним соціальним статусом, що визначає людину.

Тобто поняття «особа» у зв'язку державними інтересами може об'єднувати в собі поняття «людина» і «громадянин» та визначатися у правових нормах, що встановлені державою і забезпечуються її примусовою силою [51, С. 17].

У цьому контексті важливим є також уточнення змісту терміну «персональні дані». На наше переконання, слід погодитися з думкою науковців, щодо визначення терміну «персональні дані», адже воно є достатньо лаконічним і чітким та відповідає існуючим міжнародним підходам до розуміння цього

поняття [52, С. 21], чіткістю його розуміння, як в рамках теоретичних наукових досліджень, так і під час практичного використання.

Крім того вищезазначене визначення охоплює як теоретичні, так і практичні аспекти ідентифікації, що дозволяє ефективно застосовувати його у різних сферах діяльності. Особливо важливо, що це визначення враховує можливість ідентифікації особи навіть за мінімальним обсягом даних, що забезпечує його універсальність і практичну значущість.

Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Ідентифікованою особа вважається, якщо її можна безпомилково виділити серед інших. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи). Однак, за певних умов наявність меншої кількості інформації чи певного об'єму іншої інформації є достатніми для того, щоб ідентифікувати особу [52, С. 21] конкретно.

Необхідно зазначити, що відповідно до ст. 3 Закону [53] ідентифікувати – це здійснювати комплекс заходів, що дає змогу виконувати пошук за принципом «один до багатьох», зіставляючи дані (параметри) особи, у тому числі біометричні, з інформацією Реєстру, а ідентифікація особи – це встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних, тощо.

Однак, як зазначає дослідниця О. О. Самойленко, попри здійснення комплексу заходів щодо ідентифікації особи, шляхом порівняння даних, законодавством України не встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, адже сутність інформації та її різновиди, які складають базу персональних даних є досить широкою [54, С. 32].

У цьому контексті варто звернути увагу на вимоги чинного законодавства щодо надання певних документів, які містять персональні дані, адже в окремих вони різняться.

В статті 24 Кодексу законів про працю України [55], зазначено, що громадянин при укладанні трудового договору зобов'язаний подати паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, також документ про освіту (спеціальність, кваліфікацію), про стан здоров'я та інші необхідні документи, котрі потрібні для виконання роботи. У разі, якщо трудовий договір укладається з особою, котра не досягла повноліття, також додаються документи, котрі підтверджують їх вік.

На нашу думку, хоча в українському законодавстві і закріплено загальні положення щодо використання персональних даних, відсутність чіткого визначення їх складу може створювати певну правову невизначеність у практичному застосуванні. Особливо це може проявлятися в контексті вимог щодо надання документів, які містять персональні дані, у різних сферах правовідносин, а особливо таких як трудові відносини. Вважаємо, що запровадження детального переліку персональних даних та уніфікованих вимог до їх використання сприятиме вдосконаленню правового регулювання і забезпечить захист прав фізичних осіб.

У зв'язку з цим персональні дані працівника, які містяться в паспорті або документі, що посвідчує особу, в трудовій книжці, документі про освіту (спеціальність, кваліфікацію), документі про стан здоров'я та інших документах, які він подав при укладенні трудового договору, обробляються володільцем бази персональних даних на підставі статті 24 Кодексу [55] виключно для здійснення повноважень володільця бази персональних даних у сфері правовідносин, які виникли в нього з працівником на підставі трудового договору (контракту). Отже інформація про найманих працівників складає базу персональних даних оскільки містить особові справи, трудові книжки, копії паспортів, документів про освіту та інше [54, С. 33].

Варто зазначити, що персональні дані, наприклад, військовослужбовців Державної прикордонної служби України (надалі – ДПСУ), можуть містити таку інформацію, як: посада, військове звання, прізвище та ім'я, підрозділ, серія та номер службового посвідчення, номер наказу про призначення (переміщення) на

посаду, дата народження, адреса реєстрації та місце проживання, ідентифікаційний номер, медичну інформацію та інші дані.

Отже інформація про найманих працівників та військовослужбовців ДПСУ складає базу персональних даних оскільки вона містить особові справи, в яких є копії документів, а саме – паспорта, ідентифікаційного коду (або довідки про відмовлення від ідентифікаційного коду в зв'язку з певними релігійними переконаннями), документів (дипломів та додатків) про здобуту освіту (курсів підвищення кваліфікації), автобіографії, медичної та іншої інформації.

Законом України «Про захист персональних даних» [6, ст. 2] база персональних даних визначається як іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних та створюється з метою обробки, зберігання, захисту та передачі персональних даних відповідно до чинного законодавства.

До бази персональних даних про фізичну особу віднесено дані, які зберігаються та обробляються відповідним програмним забезпеченням (електронна база) та дані, що зберігаються та обробляються на паперових носіях інформації (документальна паперова база). Для забезпечення легкого доступу до персональних даних використовуються картотеки персональних даних. Це структуровані бази даних, які групують інформацію про фізичних осіб за визначеними критеріями. Такі картотеки підтримуються та зберігаються на всіх підприємствах, установах та організаціях, незалежно від їхньої форми власності та підпорядкування, що здійснюють обробку персональних даних відповідно до законодавства України [54, С. 33].

Бази персональних даних є основним інструментом для впорядкування інформації та надання доступу до неї для службового використання. Картотеки персональних даних мають забезпечувати високий рівень безпеки та конфіденційності інформації, а також дотримання вимог законодавства щодо захисту персональних даних.

Необхідно зазначити, що відповідно до ст. 2 Закону [6] володільцем бази персональних даних є фізична або юридична особа, якій законом або за згодою

суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних та процедуру їх обробки, якщо інше не визначене законом.

Не викликає труднощів визначення володільця, коли мова йде про приватних суб'єктів, які в більшості випадків дійсно самостійно визначають ціль обробки, склад даних та процедури їх обробки. Дещо інша ситуація, коли мова йде про обробку персональних даних, наприклад ведення реєстру, державними органами влади. У таких випадках мета обробки, склад даних, порядок їх обробки, як і те, хто є володільцем, зазвичай визначено законодавством, а не самим володільцем. Слід наголосити, що на практиці саме законодавством визначається володілець, а не законом, як це вказано у визначенні [41, С. 14].

Науковці, М. В., Городиський І. М., Саттон Г. та О. М. Родіоненко О. М., зазначають, що зазвичай володільцем бази персональних даних є юридична чи фізична особа, окрім того:

1) якщо одні і ті дані окремо зберігаються у декількох суб'єктів (наприклад юридичних осіб), вони усі є володільцями;

2) якщо рівним доступом до однієї бази даних користуються два суб'єкти і кожен може приймати на свій розсуд рішення щодо обробки наявних у ній даних, їх слід розглядати як співволодільців;

3) якщо двоє чи більше суб'єктів мають різні рівні доступу до однієї бази даних і кожен може приймати рішення щодо обробки наявних у ній даних, до яких він має доступ, кожен з них є володільцем вказаного об'єму даних.

Поширеним прикладом такого виду обробки є функціонування міжвідомчих баз даних, порядок функціонування яких визначається спільними документами [52, С. 27–28].

Однак, якщо доступ до однієї бази даних мають лише тимчасові користувачі або користувачі з обмеженими правами, такі користувачі не мають статусу володільців даних. Також, якщо доступ до даних обмежено лише для здійснення певних операцій, наприклад, технічного обслуговування, такі особи

також не визнаються володільцями даних, оскільки їхні дії мають вузько визначений характер та обмежений вплив на обробку даних.

Варто зазначити, що функціонування баз персональних даних не можливе без розпорядника бази персональних даних, котрим згідно ст. 2 Закону [6] може бути фізична чи юридична особа, якій володільцем бази персональних даних або законом надано право обробляти ці дані, здійснюючи, таким чином, належну обробку, контроль та захист персональних даних громадян, які перетинають державний кордон України. Необхідно зазначити, що розпорядник бази персональних даних є співробітником організації, який працює на постійній основі та забезпечує, організовує і проводить роботу у зв'язку із захистом персональних даних [44, С. 75].

Відповідно до положень ст. 4 Закону [6] розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу. Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно договору, укладеного в письмовій формі. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі про обробку персональних даних.

У договорі також зазначаються права та обов’язки розпорядника персональних даних та вимоги до забезпечення захисту персональних даних.

Розпорядник персональних даних також зобов’язаний забезпечити конфіденційність і безпеку персональних даних, які йому довірені для обробки та не має права використовувати персональні дані для власних потреб або передавати їх третім особам без відповідного дозволу володільця даних.

Крім того, розпорядник персональних даних повинен забезпечувати реалізацію прав суб’єктів персональних даних, таких як право на доступ до своїх даних, право на їх виправлення, видалення чи обмеження обробки, а також право на заперечення проти обробки в передбачених законодавством випадках.

Варто звернути увагу на те, що недотримання умов договору або вимог законодавства щодо обробки персональних даних може призвести до відповідальності розпорядника персональних даних, включаючи адміністративну або кримінальну відповідальність залежно від характеру порушення.

Таким чином, встановлюються ключові аспекти щодо поняття розпорядника та його відносин із володільцем, визначаючи правові обов'язки та відповідальність кожної сторони. Розпорядник має зобов’язання діяти в інтересах володільця з урахуванням встановлених законом обмежень та умов, забезпечуючи збереження та раціональне використання майна. Водночас, володільцеві надаються певні права та можливості контролю за діяльністю розпорядника для забезпечення відповідності його дій законодавству та визначеним угодами [6].

На нашу думку, володільці та розпорядники персональних даних все ж таки повинні дотримуватися конфіденційності та зобов’язані здійснювати необхідні організаційно-технічні заходи з метою охорони та захисту персональних даних, особливо в сфері прикордонної безпеки.

Крім того, відповідно до ст. 24 Закону [6] нормативно закріплено порядок забезпечення захисту персональних даних, відповідно до якого забезпечення захисту персональних даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних покладається на володільців, розпорядників персональних даних.

Варто зазначити, що згідно положень ст. 24 Закону [6], в органах державної влади, органах місцевого самоврядування, а також у володільців чи розпорядників персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, з урахуванням принципів конфіденційності, цілісності, доступності та безпеки.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

Структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, відповідно до ст. 24 Закону [6]:

1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

2) взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

Разом з тим, структурний підрозділ також контролює дотримання вимог щодо безпеки персональних даних, забезпечує створення та підтримання системи захисту інформації відповідно до чинного законодавства, а також здійснює моніторинг за обробкою персональних даних для виявлення та запобігання потенційним загрозам їх безпеці. У разі виявлення порушень, структурний підрозділ вживає заходів для їх усунення та забезпечує належне відновлення інформації у випадку її неправомірного доступу або витоку.

Слід зазначити, що відповідальність за безпосередній захист покладена на володільців та розпорядників персональних даних, адже вони зобов'язані створювати структурні підрозділи чи призначати відповідальних осіб, які організовують роботу з захисту персональних даних від випадкових втрат, незаконної обробки та інформувати, консультувати володільців чи розпорядників персональних даних, а також взаємодіяти з Уповноваженим Верховної Ради України з прав людини

Важливою юридично значущою процедурою, згідно ст. 2 Закону [6] є обробка персональних даних, а саме - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням

інформаційних (автоматизованих) систем, та надання на це згоди суб'єкта персональних даних. Таким чином обробка персональних даних є невід'ємною частиною сучасного інформаційного суспільства, а згода суб'єкта на їх обробку визначає легітимність цього процесу.

Згода має бути добровільною, усвідомленою та конкретною, із наданням повної інформації про мету й способи обробки. Недотримання цих вимог може спричинити певні юридичні та репутаційні наслідки, тому прозорість і відповідність законодавству є ключовими.

Зазначимо, що мета обробки персональних даних, відповідно до положень ст. 6 Закону [6] має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документів, які регулюють діяльність володільця персональних даних та відповідати законодавству про захист персональних даних та здійснюватися відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначенням цілі цієї обробки.

З огляду на зазначене, мета обробки персональних даних полягає в забезпеченні відповідності діяльності володільця бази персональних даних вимогам законів, інших нормативно-правових актів та установчих документів, що регулюють його діяльність. Обробка персональних даних повинна відбуватися відповідно до визначеної мети та не повинна перевищувати необхідного обсягу та змісту для виконання завдань, що виникають у зв'язку з діяльністю володільця бази. Також важливо дотримуватися принципу відповідності та уникати надмірності при обробці особистих даних [54, С. 39].

Таким чином, обробка персональних даних повинна здійснюватися виключно в межах встановленої мети, дотримуючись законодавчих вимог, принципів відповідності та мінімізації, щоб забезпечити належне функціонування діяльності володільця бази даних.

При цьому варто враховувати, що згідно ст. 6 Закону [6] обробка персональних даних здійснюється за згодою суб'єкта персональних даних, або у випадках, передбачених законами України та у встановленому порядку

законодавством, з дотриманням принципів законності, прозорості та мети обробки.

Зокрема, відповідно до положень ст. 2 Закону [6] згодою суб'єкта персональних даних є будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки. Таким чином, згода суб'єкта персональних даних є ключовим елементом у процесі обробки персональної інформації, що забезпечує дотримання прав фізичних осіб. Вона повинна бути чітко задокументованою, добровільною, і наданою для конкретної, визначеної мети обробки даних, що підкреслює важливість прозорості та дотримання правового порядку в цьому процесі.

Згідно ст. 6 Закону [6] обробка даних про фізичну особу без її згоди не допускається, а можлива лише в інтересах національної безпеки, економічного добробуту та прав людини. В цьому випадку під Законами розуміються всі інші Закони, які надають право на обробку персональних даних із зазначенням чіткого переліку таких даних.

Його зміст також передбачає здійснення обробки персональних даних без згоди суб'єкта персональних даних, якщо обробка персональних даних є необхідною для захисту його життєво важливих інтересів. У такому випадку обробляти персональні дані без згоди суб'єкта персональних даних можна до часу, коли отримання згоди стане можливим. Таким чином, це забезпечує баланс між захистом інтересів суб'єкта персональних даних та дотриманням принципів законності й етичності в обробці персональних даних.

Згідно з положенням ст. ст. 2, 6, 10, 16 Закону [6], згода суб'єкта персональних даних на обробку персональних даних повинна містити інформацію щодо:

- мети, яка визначається володільцем бази персональних даних в залежності від виду його діяльності, при здійсненні якої виникає необхідність у обробці персональних даних в базах персональних даних, конкретних цілей

обробки персональних даних, для досягнення яких володілець бази персональних даних обробляє персональні дані у цій базі;

- обсягу персональних даних, а саме чіткого переліку персональних даних фізичної особи, які можуть обробляються володільцем бази персональних даних у цій базі;

- порядку використання персональних даних, який передбачає дії володільця бази щодо обробки цих даних, в тому числі використання персональних даних працівниками володільця бази персональних даних, відповідно до їхніх професійних чи службових або трудових обов'язків, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними;

- порядку доступу до персональних даних третіх осіб, який визначає дії володільця бази персональних даних у разі отримання запиту від третьої особи щодо доступу до персональних даних, у тому числі порядок доступу суб'єкта персональних даних до відомостей щодо себе.

В такому випадку, згода суб'єкта персональних даних на їх обробку є ключовим елементом у забезпеченні прав фізичних осіб у сфері захисту персональної інформації. Вона повинна містити чітку та повну інформацію щодо мети обробки, обсягу персональних даних, порядку їх використання, поширення та доступу третіх осіб. Такий підхід дозволяє забезпечити прозорість процесів обробки персональних даних, дотримання прав суб'єктів даних і знижує ризики порушення законодавства. Зокрема, визначення конкретних дій володільця бази даних щодо захисту та передачі персональних даних сприяє формуванню довіри між сторонами та підтримці належного рівня інформаційної безпеки.

Важливою складовою процесу обробки персональних даних є їх збирання, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу та внесення їх до бази персональних даних та може здійснюватися лише з дозволу особи, дані про яку обробляються. Цій особі надано право знати місце роботи та проживання розпорядника бази персональних даних (відповідно за обробку

даних), а також право отримувати відповідні дані без затримки та у зрозумілій формі. У випадку відмови зацікавлена особа може звернутися до суб'єкту нагляду за дотриманням законодавства у державі, який повинен забезпечити припинення порушень положень, що зазначені у національному законодавстві.

Крім того, згідно ст. 12 Закону [6] володілець бази персональних даних протягом десяти робочих днів з дня включення персональних даних до бази персональних даних, що є дією зі збирання персональних даних, зобов'язаний повідомити суб'єкта персональних даних, виключно в письмовій формі, про його права, що визначені статтею 8 Закону, мету збору даних, яка визначається володільцем бази персональних даних та осіб, яким будуть передаватися персональні дані.

Таким чином, встановлюються чіткі терміни та вимоги для володільців баз персональних даних щодо повідомлення суб'єктів щодо їхніх прав, мети обробки та осіб, яким передаються дані. Необхідно враховувати, що такий підхід сприяє підвищенню прозорості та захисту прав громадян. Додержання встановлених термінів і процедур є не лише обов'язковим, а й сприяє підтриманню довіри до систем обробки персональних даних, адже це є важливим забезпеченням інформаційної безпеки, як аспекту національної безпеки в цілому.

Разом із тим, здійснення необхідного контролю за додержанням законодавства про захист персональних даних покладено, відповідно ст. 22 Закону [6] на Уповноваженого та суди, які в межах своїх повноважень розглядають спори, пов'язані з порушенням цього законодавства, забезпечуючи захист прав і законних інтересів осіб.

Водночас, Уповноважений має такі повноваження у сфері захисту персональних даних, відповідно до положень ст. 23 Закону [6]:

- отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

- проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників

персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

- отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

- затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом;

- за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

- надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

- взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб;

- звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

- надавати за зверненням професійних, самоврядних та інших громадських об’єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;

- складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом.

Таким чином, Уповноважений з питань захисту персональних даних має широкий спектр повноважень, спрямованих на забезпечення належного рівня захисту персональних даних. Ці повноваження охоплюють прийняття та розгляд звернень, проведення перевірок, доступ до інформації, підготовку нормативно-правових актів, надання рекомендацій, взаємодію з іншими органами та інститутами, а також контроль за дотриманням законодавства у цій сфері. Така діяльність сприяє запобіганню порушенням прав суб’єктів персональних даних та ефективному реагуванню на випадки їх недотримання.

Судовий контроль у сфері захисту персональних даних проявляється у компетенції судів розглядати матеріали справ про порушення законодавства у сфері захисту персональних даних, направлених до суду посадовими особами Секретаріату Уповноваженого, відповідно до ст. 221 Кодексу України про адміністративні правопорушення (надалі – КУпАП) [7], а також виносити ухвали щодо усунення підстав порушення законодавства у сфері захисту персональних даних.

Також вважаємо за доцільне звернути увагу не тільки на законодавчі визначення терміну «персональні дані», але й на судову практику.

Зокрема, у Рішенні [56] від 20.01.2012р. № 2-рп/2012 Конституційний Суд України (надалі – КСУ) зазначив: «інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов’язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною: збирання, зберігання, використання та

поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання допускається винятково у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Таким чином, КСУ розглядає інформацію про особисте та сімейне життя особи як поняття «інформація про особу», і саме інформацію про особисте та сімейне життя називає «конфіденційною інформацією про особу». Це означає, що така інформація підлягає захисту та повинна мати обмежений доступ для сторонніх осіб, крім випадків, коли це дозволяється законом або за наявності належного дозволу суб'єкта інформації.

У мотивувальній частині цього ж рішення суд зазначив: «інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини тієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану із здійсненням функцій держави або органів місцевого самоврядування».

Тобто, фактично суд ототожнив поняття «інформація про особисте і сімейне життя» та «персональні дані», а це означає, що будь-які відомості, які стосуються фізичної особи, незалежно від того чи йдеться лише про її приватну або сімейну сферу, охоплюються категорією персональних даних.

Таким чином, персональні дані – це усі відомості про фізичну особу (якщо вона є ідентифікованою або може бути конкретно ідентифікованою), а не лише відомості про особисте й сімейне життя [57, С. 26]. До таких відомостей

належать: ім’я, прізвище, дата народження, контактні дані, паспортна інформація, ідентифікаційний номер, фінансова інформація, дані про місцезнаходження, онлайн-ідентифікатори (наприклад, IP-адреса) тощо.

Підсумовуючи, варто зауважити, що законодавство України у сфері захисту персональних даних базується на міжнародних правових актах, метою якого є захист основних прав і свобод, а особливо права на невтручання в особисте життя та визначає сучасні стандарти захисту інформації.

1.3. Правовий статус Державної прикордонної служби України як суб’єкта забезпечення прикордонної безпеки України

Сучасні умови геополітичної нестабільності в Україні вказують на те, що в умовах збройної агресії, стабільний розвиток нашої держави тісно пов’язаний із безпекою її кордону. Практика показує, що багато загроз національним інтересам України формується за межами прикордонних територій. Саме тому розбудова і розвиток України як правової держави невід’ємно пов’язана з належною організацією і функціонуванням системи інституцій, покликаних забезпечити правопорядок в усіх сферах життєдіяльності, включаючи сферу захисту державного кордону. Ефективна діяльність цих державних органів є необхідною умовою захисту конституційного ладу, дотримання прав і свобод людини, а також забезпечення законності та правопорядку [58, С. 146].

Як зазначає І. П. Кушнір, питання безпеки нині гостро стоїть не тільки перед Українським народом, але й перед усією міжнародною спільнотою. Стурбованість посилюється здійсненням методами та способами сучасного гібридного протистояння і ведення інформаційної війни, що використовуються владою окремих країн, організацій, як засіб для втручання та дестабілізації внутрішньополітичної ситуації інших країн. Наприклад, використання будь-якої інформації у своїх цілях завдяки її спотворенню, інформаційної маніпуляції нині є яскравим прикладом міжнародної політики кремлівської влади.

Але існують й інші, як гібридні, так і інформаційні загрози, які загалом викликають необхідність посилення забезпечення безпеки державного кордону,

утримання та відновлення контролю над державним кордоном на його південно-східних ділянках, усебічного розвитку та захисту інформаційного середовища Державної прикордонної служби України, які є складниками забезпечення ефективної реалізації державної політики у сфері безпеки державного кордону України [59, С. 81].

Важливе місце у процесі забезпечення національної безпеки належить спеціально створеним державним органам, які у своїй сукупності та за функціональним призначенням складають систему органів сектору безпеки і оборони, однією із складових якого є Державна прикордонна служба України (надалі – ДПСУ) [60], на яку покладаються завдання щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні [59].

ДПСУ є важливою складовою системи національної безпеки, забезпечуючи охорону державного кордону та захист суверенних прав України, адже її діяльність спрямована на підтримання стабільності, правопорядку та протидію зовнішнім загрозам на державному кордоні України.

Як зазначалося, охорона та захист державного кордону України, відповідно ст. 1 Закону України «Про Державну прикордонну службу України» [61] покладається на ДПСУ, яка згідно положень ст. 18 Закону [62] є правоохоронним органом спеціального призначення, що реалізує державну політику у сфері охорони державного кордону України.

Водночас ДПСУ має статус військового формування, оскільки їй притаманні такі основні ознаки військового формування, як: функціонування в ДПСУ такого специфічного інституту, як військова служба; наявність відповідних принципів функціонування згаданого інституту; наявність характерних вимог до кандидатів для вступу на військову службу; правове регулювання започаткування військово-службових відносин, проходження військової служби та її припинення; встановлення для військовослужбовців прав, обов'язків, відповідальності, обмежень і заборон; виконання завдань щодо

військового захисту територіальної цілісності держави, участь у територіальній обороні тощо [63, С. 227].

Як військове формування ДПСУ здійснює охорону, включаючи захист, державного кордону України, таким чином беручи участь у забезпеченні територіальної цілісності України та територіальній обороні.

Підтвердженням статусу правоохоронного органу спеціального призначення є те, що ДПСУ здійснює організацію запобігання злочинам та адміністративним правопорушенням, протидія яким законодавством віднесена до її компетенції, їх виявлення, припинення, проведення дізнання, здійснення провадження у справах про адміністративні правопорушення згідно із законом.

Як правоохоронний орган спеціального призначення ДПСУ запобігає правопорушенням та злочинам на державному кордоні та у виключній (морській) економічній зоні України, застосовуючи превентивні та юрисдикційні заходи адміністративного характеру. Для виконання зазначених завдань ДПСУ наділена повноваженнями провадити оперативно-розшукову, розвідувальну, інформаційно-аналітичну діяльність та здійснювати окремі заходи контррозвідувального характеру [63, С. 228].

Варто відзначити, що сьогодні основні завдання ДПСУ можна умовно поділити на: охоронні, контролюючі; щодо взаємодії; превентивні та інформаційні [64, С. 155]. Окремо слід виділити ті повноваження ДПСУ, які безпосередньо спрямовані на забезпечення прикордонної безпеки держави, як ключового елементу забезпечення національної безпеки [64, С. 155]. Серед них, відповідно до ст. 19 Закону [61] є наступні:

- припинення будь-яких спроб незаконної зміни проходження лінії державного кордону України;

- припинення у взаємодії з відповідними правоохоронними органами збройних конфліктів та інших провокацій на державному кордоні України;

- здійснення прикордонного контролю і пропуску в установленому порядку осіб, транспортних засобів, вантажів в разі наявності належно

оформлених документів після проходження ними митного та інших видів контролю;

- контроль за дотриманням прикордонного режиму; встановлення режимних правил у контрольних пунктах в'їзду – виїзду;

- участь у взаємодії із Збройними Силами України та іншими військовими формуваннями у відбитті вторгнення або нападу на територію України збройних сил іншої держави або групи держав тощо.

Крім того, за ДПСУ закріплюється широкий перелік повноважень, які дозволяють ефективно здійснювати охорону та оборону державного кордону України, запобігати правопорушенням у прикордонній сфері та загалом сприяти зміцненню національної безпеки України.

Як стверджує В. С. Нікіфоренко, забезпечення національної безпеки є одним із пріоритетних напрямів державної політики будь-якої країни світу. Важливим це питання є і для України, адже у сьогоднішніх умовах наша держава зіткнулася з реальною загрозою її національній безпеці – зазіханням на суверенітет і територіальну цілісність. Це питання, безумовно, перетинається із забезпеченням безпеки державного кордону України [65, С. 328].

Відповідно до положень ст. 20 Закону [61], де безпосередньо визначено, що ДПСУ з метою забезпечення безпеки кордону України має право:

- здійснювати контрольований (під оперативним контролем) пропуск через державний кордон України осіб у пунктах пропуску або поза ними;

- перевіряти в осіб, які прямують через державний кордон України, документи на право в'їзду в Україну або виїзду з України;

- здійснювати адміністративне затримання осіб, які незаконно перетнули державний кордон України;

- здійснювати особистий огляд затриманих, а також проводити в установленому порядку огляд українських та іноземних невійськових суден, що допустили порушення законодавства під час плавання і перебування в територіальному морі, внутрішніх водах, а також під час стоянки суден у портах України;

- також здійснювати розвідувальні, контррозвідувальні та оперативно розшукові заходи згідно із законами України.

Варто зазначити, що через широкомасштабну військову агресію РФ проти України докорінно змінилася безпекова ситуація на державному кордоні України, спричинивши таким чином різке зростання терористичної та розвідувально-диверсійної діяльності сепаратистських угруповань, а тому виникла необхідність у реформуванні ДПСУ – перегляді повноважень та розширення її оперативних можливостей.

Метою реформування ДПСУ є створення прикордонного відомства європейського типу, яке гарантовано забезпечуватиме захист національних інтересів на державному кордоні України, що визначено в Концепції розвитку [66]. В основу створення сучасної інтегрованої системи охорони державного кордону України та її виключної (морської) економічної зони покладено введення в оперативно-службову діяльність принципово нових підрозділів [67], таких як відділ прикордонної служби (надалі – ВПС), що є одним із пріоритетних напрямів у досягненні даної мети.

Варто відзначити, що національна безпека є надбанням лише сильної державної організації суспільства, а тому забезпечення прикордонної безпеки, як аспекту національної, безпосередньо реалізується у діяльності підрозділів охорони кордону [68, С. 18].

Відповідно до ст. 6 Закону [61] ДПСУ має таку загальну структуру:

- центральний орган виконавчої влади, що реалізує державну політику у сфері охорони державного кордону;

- територіальні органи центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону;

- морська охорона, яка складається із загонів морської охорони;

- органи охорони державного кордону – прикордонні загони, окремі контрольно-пропускні пункти, авіаційні частини;

- розвідувальний орган центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону.

Центральний орган виконавчої влади, Адміністрація ДПСУ (надалі – АДПСУ), що реалізує державну політику у сфері охорони державного кордону, здійснює управління ДПСУ, бере участь у розробленні та реалізації загальних принципів правового оформлення і забезпечення недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні.

З метою ефективного виконання покладених на ДПСУ завдань центральним органом виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, утворюються територіальні органи – регіональні управління.

Морська охорона, яка складається із загонів морської охорони здійснює охорону державного кордону на морі, річках, озерах та інших водоймах, а також контроль за плаванням і перебуванням українських та іноземних невійськових суден і військових кораблів у прилеглій зоні, територіальному морі та внутрішніх водах.

Органи охорони державного кордону, які безпосередньо виконують поставлені перед ДПСУ завдання щодо забезпечення недоторканності державного кордону України та до яких належать прикордонні загони, загони морської охорони, загони оперативного реагування, окремі контрольно-пропускні пункти, авіаційні частини та інші оперативно-службові підрозділи ДПСУ здійснюють охорону державного кордону, а також виконують завдання з оперативно-розшукової діяльності, протидії незаконній міграції, боротьби з контрабандою та іншими правопорушеннями у межах прикордонної смуги та контрольованих прикордонних районів

Прикордонний загін є основною оперативно-службовою ланкою ДПСУ, на яку покладаються охорона певної ділянки державного кордону самостійно чи у взаємодії з іншими органами охорони державного кордону та Морською охороною, забезпечення дотримання режиму державного кордону і прикордонного режиму, здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України та до тимчасово

окупованої території і з неї осіб, транспортних засобів, вантажів, охорона та захист пунктів пропуску через державний кордон України, припинення у взаємодії з відповідними військовими частинами та підрозділами Збройних Сил України (надалі – ЗСУ), інших утворених відповідно до законів України військових формувань, відповідними правоохоронними органами збройних та інших провокацій на державному кордоні України. Під час дії воєнного стану прикордонні загони у встановленому законом порядку можуть залучатися відповідними органами військового управління ЗСУ до ліквідації (нейтралізації) збройного конфлікту на державному кордоні України, міжнародного збройного конфлікту, відсічі збройній агресії проти України.

До складу прикордонного загону можуть входити прикордонні комендатури, відділи прикордонної служби, прикордонні застави, контрольно-пропускні пункти, відділення прикордонного контролю, відділення інспекторів прикордонної служби та інші підрозділи.

Відділ прикордонної служби (надалі – ВПС) – це підрозділ ДПСУ, призначений для безпосередньої охорони визначеної ділянки державного кордону України, здійснення прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів та вантажів, оперативно-розшукової діяльності, запобігання злочинам та адміністративним правопорушенням, протидію яким законодавством віднесено до компетенції ДПСУ. Це вказує на наявність кількох структурних елементів, ієрархічно пов’язаних між собою через розподіл функцій, повноважень і відповідальності.

Управління ВПС полягає у цілеспрямованій діяльності керівництва відділу щодо підтримання високої готовності структурних підрозділів до дій, їх підготовки та керування під час виконання покладених завдань, а діяльність ВПС спрямована на забезпечення недоторканності державного кордону України та здійснюється на території України у прикордонній смузі та контрольованих прикордонних районах та здійснюється, відповідно, змінами прикордонних нарядів, які забезпечують безпеку державного кордону України [61].

Діяльність ВПС визначається характером функцій, які реалізуються в процесі охорони визначеної ділянки державного кордону України. Варто зазначити, що функції ДПСУ рівнозначні, взаємопов'язані та взаємообумовлені, адже в сукупності вони становлять узагальнювальну характеристику призначення й спрямованості дій всіх їх структурних елементів, націлених на досягнення об'єктивно обумовлених мети і завдань у сфері прикордонної безпеки [69, С. 23], як аспекту національної безпеки в цілому.

Відповідно до ст. 5 Інструкції [71] ВПС є основними підрозділами органів охорони державного кордону, які призначені для безпосереднього виконання їх функцій з охорони визначеної ділянки державного кордону України, здійснення прикордонного контролю і пропуску через державний кордон України.

Основними функціями ВПС є:

- охорона державного кордону України на суші, морі, річках, озерах та інших водоймах з метою недопущення незаконної зміни проходження його лінії, забезпечення дотримання режиму державного кордону та прикордонного режиму;

- здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів та іншого майна, а також виявлення і припинення випадків незаконного їх переміщення;

- ведення оперативно-розшукової роботи в інтересах забезпечення захисту державного кордону України згідно із законодавством України та нормативно-правовими актами АДПСУ;

- участь у боротьбі з організованою злочинністю та протидія незаконній міграції на державному кордоні України та в межах контрольованих прикордонних районів;

- координація діяльності підрозділів військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України або беруть участь у забезпеченні

режиму державного кордону, прикордонного режиму і режиму в пунктах пропуску через державний кордон України.

Таким чином основні функції ВПС спрямовані на забезпечення охорони та захисту державного кордону України. Вони охоплюють контроль за перетином кордону, запобігання незаконним переміщенням осіб і вантажів, боротьбу з організованою злочинністю та незаконною міграцією. Крім того, ВПС виконує оперативно-розшукову діяльність і координує дії військових та правоохоронних органів для ефективного забезпечення безпеки державного кордону. Ці заходи є ключовими для збереження суверенітету та територіальної цілісності України.

Окремий контрольно-пропускний пункт (надалі – ОКПП) є оперативно-службовою ланкою ДПСУ, на яку покладається здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів.

До складу ОКПП можуть входити інші підпорядковані йому контрольно-пропускні пункти, відділи прикордонної служби, відділення прикордонного контролю і контролерські пости.

Авіаційна частина є оперативно-службовою ланкою ДПСУ, на яку покладаються охорона державного кордону у взаємодії з іншими органами охорони державного кордону і Морської охорони, забезпечення дотримання режиму державного кордону і прикордонного режиму, а також здійснення охорони суверенних прав України в її виключній (морській) економічній зоні. До складу авіаційної частини входять авіаційні ланки [61].

Розвідувальний орган центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, організовує свою діяльність відповідно до Закону України «Про розвідку» [71].

У складі центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, територіальних органів центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, органів охорони державного кордону функціонують підрозділи спеціального призначення, а саме: оперативного

документування, оперативно-технічні, забезпечення внутрішньої та власної безпеки.

Органами забезпечення ДПСУ є підприємства, установи, а також підрозділи технічного, матеріального, медичного та інших видів забезпечення її діяльності, які функціонують як самостійно, так і в складі відповідно центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, його територіальних органів, Морської охорони, інших органів охорони державного кордону, навчальних закладів ДПСУ.

У складі підрозділів органів забезпечення функціонує Головний центр обробки спеціальної інформації (надалі – ГЦОСІ), основним завданням якого є обробка інформації, у тому числі персональних даних, з використанням інформаційно-комунікаційних систем (надалі – ІКС) «ГАРТ» та «Аркан», а також баз даних ДПСУ [72]. Для належної організації роботи цих систем було прийнято низку нормативних актів, серед яких головне значення має наказ АДПСУ № 472, яким було затверджено Положення про базу даних «Відомості про осіб, які перетнули державний кордон України» [73]. Цей нормативний акт визначав порядок функціонування інтегрованої інформаційно-телекомунікаційної системи «ГАРТ», яка забезпечувала централізований облік даних про перетин державного кордону.

У подальшому його положення були оновлені наказом Міністерства внутрішніх справ України № 614, яким було затверджено нову редакцію Положення про базу даних «Відомості про осіб, які перетнули державний кордон України, в'їхали на тимчасово окуповану територію України або виїхали з такої території» [74].

На нашу думку, такі нормативні зміни відображають стратегічну спрямованість державної політики на посилення інформаційної безпеки та захисту персональних даних у сфері прикордонного контролю, що безпосередньо пов'язано із забезпеченням прикордонної безпеки, як аспекту національної безпеки загалом та територіальної цілісності України.

Серед напрямів здійснення державної національної безпекової політики, пріоритетними є забезпечення державної та інформаційної безпеки, а також територіальної цілісності, що є складником національної і державної безпеки України, які тісно пов'язані із принципом непорушності та безпеки державних кордонів України [59, С. 81], що гарантується відповідно до норм міжнародного права, Конституції України та інших законодавчих актів, спрямованих на збереження суверенітету, стабільності та правопорядку в державі.

Однією з ключових функцій ДПСУ є охорона персональних даних, які обробляються під час виконання завдань, пов'язаних із здійсненням прикордонного контролю та охороною державного кордону України.

Сучасність – це світ інформаційних технологій, в якому швидкість та якість прийняття управлінських рішень прямо пропорційні швидкості та якості функціонування систем електронних комунікацій. Не осторонь цього дійства стоять суб'єкти інтегрованого управління кордонами [75, С. 65], до складу яких, відповідно до Стратегії інтегрованого управління кордонами (надалі – Стратегія) [76], належить ДПСУ, адже від ефективності управління державним кордоном України залежить безпека держави, розвиток її економіки та людський потенціал.

Оскільки ДПСУ виконує важливу роль у забезпеченні безпеки державного кордону України та захисту прав громадян, то ефективне управління кордонами не можливе без функціонування ІКС відомства. Адже у процесі охорони та захисту державного кордону ДПСУ збирає та обробляє персональні дані у різних сферах своєї діяльності.

Основою ІКС ДПСУ є Інтегрована інформаційно-комунікаційна система «ГАРТ» (ІІКС «ГАРТ»), яка призначена для створення єдиного інформаційного простору та електронної системи управління Держприкордонслужби, виконання завдань з підвищення ефективності управління органами ДПСУ під час охорони державного кордону України.

Зазначимо, що діяльність ІІКС «ГАРТ» регламентується законами [77,78,79] та складається з ряду інформаційно-комунікаційних систем (ІКС), а

саме: «Гарт-1» – прикордонний контроль, «Гарт-2» – інформаційно-телекомунікаційні системи оперативно-чергової служби, «Гарт-3» – прикордонна служба, «Гарт-4» – тилове забезпечення, «Гарт-5» – інформаційно-аналітична служба, «Гарт-6» – фінансове забезпечення, «Гарт-7» – кадрове забезпечення, «Гарт-8» – професійна підготовка, «Гарт-9» – санітарно-епідеміологічне забезпечення, «Гарт-10» – оперативно-розшукова діяльність, «Гарт-11» – виховна робота, «Гарт-12» – морська охорона, «Гарт-13» – правове забезпечення, «Гарт-14» – спостереження, «Гарт-15» – інформаційно-телекомунікаційні системи радіаційного, хімічного, біологічного захисту та екологічної безпеки, «Гарт-16» – авіаційна служба, «Гарт-17» – геоінформаційна система, «Гарт-18» – документальне забезпечення, «Гарт-19» – електронна пошта, «Гарт-20» – факсимільне повідомлення, «Гарт-21» – внутрішня безпека.

Варто зазначити, що забезпечення функціонування, а також захист інформації та технічне забезпечення ІІКС «ГАРТ» здійснюється Головним центром зв'язку [74], а обробка інформації про перетинання особами і транспортними засобами державного кордону України здійснюється ГЦОСІ [72].

Важливим аспектом діяльності ДПСУ є здійснення контролю за перетином державного кордону: реєстрація осіб, транспортних засобів та вантажів, тобто здійснення прикордонного контролю, який, відповідно до ст. 2 Закону [3], визначається як державний контроль, що здійснюється ДПСУ, який включає комплекс дій і систему заходів, спрямованих на встановлення законних підстав для перетинання державного кордону особами, транспортними засобами і переміщення через нього вантажів.

Також важливу роль у забезпеченні безпеки державного кордону України відіграють контррозвідувальні та розвідувальні заходи, які сприяють виявленню та нейтралізації потенційних загроз. Застосування технологій та аналітичних методів дозволяє підвищити ефективність охорони кордону та оперативно реагувати на виклики.

Метою контррозвідувальної діяльності, є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України,

припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють та причин їх виникнення.

Завданням контррозвідувальної діяльності є: добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян.

Варто зазначити, підрозділи управління внутрішньої та власної безпеки (надалі – УВВБ) ДПСУ [80, С. 69–70] мають право на здійснення окремих контррозвідувальних заходів з іншими суб'єктами контррозвідувальної діяльності. Також важливими заходами забезпечення прикордонної безпеки підрозділами УВВБ, є здійснення ними розвідувальної діяльності, боротьба з тероризмом та боротьба з організованою злочинністю.

Важливим аспектом забезпечення прикордонної безпеки є належне регулювання обігу конфіденційної, публічної та службової інформації, яка використовується в процесі здійснення прикордонного контролю, контррозвідувальної та розвідувальної діяльності, адже ДПСУ займає важливе місце у системі забезпечення національної безпеки України.

Дослідник А. І. Марущак зазначає, що відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України та які визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей – це інформація з обмеженим доступом [81, С. 23], яка обробляється в інформаційно-комунікаційній системі «Аркан», з метою забезпечення прикордонної безпеки.

Публічною інформацією в діяльності ДПСУ є інформація, яка регулюється Законом [6] щодо:

- фактів перетину державного кордону України громадянами;

- можливого існування стосовно громадянина тимчасового обмеження у праві виїзду за кордон;

- можливого існування стосовно іноземця та особи без громадянства рішення про заборону в'їзду.

Окрім публічної інформації, у сфері управління та діяльності державних органів, зокрема в діяльності ДПСУ, яка регулюється Законом [6] широко використовується службова інформація, яка, хоча і не належить до категорії державної таємниці, підлягає обмеженню в доступі відповідно до законодавства.

За сучасних умов військової агресії Російської Федерації проти України важливим складником забезпечення національної безпеки є безпека державного кордону, яка спрямована на ефективну реалізацію політики безпеки у сфері захисту й охорони державного кордону України, а також охорони суверенних прав України в її виключній (морській) економічній зоні [82, С. 36], яку прийнято вважати прикордонною безпекою України [83, С. 40].

Сутність поняття прикордонна безпека найбільш концептуально розкрито М. М. Литвином, який визначає її як: захищеність життєво важливих інтересів особи, суспільства і держави в її прикордонному просторі, при якому суспільству, державі і особі не завдається шкода, а навпаки, створюються умови для реалізації їх інтересів, пов'язаних із свободою пересування через державний кордон, оперативно виявляються та припиняються правопорушення, здійснюється протидія загрозам національній безпеці на кордоні та планомірна діяльність з усунення причин їх виникнення [84. С. 19-21].

М. М. Литвин зазначає, що процес формування та реалізації державної політики України у прикордонній сфері умовно поділяється на чотири етапи (критерієм класифікації є прийняття і запровадження відповідних нормативно-правових актів та концепцій): 1991 – 1993 роки; 1994 – 1999 роки; 2000 – 2005 роки; 2006 рік – по теперішній час.

На його думку, слід виокремлювати чотири рівні забезпечення прикордонної безпеки.

- перший рівень – рівень забезпечення співробітництва з державами, що не мають спільного кордону з Україною.

- другий – забезпечення співробітництва з державами, що межують з Україною.

- третій – рівень проведення внутрішньодержавних процедур.

- четвертий – рівень забезпечення співробітництва щодо охорони кордону, дотримання режиму кордону та прикордонного режиму.

У свою чергу О. Г. Мельников визначає прикордонну безпеку як сукупність політичних, економічних, військових та правоохоронних заходів, спрямованих на забезпечення суверенітету, недоторканості і територіальної цілісності держави, які реалізуються шляхом здійснення прикордонної політики держави. Заходи з реалізації прикордонної безпеки зумовлюються пріоритетністю національних інтересів, всебічним аналізом глобальних викликів та загроз у прикордонній сфері та необхідністю вжиття своєчасних адекватних заходів з їх мінімізації. Прикордонна безпека є невід'ємною складовою національної безпеки щодо захисту і забезпечення своїх національних інтересів і національної безпеки у сфері захисту і охорони державного кордону. Головними об'єктами прикордонної безпеки є права й свободи людини, духовні і матеріальні цінності суспільства, конституційний лад, суверенітет, територіальні цілісність, економічні, політичні та військові інтереси держави. Головними суб'єктами прикордонної безпеки є органи державної влади, органи місцевого самоврядування, громадські організації і громадяни України [85, С. 46–51].

Ю. Б. Курилюк зазначає, що прикордонна безпека – це збалансований стан захищеності суспільних відносин у прикордонній сфері від зовнішніх і внутрішніх загроз охоронюваним законодавством про державний кордон інтересам людини, суспільства й держави [86, С. 50], який забезпечується системою правових, організаційних та технічних заходів.

І. П. Кушнір визначає прикордонну безпеку, як сформований у нормативно-правових актах і забезпечений діяльністю ДПСУ стан безпеки державного кордону й усіх її складників (у тому числі інформаційного), забезпечення реалізації прав і законних інтересів суб'єктів у прикордонній сфері [87, С. 123], який досягається шляхом комплексного застосування сил, засобів і методів прикордонного контролю та охорони.

Дослідження науковців у сфері прикордонної безпеки дозволяють зробити важливий висновок: прикордонна безпека є комплексним явищем, що охоплює широкий спектр заходів та механізмів, спрямованих на захист життєво важливих інтересів особи, суспільства та держави в прикордонному просторі. Вона гарантує суверенітет, територіальну цілісність держави та сприяє реалізації національних інтересів.

Важливо підкреслити, що ключовим аспектом прикордонної безпеки є захист персональних даних як осіб, що перетинають кордон, так і військовослужбовців ДПСУ. Оскільки персональні дані становлять чутливу інформацію, їхня безпека є критичною для національної безпеки та прав людини. Несанкціонований доступ, витік або зловживання такими даними можуть мати серйозні наслідки, зокрема загрожувати життю та діяльності як цивільних осіб, так і військовослужбовців.

Основними об'єктами прикордонної безпеки залишаються права та свободи громадян, конституційний лад, суверенітет і територіальна цілісність, а її суб'єктами – державні органи, місцеве самоврядування та громадськість. Отже, ефективне забезпечення прикордонної безпеки потребує комплексного підходу, зокрема посилення нормативно-правового регулювання у сфері захисту персональних даних, удосконалення механізмів їхньої обробки та координації дій між усіма зацікавленими сторонами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 1:

1. Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році. URL: https://ombudsman.gov.ua/report-2023/images/documents/annual-report-2023.pdf (дата звернення: 24.07.2023).

2. Конституція України: Закон України від 28 червня 1996 року №254к/96-ВР. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 24.07.2023).

3. Про прикордонний контроль: Закон України від 05 листопада 2009 року № 1710-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1710-17#Text (дата звернення: 25.07.2023).

4. Законодавство України: Термінологія законодавства. Термін «персональні дані». *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/term/20618:116444 (дата звернення: 25.07.2023).

5. Дяковський О. С. Визначення поняття персональних даних як правової категорії: сучасні проблеми та шляхи вирішення. *Інформація і право*. 2017. № 3 (22). С. 51–56. URL: https://doi.org/10.37750/2616-6798.2017.3(22).273049

6. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 24.07.2023).

7. Кодекс України про адміністративні правопорушення: Закон України від 07 грудня 1984 року № 8073-X. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 26.07.2023).

8. Уповноважений закликає володільців персональних даних забезпечити захист персональних даних від незаконного поширення. URL: https://lnk.ua/No9GVg6PZ (дата звернення: 27.07.2023).

9. Миронюк О. Охорона персональних даних як необхідність сучасного українського суспільства. URL: https://law.chnu.edu.ua/okhorona-personalnykh-danykh-yak-neobkhidnist-suchasnoho-suspilstva/ (дата звернення: 29.07.2023).

10. В офісі Омбудсмана розповіли про захист персональних даних для близько пів тисячі працівників МВС та його підрозділів. URL: https://lnk.ua/I71UgPeTs (дата звернення: 29.07.2023).

11. Брижко В. М. Організаційно-правові питання захисту персональних даних: автореф. дис. … канд. юрид. наук: 12.00.07. Київ, 2004. 23 С.

12. Чернобай А. М. Правові засоби захисту персональних даних працівника: дис. … канд. юрид. наук: 12.00.05. Одеса, 2006. 200 С.

13. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: дата набрання чинності для України – 01 січня 2011 року. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 01.08.2023).

14. Сокол М. В., Тимощук А. В. Поняття персональних даних працівника та їх відмежування від іншої інформації. *Право та державне управління*. 2020. № 2. С. 48–54. URL: DOI: https://doi.org/10.32840/pdu.2020.2.7

15. Гусаров С. М., Мельник К. Ю. Захист персональних даних працівника. *Право і безпека*. 2023. № 52. С. 133–144. URL: DOI: https://doi.org/10.32631/pb.2023.2.12

16. Чанишев Р. І. Інформація про персональні дані працівника та її захист. *Актуальні проблеми держави і права.* 2010. № 52. С. 94–99.

17. Буртник Х. Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання. URL: https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/ (дата звернення: 01.08.2023).

18. Тунік А. В. Правові основи захисту персональних даних: дис. … канд. юрид. наук: 12.00.07. Київ, 2012. 213 С.

19. Цвірюк Д. В. Адміністративно-правовий захист персональних даних в Україні: автореф. дис. … канд. юрид. наук: 12.00.07. Київ, 2014. 18 С.

20. Різак М. В. Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні: автореф. дис. док-ра юрид. наук: 12.00.07. Харків, 2018. 36 С.

21. Саєнко М. І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні. *Право і суспільство*. 2015. № 3. С. 102–107.

22. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні: навчальний посібник. Київ: Юстініан, 2006. 176 С.

23. Брижко В. М. Модальність правової визначеності у сфері захисту та безпеки приватності персональних даних. *Інформація і право*. 2021. № 4 (39). С. 52–69. URL: https://doi.org/10.37750/2616-6798.2021.4(39).248790

24. Великий тлумачний словник сучасної української мови: 250000 / уклад. та голов. ред. В. Т. Бусел. Київ; Ірпінь: Перун, 2005. 1728 С.

25. Корж А. В., Фонтош Н. М. Проблеми вдосконалення юридичної термінології в українському законодавстві. *Держава і право*. 2009. № 46. С. 610–616.

26. Великий тлумачний словник сучасної української мови: словник / за ред. В. М. Білоножко та ін. Дніпро, ін-т укр. Мови НАН України, Ін-т мовознав. НАН України, Всеукр. Т-во «Просвіта» ім. Тараса Шевченка: 2009. 1332 С.

27. Юридична енциклопедія: в 6 т. / за ред. Ю. С. Шемшученка. Київ: Укр. енциклопедія, 1998. Т.2: Д-Й. 744 С.

28. Попелюшко В. О. Функція захисту в кримінальному судочинстві України: правові, теоретичні та прикладні проблеми: дис. … док-ра юрид. наук: 12.00.09. Київ, 2009. 502 С.

29. Галунько В. В. Адміністративне право України: навчальний посібник / у 2-х томах / В. В. Галунько, В. І. Олефір, М. П. Пихтін та ін.; за заг. ред. В. В. Галунька. Херсон, 2011. Т.1: Загальне адміністративне право. 320 С.

30. Гіда Є. О. Права людини (охорона і захист) / Є. О. Гіда // Міжнародна поліцейська енциклопедія: у 10 т. Київ: «Ін Юре», 2005. Т. 2: Права людини у контексті поліцейської діяльності. 759 С.

31. Обущак О. О., Обущак С. А. Адміністративне регулювання у сфері охорони прав на об’єкти інтелектуальної власності. *Гуманітарний вісник Запорізької державної інженерної академії*. 2009. № 36 (3). С. 75–86.

32. Назаров В. В. Особливості механізму захисту прав людини у кримінальному провадженні. *Форум права*. 2009. № 1. С. 385–391.

33. Ромовська З. В. Особисті немайнові права фізичних осіб. *Українське право*. 1997. № 1 (6). С. 11–13.

34. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. *Юридичний вісник*. 2014. № 4 (33). С. 70–75.

35. Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція.* 2021. № 2 (31). С. 74–79. URL: https://doi.org/10.32836/2521-6473.2021-2.15

36. Стефанчук Р. О. До питання забезпечення цивільно-правової охорони приватного життя фізичної особи: досвід України та Німеччини. *Університетські наукові записки.* 2005. № 4 (16). С. 68–72.

37. Врублевська-Місюна К. М., Тичина В. П. Міжнародно-правові стандарти захисту інформації про особу. *Науковий вісник Ужгородського Національного Університету.* 2022. № 74/2. С. 149–154. URL: DOI https://doi.org/10.24144/2307-3322.2022.74.58

38. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 21.05.2024).

39. Директива 2002/58/ЄС Європейського Парламенту і Ради «Щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації)» від 12 липня 2002 року. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058 (дата звернення: 21.05.2024).

40. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС» від 27 квітня 2016 року. *Офіційний сайт Верховної Ради України*. URL:

https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 22.05.2024).

41. Бем М. В., Городинський І. М. Стандарти захисту персональних даних в соціальній сфері: посібник. Львів, 2018. 110 С.

42. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-XI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 01.06.2024).

43. Про інформацію: Закон України від 02 жовтня 1992 року № 2657-XII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 02.06.2024).

44. Брижко В. М., Радянська А. І., Швець М. Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ: Тріумф, 2006. 256 С.

45. Брижко В. М., Фурашев В. М. Інформаційне право та інформаційне законодавство. Харків: Право, 2021. 288 С.

46. Корнєєва Т. Права людини і інформаційному суспільстві. Комунікаційні права: четверте покоління прав людини: тлумачний словник української мови / за ред. проф. Калачника В. С. Харків: Прапор, 2002. 992 С.

47. Теорія держави і права: підручник / за ред. Лисенков С. Л. Київ: Юрінком Інтер, 2005. 448 С.

48. Юридична енциклопедія: в 6 т. / за ред. Ю. С. Шемшученка. Київ: Укр. Енциклопедія, 1998. Т.1: А-Г. 672 С.

49. Юридична енциклопедія: в 6 т. / за ред. Ю. С. Шемшученка. Київ: Укр. Енциклопедія, 1998. Т.4: Н-П. 720 С.

50. Тодика Ю. Н. Конституційно-правовий статус людини і громадянина в Україні. Київ: Видавничий Дім Ін Юре, 2004. 386 С.

51. Анпілогов О. В. Захист прав та свобод громадянина прокурором в адміністративному судочинстві: монографія. Київ: Видавничий Дім Ін Юре, 2008. 168 С.

52. Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С., 2015. 220 С.

53. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20 листопада 2012 року № 5492-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення: 25.06.2024).

54. Самойленко Ю. С. Адміністративно-правове забезпечення захисту персональних даних в Україні: дис. … канд. юрид. наук: 12.00.07. Запоріжжя, 2023. 212 С.

55. Кодекс законів про працю України: Закон України від 10 грудня 1971 року № 322-08. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/322-08#Text (дата звернення: 25.06.2024).

56. Рішення Конституційного Суду України за справою № 1-9/2012 від 20 січня 2012 року № 2-рп/2012. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення: 28.06.2024).

57. Концевой Р. С. До питання визначення поняття персональні дані. *Інформація і право.* 2012. № 2. С. 23–28. URL: https://doi.org/10.37750/2616-6798.2012.2(5).271831

58. Курилюк Ю. Б. Державна прикордонна служба України в системі органів охорони правопорядку. *Науковий вісник публічного та приватного права.* 2019. № 2 (5). С. 145–150. URL: DOI https://doi.org/10.32844/2618-1258.2019.5-2.27

59. Кушнір І. П. Співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності Державної прикордонної служби України. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2018. № 35. Т-1. С. 81–84.

60. Корж І. Ф. Державна прикордонна служба України: правовий статус та місце в системі сектору безпеки і оборони. *Вісник Національної академії Державної прикордонної служби України. Серія: Юридичні науки*. 2017. № 2.

61. Про Державну прикордонну службу України: Закон України від 03 березня 2003 року № 661-IV. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 01.07.2024).

62. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.07.2024).

63. Корж І. Ф. Адміністративно-правове регулювання відносин у сфері державної безпеки України: монографія. – В. : ТОВ «Нілан-ЛТД», 2013. 384 С.

64. Михайлова Ю. О. Роль та місце Державної прикордонної служби у системі суб'єктів забезпечення національної безпеки України. *Форум права.* 2017. № 4. С. 152–158.

65. Нікіфоренко В. С. Особливості державної політики у сфері забезпечення безпеки державного кордону. *Юридичний бюлетень.* 2019. № 11. Ч. 1. С. 328–335.

66. Про концепцію розвитку Державної прикордонної служби України на період до 2015 року: Указ Президента України від 19 червня 2006 року № 546 / 2006. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/546/2006/print (дата звернення: 03.07.2024).

67. Про схвалення Концепції інтегрованого управління кордонами: Розпорядження Кабінету Міністрів України від 27 жовтня 2010 року № 2031-р. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2031-2010-%D1%80#Text (дата звернення: 05.07.2024).

68. Ляшук Р. М. Діяльність відділів прикордонної служби Державної прикордонної служби України (адміністративно-правовий аспект): монографія / за заг. ред. д-ра юрид. наук, проф. В. Л. Грохольського. Хмельницький: НАДПСУ, 2015. 386 С.

69. Пономаренко Г. О. Адміністративно-правові засади управління у сфері забезпечення внутрішньої безпеки держави: автореф. дис. на здобуття наук. ступеня д-ра юрид. наук:12.00.07. Харків, 2008. 36 С.

70. Інструкція з організації оперативно-службової діяльності відділу прикордонної служби Державної прикордонної служби України. Частина І (відділ прикордонної служби): наказ Адміністрації Держаної прикордонної служби України від 29 вересня 2009 року № 1040. Хмельницький: НАДПСУ, 2010. 176 С.

71. Про розвідку: Закон України від 17 вересня 2020 року № 912-IX. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/912-20#n2 (дата звернення: 20.07.2024).

72. Головний центр обробки спеціальної інформації. *Офіційний сайт Державної прикордонної служби України.* URL: https://dpsu.gov.ua/uk/golovnij-centr-obrobki-specialnoyi-informaciyi (дата звернення: 20.07.2024).

73. Наказ Адміністрації Державної прикордонної служби України «Про затвердження Положення про базу даних «Відомості про осіб, які перетнули державний кордон України»» від 25 червня 2007 р. № 472. URL: https://document.vobu.ua/doc/14696 (дата звернення: 20.07.2024).

74. Наказ «Про затвердження Положення про базу даних “Відомості про осіб, які перетнули державний кордон України”» від 27 вересня 2022 р. №614. Зареєстровано в Міністерстві юстиції України 11 жовтня 2022 р. за №1319/38555. *Офіційний вісник України*. URL: https://zakon.rada.gov.ua/laws/show/z1319-22 (дата звернення: 07.06.2026).

75. Басараб О., Басараб О. Деякі підходи підвищення ефективності функціонування інформаційно-комунікаційної системи Державної прикордонної служби України. *Збірник наукових праць НАДПСУ – Migration & Law.* 2022. С. 63–73. URL: https://doi.org/10.32752/2786-5185-2022-2-3-4-63-73

76. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року: Розпорядження Кабінету Міністрів України від 24 липня 2019 року № 687-р. *Офіційний сайт Верховної Ради України*. URL:

https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text (дата звернення: 22.07.2024).

77. Про контррозвідувальну діяльність: Закон України від 26 грудня 2002 року № 374-IV. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text (дата звернення: 25.07.2024).

78. Про розвідувальні органи України: Закон України від 22 березня 2001 року № 2331-III. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2331-14#Text (дата звернення: 28.07.2024).

79. Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 01.08.2024).

80. Байдюк І. І. Адміністративно-правове забезпечення взаємодії Державної прикордонної служби України з правоохоронними органами: дис. … док-ра філос. юрид. наук. Суми, 2021. 235 С.

81. Марущак А. І. Правові основи захисту інформації з обмеженим доступом: курс лекцій. Київ: КНТ, 2007. 208 С.

82. Цевельов О. Є. Державне реагування на загрози національній безпеці у сфері безпеки державного кордону України: дис. … канд. наук з держ. упр.: 25.00.05. Хмельницький, 2017. 313 С.

83. Ксензюк А. Я. Поняття та значення прикордонної безпеки держави. *Київський часопис права.* 2021. № 4. С. 38–42. URL: https://doi.org/10.32782/klj/2021.4.5

84. Литвин М. М. Шляхи реалізації правоохоронних функцій Державної прикордонної служби України. *Збірник наукових праць НАДПСУ*. 2008. № 43. Ч. 2. С. 19–21.

85. Мельников О. Г. Інтегрований прикордонний менеджмент – європейська модель управління кордонами для України. *Вісник Державної прикордонної служби України*. 2008. № 3. С. 46–51.

86. Курилюк Ю. Б. Державний кордон і правопорядок (законодавство, теорія, практика): монографія. Київ: ВД «Дакор», 2020. 440 С.

87. Кушнір І. П. Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: монографія. Хмельницький: ПП «Монускрипт», 2020. 528 С.

РОЗДІЛ 2. СТАН ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

2.1. Впливи глобальних процесів цифровізації та діджиталізації на механізми регулювання захисту персональних даних

У зв'язку з обраним Україною євроінтеграційним шляхом та стрімким розвитком інформаційних технологій (надалі – ІТ) [1, С. 7] виникає потреба в регулюванні процесів цифровізації в частині виконання завдань охорони персональних даних у сфері охорони державного кордону України, що актуалізується в умовах гібридного збройного конфлікту.

В сучасних умовах розвитку ІТ Державна прикордонна служба України (надалі – ДПСУ), з метою належного забезпечення прав і свобод людини і громадянина, зокрема права на захист персональних даних осіб, котрі перетинають державний кордон України, також адаптується до сучасних процесів цифровізації.

Сучасне суспільство характеризується швидким розвитком ІТ, що вимагає від державних органів та установ адаптації і модернізації своїх службових процесів, адже в умовах цифровізації зростає обсяг інформації, а саме персональних даних, яка обробляється ДПСУ, оскільки збільшується кількість перетинань державного кордону України [2, С. 89].

Зазначені процеси є складовою ширшої тенденції цифровізації суспільства, в межах якої ІТ виступають не лише інструментом оптимізації управлінської діяльності, а й визначальним чинником зміни соціальних, економічних і правових відносин, що зумовлює переосмислення ролі держави у сфері використання та захисту інформації, зокрема персональних даних, а особливо це важливо в діяльності ДПСУ.

Розвиток ІТ відіграє ключову роль у зростанні розвитку вектора трансформації сучасного суспільства, адже на ці технології покладаються значні очікування, зокрема, щодо потенційної повної перебудови соціальних структур, формування цифрової реальності, яка може змінити традиційну [3, С. 66]. ІТ докорінно трансформували уявлення про сучасні суспільні відносини, зокрема

щодо функціонування віртуального простору ведення бізнесу, Інтернету речей, обігу цифрового контенту, використання штучного інтелекту (надалі – ШІ) та формування нової цифрової реальності [4, С. 60].

Зазначені трансформаційні процеси безпосередньо впливають на публічне управління та діяльність державних інституцій, зокрема і на діяльність ДПСУ, зумовлюючи необхідність переосмислення традиційних підходів до організації державної влади, надання публічних послуг і забезпечення правового регулювання в умовах цифровізації.

Як зазначає науковиця Я. М. Сандул, цифровізація в Україні продовжує формувати новий тип держави та становлення правової системи із чітким орієнтиром на задоволення потреб суспільства, реалізуючи заходи практичного впровадження, інтеграції та освоєння нових цифрових сервісних технологій [5, С. 58] в системі охорони державного кордону України.

У цьому контексті цифровізація розглядається не лише як напрям технологічного оновлення державних інституцій, а розглядається і як важливий інструмент забезпечення прикордонної безпеки, як аспекту національної безпеки в цілому.

Цифровізація в умовах розвитку інформаційного суспільства та подальшого становлення суспільства знань, а також в умовах гібридного збройного конфлікту, є вкрай важливим інструментом створення відповідної електронної інфраструктури як у приватному, так і публічному секторі управління, покращення рівня цифрової грамотності державних службовців, громадян, побудови цифрової економіки [6, С. 813].

Зазначені процеси мають системний характер і виходять за межі внутрішньодержавних трансформацій, оскільки цифрові технології дедалі більше впливають на конкурентоспроможність держав на міжнародній арені, визначають напрями соціально-економічного розвитку та стають важливим чинником адаптації національних економік до глобальних викликів.

Варто зазначити, що сучасні геополітичні процеси, подальша інтеграція України у міжнародний простір та у Європейську спільноту довели важливість

та актуальність цифрових технологій для зростання добробуту населення, ефективності реалізації стратегічних напрямів та розвитку економік. Використання цифровізації у країнах світу вже протягом тривалого часу є об'єктивною потребою сьогодення [1, С. 7].

Водночас, масштабність процесів цифровізації зумовлюють необхідність їх належного теоретичного осмислення, зокрема в контексті правового регулювання, що актуалізує питання визначення сутності та змісту цифровізації як самостійної науково-правової категорії.

На думку О. Вжишневської, впровадження досліджуваної категорії у правову матерію, виходячи з її глобального розуміння у філософії, соціології, економічних, технічних науках, передбачає конкретизацію її змістовного наповнення та ознак, адже як у законодавстві, так і у науковій літературі відсутній єдиний підхід до визначення цифровізації як правової категорії [6, С. 813].

У зв'язку з цим особливої актуальності набуває звернення до нормативно-правових актів, які закріплюють офіційне тлумачення зазначеного поняття та слугують орієнтиром для його правового осмислення і практичного застосування. За цих умов потрібно орієнтуватися на законодавче його визначення, де відповідно до положень ст. 2 Закону України «Про Національну програму інформатизації», зазначено, що цифровізація – процес впровадження цифрових технологій у всі сфери суспільного життя [7].

Кабінетом Міністрів України (надалі – КМУ) було схвалено «Концепцію розвитку цифрової економіки та суспільства України на 2018 – 2020 роки» [8], і відповідно до її положень зазначено, що цифровізація – це насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір.

У сучасній науці та на практиці цифровізація визначається як провідний напрям розвитку людської цивілізації, що формує більш інклюзивне суспільство

та ефективні механізми управління, підвищує якість та охоплення державних та адміністративних послуг, розширює доступ до охорони здоров'я та освіти, банківських послуг, визначає найкращий спосіб співпраці людей, а також дає змогу скористатися більшим розмаїттям товарів за нижчими цінами [9, С. 7].

З огляду на комплексний характер зазначених процесів цифровізація істотно впливає не лише на соціально-економічні відносини, а й на правову сферу, зумовлюючи трансформацію традиційних правових інститутів та переосмислення змісту і механізмів реалізації прав людини. Саме в цьому контексті ІТ постають як чинник, що змінює способи взаємодії особи з державою, суспільством та іншими суб'єктами правовідносин.

Варто зауважити, що особливих впливів в нинішніх умовах цифровізації зазнають права людини. Особливо показовим у цьому контексті є стрімкий розвиток електронної демократії, впровадження електронного документообігу, доступ до інтернету, розвиток телекомунікацій, впровадження національних електронних інформаційних ресурсів, надання електронних послуг у всіх сферах суспільного життя, здійснення електронної ідентифікації, цифровізація адміністративних послуг тощо. Як зазначають науковці, процес трансформації прав людини значно прискорився в умовах глобалізації технологій та зумовлює виділення п'ятого покоління прав людини, які характеризуються штучним інтелектом та цифровою трансформацію суспільства [10, С. 7].

У цьому контексті цифровізація виступає не лише чинником правової модернізації, а й інструментом соціально-економічних змін, що безпосередньо відображається на повсякденному житті людини та функціонуванні економічних суб'єктів, адже процеси цифровізації суспільства зумовлюють забезпечення балансу між ІТ прогресом та захистом прав і свобод людини.

В умовах глобалізації, саме цифровізація суттєво впливає на якість життя пересічних громадян та ефективність діяльності суб'єктів господарювання на основі автоматизації, механізації і роботизації, адже вона стосується всіх сфер діяльності, оскільки суспільство, держава і суб'єкти господарювання є споживачами інноваційних ІТ [11, С. 68].

Водночас багатовимірний характер цифровізації зумовлює відсутність єдиного універсального підходу до її тлумачення, що проявляється у наявності різних наукових і практичних дефініцій особливо залежно від сфери застосування. Саме тому у науковому дискурсі цифровізація розглядається не лише як ІТ процес, а й як інструмент реформування публічного управління та надання державних послуг.

Розглядаючи питання цифровізації ми стикаємося з різноманіттям цього поняття, адже одним з таких висловлювань є те, що цифровізація – це поступове перетворення усіх державних послуг на зручні онлайн – сервіси, які повинні зменшити бюрократію та корупцію у державних установах [12, С. 164].

У свою чергу, на думку К. Маркевич, цифровізацію доречно характеризувати як зміну культури, яку інтегрують у всі сфери діяльності та трансформацію, спрямовану на управління різними командами [13].

Термінологічно цифровізація (англ. – digitalization) розуміється як впровадження цифрових технологій в усі сфери життя від взаємодії між людьми до промислових виробництв [14].

Водночас розуміння цифровізації доповнюється підходами, які акцентують увагу на практичному вимірі інтеграції ІТ у повсякденне життя та діяльність суспільства.

У Енциклопедії інформаційних наук і технологій зазначено, що цифровізація – це інтеграція цифрових технологій у повсякденне життя суспільства шляхом оцифровки всього, що можна оцифрувати. Цифровізація означає комп’ютеризацію систем і робочих місць для більшої легкості та доступності [15].

М. В. Руденко зазначає, що змістом цифровізації є: впровадження інформаційно-комунікаційних технологій (хмарних технологій, Big Data аналітики, Інтернету, соціальних мереж) для автоматизації процесів, оптимізації виробництва, покращення якості послуг, зростання продуктивності, зниження витрат на управління та виробництво, підвищення конкурентоспроможності суб’єктів господарювання, оптимізації бізнес-процесів, забезпечення

доступності освіти, медичних, адміністративних послуг всім громадянам, особливо у віддалених територіальних громадах [16]. Заслуговує на підтримку сформований автором філософський аспект цифровізації, а саме – це формування нової системи комунікації, нового інформаційного глобального простору. Правовий аспект цифровізації визначається необхідністю встановлення загальнообов'язкових правил обміну інформацією за допомогою інформаційно-телекомунікаційних технологій, захисту персональних даних [6, С. 814].

Окремої уваги заслуговує виокремлення філософського та правового аспектів цифровізації, що підкреслює її комплексний і багатоаспектний характер. Водночас, різноманіття підходів до осмислення цього явища зумовлює необхідність подальшого теоретичного уточнення його змісту.

Науковиця М. Хаустова зазначає, що термін «цифровізація» використовують у двох значеннях: вузькому та широкому. За її твердженням, у вузькому значенні цифровізація є перетворенням інформації у цифрову форму, що знижує витрати і сприяє виникненню нових можливостей тощо. Натомість цифровізація у широкому сенсі є трендом, який свідчить про ефективний світовий розвиток лише тоді, коли цифрова трансформація відповідає певним вимогам, зокрема таким:

- охоплення виробництва, бізнесу, науки, соціальної сфери та звичайного життя громадян;

- лише ефективне використання її результатів;

- доступність її результатів для користувачів перетвореної інформації;

- її результати використовують не лише фахівці, а й пересічні громадяни, навичками роботи з нею володіють користувачі цифрової інформації [9, С. 9].

Загалом, цифровізація – це визначальна тенденція розвитку людської цивілізації, яка формує більш інклюзивне суспільство та кращі механізми управління, розширює доступ до охорони здоров'я, освіти та банківської справи, підвищує якість та охоплення державних послуг, розширює спосіб співпраці людей [9, С. 7]. Усвідомлення масштабності та комплексності зазначених

процесів зумовлює необхідність їх теоретичного осмислення через призму різних наукових підходів.

Варто виділити декілька підходів до розуміння природи та характеристик цифровізації. Перший зосереджується на технологічних аспектах розширення цифрових технологій в усіх сферах суспільного життя, спрямованого на вдосконалення комунікації між учасниками та впровадження інформаційно-комунікаційних технологій у різноманітні процеси та взаємодії. Другий підхід розглядає фундаментальні трансформації в організації суспільства, де цифрові технології стають основою для створення нових інститутів, що призводить до зміни самої моделі суспільного розвитку. У цьому контексті цифрові технології перетворюються з інструменту взаємодії на сутнісну складову розвитку та його ресурс, супроводжуючи модифікацію механізмів, процедур і методів діяльності.

Інформація перетворюється на цифровий формат, охоплюючи виробничу, підприємницьку, наукову, соціальну сфери та державне управління. Цифрові технології трансформують сучасні суспільні відносини, стаючи невіддільною частиною повсякденного життя людей. Таким чином відбувається цифрова трансформація, що перетворює наше суспільство на цифрове [17].

Усвідомлення системного характеру змін цифровізації, зумовлює необхідність визначення ключових її завдань, як цілеспрямованого процесу державної та суспільної модернізації.

Основні завдання цифровізації відповідно до Концепції [8] полягають у корегуванні недоліків ринкових механізмів, подоланні інституційних, законодавчих перешкод, започаткуванні проєктів цифрових трансформацій на національному рівні та залученні відповідних інвестицій, стимулюванні розвитку цифрової інфраструктури, формуванні потреб щодо використання цифрових технологій громадянами, а також розвитку відповідних цифрових компетенцій, створенні відповідних стимулів, мотивацій із метою підтримки цифрового підприємництва та цифрової економіки.

Реалізація зазначених завдань зумовлює певні зміни у соціально-економічному розвитку суспільства, які проявляються не лише на рівні

державної політики чи окремих секторів оборони, а й у повсякденному житті громадян. Саме тому в науковому дискурсі цифровізація розглядається крізь призму її переваг і позитивних наслідків, що виникають на різних рівнях суспільної організації.

Науковиця О. Пищуліна зазначає, що цифровізація всіх життєвих аспектів обумовлена передусім високою швидкістю, а також можливістю позитивних проявів і наслідків, які виникають на усіх рівнях та називає перевагами цифровізації на суспільному рівні:

- економічний, соціальний ефекти, які виникають під впливом використання цифрових технологій, зокрема для бізнесу й суспільства;

- підвищення якісного рівня життя людей; зростання продуктивності суспільної праці з урахуванням її підвищення на окремих виробництвах та підприємствах;

- появу нових видів та форм бізнесу, які сприяють підвищенню прибутковості, конкурентоспроможності діяльності;

- забезпечення функціонування прозорих економічних операцій, можливість їх моніторингу;

- доступність державних, комерційних товарів та послуг, їх просування на світовий рівень;

- створення людинозамінних систем, до прикладу, для певних підприємств [18, С. 82].

В нинішній час цифровізація потребує нових форм партнерства та співробітництва у різних сферах економіки й суспільства. З огляду на це сформульовано такі принципи цифровізації:

- забезпечення кожному громадянинові рівного доступу до послуг, інформації, знань, які надають за допомогою інформаційно-комунікаційних і цифрових технологій;

- спрямованість на створення переваг у різноманітних сферах повсякденного життя;

- здійснення цифровізації через механізм економічного зростання за допомогою підвищення ефективності, продуктивності, конкурентоздатності від використання цифрових технологій;

- сприяння розвитку інформаційного суспільства, засобів масової інформації; орієнтування на міжнародне, європейське,

- регіональне співробітництво з метою інтеграції України в Європейський Союз (надалі – ЄС), виходу на європейський та світовий ринок;

- застосування стандартизації як основи цифровізації, одного з головних чинників її успішної реалізації; підвищення рівня довіри та безпеки, які мають супроводжувати цифровізацію [8].

В наш час паралельно з терміном «цифровізація» використовується і термін «діджиталізація» [19, С. 34], про котрі можна стверджувати як тотожні, адже обидва поняття описують комплексний процес упровадження цифрових технологій та інформаційних систем (надалі – ІС) у систему охорони державного кордону України, який охоплює автоматизацію діловодства, електронний документообіг, відеоконференції та інші інноваційні рішення [19, С. 37], спрямовані на підвищення охорони та захисту персональних даних в діяльності ДПСУ.

З огляду на зазначене, цифровізація та діджиталізація у системі охорони державного кордону України, передбачають не лише технічне впровадження сучасних ІС, а й трансформацію організаційних процесів, підвищення ефективності управління ресурсами, оптимізацію процедур контролю та моніторингу, а також забезпечення прозорості та оперативності прийняття рішень. Водночас ключовим аспектом такого впровадження є забезпечення безпеки та конфіденційності інформації, що обробляється, а також формування високого рівня цифрових компетенцій військовослужбовців ДПСУ задля ефективного використання сучасних ІТ.

Науковці М. Дубина та О. Козлянченко зазначають, що діджиталізація є сучасним етапом розвитку суспільства й економіки, якому притаманний високий рівень поширення інформаційних ресурсів, інформаційних технологій,

суспільних процесів. Завдяки цьому оцифровують різні дані, розширюючи можливості їх використання у всіх сферах діяльності людей [20, С. 28].

В контексті публічного адміністрування та безпеки діджиталізація сприяє підвищенню ефективності функціонування органів влади, оптимізації адміністративних процедур, пришвидшенню обміну інформацією та прийняттю оперативних рішень. Крім того, вона забезпечує інтеграцію різних інформаційних систем, формування електронних баз даних, розвиток електронних сервісів для громадян та підвищення прозорості й контролю за виконанням завдань у різних секторах суспільного життя.

К. Кравченко стверджує, що діджиталізація суттєво трансформує правове забезпечення інформаційної взаємодії між реєстрами, розставляючи інші акценти, зокрема, не лише про те, що комунікують, а й про що саме комунікують. До речі, за допомогою новітніх цифрових технологій створюють і поширюють значні обсяги інформації серед необмеженого кола осіб. Це відбувається якісно, з надзвичайною швидкістю та без значних витрат. Використання новітніх технологій сприяє застосуванню провідних світових досягнень (наприклад, інформація частково може зберігатись у хмарному середовищі, а частково може розміщуватись на центральних державних серверах) [21, С. 114].

Т. Шлапко, М. Старинський, В. Миргород-Карпова, А. Висоцький та Д. Шеін зазначають, що за допомогою діджиталізації держава може полегшувати виконання своїх завдань, забезпечувати прозору діяльність уряду, міст і громад, а це в свою чергу гарантує підвищення авторитету держави на світовому рівні, а також сприяє забезпеченню економічної привабливості регіонів для іноземного інвестування в державну економіку [22, С. 143].

На нашу думку, діджиталізація виступає не лише інструментом модернізації державного управління, а й важливим чинником підвищення ефективності охорони державного кордону України. Вона дозволяє оптимізувати управлінські процеси у сфері прикордонного контролю, забезпечує оперативність та точність обробки інформації про переміщення осіб і

транспортних засобів через державний кордон України, а також сприяє розвитку сучасної інфраструктури пунктів пропуску та мінімізує корупційні ризики.

Використання цифрових технологій у сфері охорони державного кордону України сприяє впровадженню інноваційних рішень для захисту національної безпеки та посилює спроможність України інтегруватися у європейський простір безпеки.

Урядом України приймаються широкомасштабні заходи з розвитку цифровізації суспільства, цифрового сектору економіки, впроваджуються електронні платежі та вдосконалюється нормативно-правова база у сфері електронної комерції [9, С. 9], а тому для прискорення процесів діджиталізації в Україні, у 2019 році було засновано Міністерство цифрової трансформації України (надалі – Мінцифри).

Відповідно до Положення «Про Міністерство цифрової трансформації України» [23], Мінцифри є головним органом у системі центральних органів виконавчої влади та відповідає за розробку та впровадження державної політики у наступних сферах:

- цифровізація, цифровий розвиток, цифрова економіка, цифрові інновації, електронне урядування та електронна демократія, розвиток інформаційного суспільства та інформатизація;

- розвиток цифрових навичок та забезпечення цифрових прав громадян;

- відкриті дані, розвиток національних електронних інформаційних ресурсів та інтероперабельність, розбудова інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронна комерція та бізнес;

- надання електронних та адміністративних послуг;

- електронні довірчі послуги та електронна ідентифікація;

- розвиток ІТ-індустрії.

Головною ціллю Мінцифри на сьогодні є втілення проєкту «Цифрова держава», який має на меті інтегрувати всі державні установи в єдину ефективну онлайн-платформу «Дія» (скорочення від «Держава і я»). Наразі «Дія» функціонує як у форматі веб-порталу, так і мобільного додатку, що значно

підвищує зручність користування. Наповнення платформи відбувається надзвичайно динамічно – менш ніж за рік вдалося оцифрувати 30 різноманітних електронних послуг для населення та бізнесу. При цьому розробники об'єднують декілька сервісів в один для оптимізації процесів. Система також дозволяє підтверджувати особу користувача через електронні версії документів: студентський квиток, ID-картку, біометричний закордонний паспорт та водійське посвідчення. Важливо зазначити, що електронні паспорти в додатку «Дія» мають офіційний статус цифрових аналогів паперових документів, що закріплено на законодавчому рівні [24].

Цей проєкт амбіційно планував покриття усіх сфер життєдіяльності країни і суспільства, а саме здійснення процесів управління в державі за допомогою інформаційних технологій, захист державної та приватної інформації від несанкціонованого використання, управління державою через референдуми, консультації та опитування за допомогою інформаційних технологій, безготівкові розрахунки та електронний документообіг, обмін документами між судами, установами й учасниками судового процесу, розгляд окремих справ онлайн, електронний обмін медичними даними пацієнта між різними установами (телемедицина) та система дистанційного моніторингу стану пацієнта, електронізація процесу навчання, електронний квиток, мобільне паркування та управління трафіком, національний план розвитку широкосмугового доступу до інтернету [5, С. 59].

Так, КМУ затвердив Положення «Про єдиний державний вебпортал електронних послуг» [25], в якому визначив мету, завдання, суб'єктний склад (користувачів, а саме суб'єкта звернення та суб'єкта розгляду звернень, держателя та технічного адміністратора) та функціональні можливості Порталу «Дія». Планами Мінцифри анонсувалася можливість забезпечення технічними можливостями доступу до 100 % державних послуг на порталі та в мобільному застосунку «Дія» до 2023 року.

У звіті «Про імплементацію Угоди про асоціацію в Україні» за період з 1 грудня 2020 року до початку військової агресії Російської Федерації (надалі –

РФ) проти України 24 лютого 2022 року, опублікованому ЄС, сфера цифровізації була відзначена як одна з найпрогресивніших у своєму розвитку. Позитивної оцінки дістали кроки цифрової трансформації України у побудові ефективного та прозорого урядування та боротьби з корупцією.

З 24 лютого саме цифровізація стала основою для ефективної роботи держави. З моменту повномасштабного вторгнення РФ, саме перед Мінцифри постало питання не тільки підтримки започаткованих ініціатив, а й надшвидкісне реагування на події шляхом адаптації існуючих послуг і створення нової взаємодії держави і суспільства. Протягом року Мінцифри активно працювали над розвитком «Дії». Зокрема, були реалізовані послуги для внутрішньо-переміщених осіб (надалі – ВПО), пошкоджене майно, виплати від держави, допомога по безробіттю тощо [5, С. 59 – 60].

Метою цифровізації України є цифрова трансформація сфер її життєдіяльності в ефективніші та сучасніші, а також трансформація наявних і створення нових галузей економіки. Водночас сучасний цифровий простір, а також відповідна інфраструктура вважаються вигідними і для громадян та бізнесу, і для зовнішнього інвестора. За пріоритетним сценарієм щодо цифровізації, для країни одне з першочергових завдань полягає в усуненні бар'єрів законодавчого, інституційного, фіскальноподаткового характеру та інших, які перешкоджають розвитку цифрової економіки [26, С. 94].

Впровадження в Україні цифровізації та сучасних ІТ не оминули й діяльність ДПСУ. Так, з 12 жовтня 2025 року в країнах ЄС почала діяти нова процедура перетину кордону «Entry/Exit System» (надалі – EES), яка замінює звичні штампи в паспортах і запроваджує автоматичний збір біометричних даних при в'їзді та виїзді з Шенгенської зони.

Система «EES» – це єдина електронна система, яка фіксує дату і місце в'їзду або виїзду громадян третіх країн, тобто тих, хто не входить до складу ЄС і Шенгенської зони.

Головна мета нововведення – це посилення безпеки і спрощення контролю за міграційними потоками. Завдяки «EES» європейські служби зможуть швидше

виявляти випадки перевищення терміну короткострокового перебування (до 90 днів протягом 180-денного періоду), а також боротися із нелегальною міграцією [27].

Під час першого в'їзду до Шенгенської зони, після запуску «EES», особа проходитиме розширену реєстрацію, яка включатиме збір біометричних даних: зображення обличчя та чотири відбитки пальців. При наступних перетинах кордону процес буде спрощено та прискорено, оскільки біометричні дані звірятимуться з уже наявною цифровою інформацією [28].

Процес впровадження «EES» буде поетапним. У Польщі, яка вважається головним хабом для перетину державного кордону серед українців, система почала працювати з 12 жовтня 2025 року [27], а протягом шестимісячного перехідного періоду країни-учасниці прикордонних відомств поступово введуть «EES» в експлуатацію [28].

На нашу думку, важливою складовою цифровізації в оперативно-службовій діяльності ДПСУ є впровадження в автомобільних пунктах пропуску через державний кордон України системи електронної черги (надалі – «єЧерга»), яка упорядковує та збільшує транспортний потік вантажних транспортних засобів.

З системою «єЧерга» перевізники можуть планувати день та час прибуття до пункту пропуску, адже можуть знати, коли настане їхня черга перетинати державний кордон України. Це дозволяє оптимізувати час, витрачений на перебування в черзі та зменшити витрати на перевезення товарів [29].

Реєстрація в системі «єЧерга» здійснюється заздалегідь у будь-якому зручному для цього місці, а не безпосередньо перед пунктом пропуску та можлива з будь-якого пристрою із доступом до мережі Інтернет. Під час реєстрації користувач (перевізник чи безпосередньо водій) зазначає контактну електронну адресу (надалі – e-mail) та номер телефону.

Під час бронювання місця в системі «єЧерга», користувач зазначає контактний e-mail, номер телефону, дані водія (прізвище, ім'я та по батькові), номер і серію закордонного паспорта водія, громадянство, державний номерний

знак авто та напівпричепа, номер митної декларації або іншого митного документа. В окремих випадках є необхідність додати фото техпаспорта на транспортний засіб. В разі, якщо під час реєстрації припустилися помилки у прізвищі водія, то потрібно скористатися функцією заміни даних про водія та виправити відповідну помилку.

Проект «єЧерга» реалізовується Міністерством розвитку громад та територій у співпраці з Міністерством цифрової трансформації, Укртрансбезпекою, Державним агентством відновлення та розвитку інфраструктури, Державною митною службою та ДПСУ за підтримки USAID / UK aid проєкту «Прозорість та підзвітність у державному управлінні та послугах/TAPAS».

Варто зауважити, що пілотний запуск проекту «єЧерга» відбувся 12 грудня 2022 року також на кордоні з Польщею, а саме в міжнародному автомобільному пункті пропуску «Ягодин – Дорогуськ» та наразі діє на 29 міжнародних пунктах пропуску для вантажівок та автобусів [30].

Таким чином, у зв'язку з приведенням у відповідність до кращих європейських стандартів цифровізації та практик, а саме задля покращення проходження прикордонного контролю, ДПСУ впроваджує «EES» та «єЧергу», а також адаптує та інтегрує власні інформаційні системи перетину державного кордону України до інформаційних систем та баз даних ЄС.

На нашу думку, варто також звернути увагу і на ще одну важливу складову цифровізації, а саме на систему електронного документообігу (надалі – «СЕД»), яка була введена в оперативно-службову діяльність ДПСУ з метою своєчасного розгляду та опрацювання електронних документів.

Відповідно до «Інструкції з діловодства в ДПСУ» [31], основною формою ведення документації є електронний документообіг, що сприяє підвищенню ефективності управління, оперативності обробки інформації та сучасному підходу до організації роботи.

Основними функціями «СЕД» в оперативно-службовій діяльності ДПСУ є:

- формування, розроблення, реєстрування та зберігання електронних документів;

- розроблення карток документів;

- маршрутизація документів за заданими маршрутами; існування можливостей щодо фіксації руху документів;

- ведення історії змін документів; формування та налаштування інформації (повідомлень) про проходження документу та його статуси; фіксація у журналах дат та строків виконання, побудови звітів, забезпечення контролю виконання;

- виконання аналітичних функцій; імпортування та експортування документів, їх друк та сканування;

- реалізація принципу конфіденційності інформації та безпеки у системі; здійснення контролю щодо доступу до документів та розмежування відповідного доступу;

- використання можливостей цифрового підпису тощо.

Також варто зазначити, що «СЕД» працює відповідно до принципів:

- реєстрація документу (одноразова) з метою однозначної ідентифікації документу в будь-якій установці такої системи;

- паралельне виконання процедур, що уможливлює скорочення часу руху документів та підвищення оперативності їх виконання;

- неперервний рух документів, що дозволяє ідентифікацію відповідальних за виконання завдань у моменти існування документу;

- єдина (в окремих випадках і розподілена за погодженням) база інформації у документах;

- неможливість копіювання (дублювання) документів;

- ефективна організація систем пошуку документів;

- розгалужена система звітності за різними статусами та атрибутами документів задля контролю руху документів та прийняття управлінських рішень на основі даних зі звітів.

Варто також зазначити, що підписання чи візування документів у «СЕД» здійснюється в електронній формі із застосуванням кваліфікованого

електронного підпису (надалі – КЕП), кваліфікованої електронної печатки та кваліфікованої позначки часу.

Як зазначає О. Морохов, саме ДПСУ стала першим відомством, де повноцінно запроваджено «СЕД», що дало змогу значно підвищити ефективність роботи органів управління та суттєво зменшити обсяг паперових документів, а також залучення людського ресурсу та часу для їх узгодження та підвищити оперативність доведення інформації, а також своєчасного реагування і прийняття управлінських рішень [32, С. 78].

На нашу думку, впровадження в оперативно-службову діяльність ДПСУ цифрової системи контролю в'їзду та виїзду «Entry/Exit System», а також системи електронної черги «єЧерга» та системи електронного документообігу «СЕД» є показником того, що прикордонна служба поступово інтегрує сучасні інформаційно-комунікаційні технології у сферу охорони державного кордону України, з метою підвищення прозорості та ефективності здійснення прикордонного контролю для громадян при перетині державного кордону, а також належного захисту персональних даних відповідно до міжнародних стандартів.

2.2. Система адміністративно-правових заходів захисту персональних даних в умовах гібридного протистояння

Сучасні виклики національній безпеці України, зокрема, зумовлені широкомасштабною агресією Російської Федерації (надалі – РФ), а також нестабільною соціально-політичною та економічною ситуацією в нашій державі, вимагають швидкого реагування на зміни в обстановці на державному кордоні з боку керівників відповідних структур. Зазначене вимагає прийняття відповідних організаційно-правових та технічних заходів, що проявляється у вигляді синтезу об'єктивних управлінських впливів. Більшість цих впливів мають інформаційний характер, оскільки процес управління охороною державного кордону – це, переважно, процес оцінки та аналізу інформації [33].

Нинішній збройний конфлікт продемонстрував, що сучасні військові протистояння вже не обмежуються лише традиційними засобами ведення бойових дій. Застосовуються безпрецедентні технології для збору інформації про населення, інфраструктуру, зокрема використовуються системи штучного інтелекту (надалі – ШІ) та інші методи і способи.

Протистояння відбувається не тільки на землі, а й в інформаційному просторі, де традиційна зброя поєднується з новітніми технологіями, адже персональні дані стали засобом для досягнення ворожих цілей. Цифрова лінія фронту не має географічних меж і кордонів. Завдяки аналізу метаданих можна ідентифікувати конкретних осіб, прогнозувати військові операції, вивчати зв'язки між особами та проводити цілеспрямовані психологічні атаки проти населення [34, С. 4].

Динамічний розвиток та глобальне впровадження в усі галузі людської діяльності інформаційних технологій (надалі – ІТ) актуалізують процес інформатизації в Державній прикордонній службі України (надалі – ДПСУ).

Використання спеціалізованих інтегрованих інформаційно-пошукових систем (надалі – СІІПС) надає можливість задля ефективної реалізації завдань підрозділам ДПСУ формувати та використовувати масиви персональних даних [35, С. 173]. Зазначимо, що ефективне управління кордонами залежить від функціонування інформаційно-комунікаційної системи (надалі – ІКС) відомства [36, С. 65].

Як вже зазначалося вище, основою ІКС ДПСУ є Інтегрована інформаційно-комунікаційна система «ГАРТ» (надалі – ІІКС «ГАРТ»).

ІІКС «Гарт-1» – це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, записування, зчитування, зберігання, знищення, приймання, передавання) щодо прикордонного контролю осіб і транспортних засобів, які перетинають державний кордон України та автоматизований доступ до інформації, яка зберігається в базах даних системи «Гарт-1».

Структура та порядок формування баз даних ІІКС «Гарт-1» визначаються положеннями про них, що розробляються та затверджуються Адміністрацією ДПСУ (надалі – АДПСУ) відповідно до законодавства, а метою їх ведення є: обробка (збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення) інформації про осіб, які перетнули державний кордон України, їх паспортні документи (інші документи, передбачені законодавством), осіб, які в'їхали на тимчасово окуповану територію України або виїхали з такої території, їх паспортні документи (інші документи, передбачені законодавством), біометричні дані іноземців та осіб без громадянства отримані під час проходження ними прикордонного контролю, а також автоматичне обчислення дозволеного іноземцю, який є громадянином держави з безвізовим порядком в'їзду, строку перебування на території України.

На нашу думку, функціонування ІІКС «ГАРТ» має не лише технічне, а й стратегічне значення, оскільки вона використовуються для забезпечення розвідувальної та правоохоронної діяльності ДПСУ.

Відповідно до положень наказу ДПСУ [37], ІІКС «Гарт-1» створюється і використовується в інтересах розвідки, контррозвідувального забезпечення охорони державного кордону України, оперативно-розшукової діяльності, участі в боротьбі з організованою злочинністю та протидії незаконній міграції з метою своєчасного та достовірного інформаційно-аналітичного забезпечення діяльності підрозділів та органів ДПСУ для здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, розшуку в пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства, а також виконання інших завдань у правоохоронній сфері згідно із законодавством.

ІІКС «ГАРТ» слугує інформаційним захистом різного виду інформації, зокрема [38, С. 163], персональних даних та забезпечує реалізацію таких функцій:

- формування баз даних про осіб, які перетнули державний кордон Україні, у тому числі з фіксуванням їх біометричних даних, осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та інших баз даних, що створюються та використовуються відповідно до законодавства;

- автоматизація процесів перевірки відомостей про осіб, які перетинають державний кордон України, за базами даних осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та іншими базами даних, що створюються та використовуються відповідно до законодавства;

- надання користувачам доступу до інформації, що зберігається в системі «Гарт-1»;

- забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних ІІКС «Гарт-1».

Завдяки цим функціям, ІІКС «ГАРТ» сприяє ефективному захисту персональних даних, підвищуючи рівень інформаційної безпеки в сфері захисту державного кордону України, що особливо важливо та необхідно в умовах відбиття широкомасштабної військової агресії РФ проти України.

АДПСУ є власником ІІКС «Гарт-1» та інформації, що в ній обробляється, а її адміністратором є Головний центр зв'язку, автоматизації та захисту інформації ДПСУ (надалі – Головний центр зв'язку), який забезпечує її

безперервне функціонування та технічну підтримку. Користувачами ІІКС «Гарт-1» є посадові та службові особи підрозділів і органів ДПСУ, яким в установленому законодавством порядку надано право доступу до обробки інформації в цій системі. Право розпоряджатися ІІКС «Гарт-1» надається розпоряднику системи – начальнику зв'язку ДПСУ.

Основним завданням розпорядника є вирішення організаційних питань щодо забезпечення функціонування ІІКС «Гарт-1», надання користувачам доступу до інформації, що в ній обробляється, ведення їх обліку, прийняття взаємоузгоджених управлінських рішень стосовно її розвитку і вдосконалення, координації діяльності відповідних складових системи. Він також відповідає за матеріально-технічне та програмне забезпечення функціонування ІІКС «Гарт-1».

Розпорядник ІІКС «Гарт-1» повинен мати необхідні матеріально-технічний та кадровий ресурси для супроводження ІІКС «Гарт-1» і структурні підрозділи, об'єднані єдиною телекомунікаційною мережею.

Програмно-технічне та інформаційне забезпечення ІІКС «Гарт-1» здійснюється:

- щодо формування і підтримання в актуальному стані баз даних – уповноваженими органами ДПСУ;

- щодо збереження та захисту від порушення цілісності та несанкціонованого доступу, дотримання правил і процедур одержання інформації – розпорядником ІІКС «Гарт-1».

Складовими ІІКС «Гарт-1» є:

- центральна підсистема;

- програмно-технічні комплекси автоматизації прикордонного контролю (надалі - ПТК АПК) «Гарт-1/РУ», «Гарт-1/ООДК», «Гарт-1/П»;

- телекомунікаційна мережа; комплексна система захисту інформації з підтвердженою відповідністю.

Центральна підсистема ІІКС «Гарт-1» – це сукупність програмних і технічних засобів, призначених для обробки інформації, які забезпечують:

- обробку (введення, записування, зберігання, знищення, приймання та передавання) інформації та формування баз даних про осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та інших баз даних, передбачених законодавством та передавання цієї інформації до ПТК АПК «Гарт-1/П», установлених у пунктах пропуску (пунктах контролю) через державний кордон (надалі – пункти пропуску) або підрозділах органів охорони державного кордону, з використанням телекомунікаційної мережі;

- формування бази даних про осіб, які перетнули державний кордон України, шляхом приймання такої інформації від ПТК АПК «Гарт-1/П», установлених у пунктах пропуску або підрозділах органів охорони державного кордону, її зберігання та знищення;

- обробку (введення, приймання, передавання, зберігання та знищення) інформації та формування інших баз даних, які створюються та використовуються відповідно до законодавства;

- обробку (приймання, передавання, зберігання та знищення) інформації про виявлення під час прикордонного контролю та пропуску через державний кордон у пунктах пропуску осіб та паспортних документів за базами даних про осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та іншими базами даних, що створюються та використовуються відповідно до законодавства;

- надання користувачам доступу до інформації, що зберігається в базах даних центральної підсистеми;

- моніторинг стану інформаційного обміну між складовими ІІКС «Гарт-1», а також системних журналів аудиту роботи користувачів, програмних і технічних засобів;

- захист інформації під час її обробки.

ПТК АПК «Гарт-1/РУ», «Гарт-1/ООДК», «Гарт-1/П» ІІКС «Гарт-1» – це сукупність технічних засобів та програмного забезпечення, призначених для забезпечення обробки інформації в органах ДПСУ.

ПТК АПК розташовуються:

- ПТК АПК «Гарт-1/РУ» – у службових приміщеннях територіальних органів спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону - регіональних управлінь;

- ПТК АПК «Гарт-1/ООДК» – у службових приміщеннях управлінь органів охорони державного кордону;

- ПТК АПК «Гарт-1/П» – у службових приміщеннях (кабінах, павільйонах паспортного контролю) підрозділів органів охорони державного кордону в усіх пунктах пропуску, де здійснюються пасажирські перевезення та пропуск осіб через державний кордон.

Категорично забороняється доступ до цих приміщень стороннім особам та розміщувати в них технічні засоби, що не є складовими ІІКС «Гарт-1».

Матеріально-технічне та програмне забезпечення функціонування ПТК АПК «Гарт-1/РУ», «Гарт-1/ООДК», «Гарт-1/П», їх адміністрування здійснюються спеціально вповноваженими підрозділами органів ДПСУ.

ПТК АПК «Гарт-1/П» застосовуються в підрозділах органів охорони державного кордону, які здійснюють прикордонний контроль і пропуск через державний кордон осіб, транспортних засобів, вантажів та іншого майна, та забезпечують:

- автоматизовану перевірку відомостей про осіб, які перетинають державний кордон України, за базами даних осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які

переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та іншими базами даних, що створюються та використовуються відповідно до законодавства;

- уведення інформації до баз даних про осіб, які перетнули державний кордон Україні, у тому числі з фіксуванням їх біометричних даних та інших баз даних, що створюються та використовуються відповідно до законодавства;

- обробку інформації, яка зберігається в базах даних центральної підсистеми, в режимі віддаленого доступу;

- цілодобове відеоспостереження за територією та об'єктами в пунктах пропуску, відеозапис, детектування руху по кожному з відеоканалів, ведення циклічного відеоархіву та здійснення пошукових функцій по ньому;

- обробку відеозображень та розпізнавання державних номерних знаків автотранспорту та перевірки зчитаних номерних знаків за базами даних викраденого автотранспорту;

- автоматизований обмін інформаційними даними з центральною підсистемою;

- надання користувачам доступу до інформації, що зберігається в базах даних ПТК АПК «Гарт-1/П»;

- моніторинг системних журналів аудиту роботи користувачів, програмних і технічних засобів комплексів;

- захист інформації під час її обробки.

Телекомунікаційна мережа є складовою системи «Гарт-1». Її завданнями є забезпечення обміну інформацією між ПТК АПК «Гарт1/П» і центральною підсистемою та доступу до інформації, що зберігається в базах даних центральної підсистеми, з відповідних автоматизованих робочих місць ПТК АПК «Гарт-1/РУ», «Гарт-1/ООДК» та «Гарт-1/П». До складу телекомунікаційної мережі ІІКС «Гарт-1» входять центри комутації, пункти комутації та кінцеве обладнання.

Проведений аналіз досліджень щодо використання ІІКС «ГАРТ» в діяльності ДПСУ свідчить [39, С. 26–30], що найбільшу роль в оперативно-службовій діяльності на сьогоднішній день відіграє інформаційно-комунікаційна система (ІКС) прикордонного контролю. Автоматизація зазначеного напрямку оперативно-службової діяльності (надалі – ОСД) здійснюється із використанням програмно-технічних комплексів (ПТК) автоматизації прикордонного контролю «Гарт-1/П», які розгорнуті в пунктах пропуску через державний кордон України і входять до складу ІКС прикордонного контролю «Гарт-1» [36, С. 68].

Відповідно до ст. 2 Закону [40] прикордонний контроль – це державний контроль, що здійснюється Державною прикордонною службою України, який включає комплекс дій і систему заходів, спрямованих на встановлення законних підстав для перетинання державного кордону особами, транспортними засобами і переміщення через нього вантажів.

Згаданий контроль здійснюється з метою протидії незаконному переміщенню осіб через державний кордон, незаконній міграції, торгівлі людьми, а також незаконному переміщенню зброї, наркотичних засобів, психотропних речовин і прекурсорів, боєприпасів, вибухових речовин, матеріалів і предметів, заборонених до переміщення через державний кордон.

Необхідно зазначити, що прикордонний контроль здійснюється щодо осіб які перетинають державний кордон, транспортних засобів, що перевозять через державний кордон осіб та вантажів, що переміщуються через державний кордон України.

Складовими прикордонного контролю є перевірка документів; огляд осіб, транспортних засобів, вантажів; виконання доручень уповноважених державних органів України; перевірка виконання іноземцями, особами без громадянства умов перетинання державного кордону у разі в’їзду в Україну, виїзду з України та транзитного проїзду територією України; реєстрація іноземців, осіб без громадянства та їх паспортних документів у пунктах пропуску через державний кордон; перевірка автомобільних транспортних засобів з метою виявлення викрадених.

Перетинання громадянами України (надалі – громадяни) державного кордону здійснюється відповідно до Правил [41] в пунктах пропуску через державний кордон та пунктах контролю, якщо інше не передбачено законом, за одним із таких документів, що дають право на виїзд з України і в'їзд в Україну: паспорт громадянина України для виїзду за кордон, дипломатичний паспорт, службовий паспорт, проїзний документ дитини (чинний протягом строку на який він виданий), посвідчення особи моряка, посвідчення члену екіпажу.

Таким чином, важливим аспектом здійснення прикордонного контролю є не лише забезпечення безпеки державного кордону, але й захист персональних даних осіб, які його перетинають. Реєстрація громадян, транспортних засобів і вантажів потребує обробки значного обсягу інформації, що містить персональні дані. Тому важливо забезпечити їх конфіденційність, запобігаючи несанкціонованому доступу, витоку або використанню цієї інформації третіми особами.

На нашу думку, ІІКС «ГАРТ» у діяльності ДПСУ є важливим інструментом для забезпечення ефективного здійснення прикордонного контролю та охорони державного кордону України. Її функціонування дозволяє здійснювати автоматизовану перевірку осіб, транспортних засобів та документів, формувати бази даних із біометричними та іншими персональними даними, а також забезпечувати комплексний захист інформації.

Серед позитивних сторін використання ІІКС «ГАРТ» варто виділити:

- підвищення ефективності прикордонного контролю – автоматизація перевірок значно скорочує час обробки даних та зменшує ризик помилок;

- захист національної безпеки – система дозволяє своєчасно виявляти осіб, яким заборонено в'їзд чи виїзд, а також тих, хто ухиляється від кримінальної відповідальності;

- комплексний захист інформації – розмежування доступу та моніторинг дій користувачів знижують ризик несанкціонованого втручання;

- можливість інтеграції з базами даних правоохоронних органів – забезпечує оперативний обмін даними для боротьби із незаконною міграцією, торгівлею людьми та іншими злочинами;

- відеоспостереження та розпізнавання номерних знаків – додаткові інструменти для контролю транспортних засобів і запобігання злочинам.

Серед негативних сторін використання ІІКС «ГАРТ» варто виділити:

- ризики порушення конфіденційності персональних даних – великі масиви інформації про громадян та іноземців можуть стати об'єктом несанкціонованого доступу чи витоку;

- залежність від технічних ресурсів – у разі збоїв або кібератак система може тимчасово втратити працездатність, що може створити загрозу національній безпеці;

- можливість зловживань – доступ до баз даних надається посадовим особам, що потребує суворого контролю, аби уникнути неправомірного використання інформації;

- потенційне обмеження прав людини – надмірне накопичення та використання персональних даних може створювати ризики для свободи пересування та приватності.

Таким чином, ІІКС «ГАРТ» є важливим елементом у забезпеченні прикордонної безпеки, а її використання потребує постійного вдосконалення механізмів захисту персональних даних, прозорого контролю за доступом та дотримання міжнародних стандартів у сфері прав людини. Баланс між безпекою держави та захистом персональних даних має бути головним принципом функціонування таких систем.

Контроль щодо осіб, транспортних засобів та вантажів, які перетинають державний кордон України здійснюється Інтегрованою міжвідомчою інформаційно-телекомунікаційною системою «Аркан».

Відповідно до Положення [42] система «Аркан» – це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, приймання, отримання,

передавання, реєстрація, зберігання) щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України та автоматизований доступ до інформаційних ресурсів (баз даних) суб'єктів системи «Аркан». Власником і розпорядником системи «Аркан» є держава в особі АДПСУ.

Система «Аркан» призначена для обробки інформації в інтересах національної безпеки, економічного добробуту, здійснення своєчасного обміну інформацією між суб'єктами системи «Аркан» під час реалізації ними державної політики у сфері охорони державного кордону, міграції, запобігання правопорушенням, захисту прав і свобод людини та для виконання інших повноважень, визначених законодавством.

Відповідно до п. 20 Положення [42] основними завданнями системи «Аркан» є:

- забезпечення обробки інформації між суб'єктами системи «Аркан» в режимі реального часу;

- здійснення між суб'єктами системи «Аркан» електронного інформаційного обміну з використанням кваліфікованого електронного підпису чи печатки з метою оперативного виконання завдань, покладених на них законодавством, зокрема в інтересах національної безпеки та економічного добробуту;

- надання уповноваженими державними органами в установленому законодавством порядку доручень ДПСУ щодо осіб, які перетинають державний кордон.

Функціями системи «Аркан» є:

- забезпечення обміну між суб'єктами системи «Аркан» інформацією щодо осіб, транспортних засобів та вантажів, які перетинають державний кордон, а також іншими електронними інформаційними ресурсами, необхідними для виконання суб'єктами такої системи їх повноважень, визначених законодавством;

- забезпечення обробки у режимі реального часу запитів/відповідей до інформаційних ресурсів суб'єктів системи «Аркан», що передаються з

використанням веб-додатка захищеними каналами національної системи конфіденційного зв'язку або через Інтернет з використанням засобів криптографічного захисту інформації чи іншими захищеними каналами зв'язку;

- здійснення віддаленого доступу до інформаційних ресурсів суб'єктів системи «Аркан» за допомогою прикладного програмного інтерфейсу (API);

- поповнення інформаційних ресурсів суб'єктів системи «Аркан» у режимі обробки повідомлень;

- забезпечення двосторонніх інформаційно-комунікаційних зв'язків між суб'єктами системи «Аркан»;

- здійснення обміну електронними даними з використанням кваліфікованого електронного підпису чи печатки між суб'єктами системи «Аркан»;

- розмежування прав доступу та надання контрольованого доступу користувачам до системи «Аркан»;

- забезпечення резервного копіювання, зберігання та захисту інформації, що міститься в системі «Аркан»;

- забезпечення кіберзахисту в системі «Аркан».

Суб'єкти управління системою «Аркан» можуть забезпечувати доступ підпорядкованим підрозділам до інформації, яка може бути передана засобами системи «Аркан», цілодобово захищеними каналами зв'язку з використанням механізмів криптографічного захисту інформації з можливістю перегляду, пошуку інформації з використанням поширених веб-оглядачів та веб-редакторів.

Слід зазначити, що в інформаційно-комунікаційній системі «Аркан» обробляється службова інформація, тобто інформація з обмеженим доступом, за винятком тієї, що становить державну таємницю, що сприяє ефективному виконанню службових завдань та забезпеченню контролю над державним кордоном України.

На нашу думку, «Аркан» є важливим інструментом у сфері прикордонного контролю, що забезпечує оперативний обмін даними між державними органами та підрозділами ДПСУ. Її функціонування спрямоване на підвищення

ефективності охорони державного кордону, протидію незаконній міграції та правопорушенням, а також на захист прав і свобод громадян. Особливе значення має складова захисту персональних даних, адже система працює з великими масивами службової інформації, що потребує високого рівня конфіденційності та кіберзахисту.

Серед позитивних сторін використання «Аркан» варто виділити:

- оперативність та ефективність – забезпечення обмін інформацією в режимі реального часу між суб'єктами системи;

- захист даних – використання криптографічних засобів, кваліфікованого електронного підпису та захищених каналів зв'язку;

- прозорість та контроль – розмежування прав доступу, ведення журналів аудиту, резервне копіювання та моніторинг інформаційних потоків;

- комплексність – охоплює дані про осіб, транспортні засоби та вантажі, що дозволяє формувати цілісну картину прикордонних процесів;

- національна безпека – сприяє своєчасному реагуванню на загрози та запобіганню правопорушенням у прикордонній сфері.

Серед негативних сторін використання «Аркан» варто виділити:

- загроза витоку персональних даних – у разі порушення кіберзахисту можливий несанкціонований доступ до конфіденційної інформації;

- технічна залежність – складність системи потребує постійного оновлення програмного забезпечення та високих матеріально-технічних ресурсів;

- людський фактор – ризики зловживання правами доступу або неналежного використання даних окремими користувачами;

- вразливість до кібератак – у сучасних умовах війни інформаційна інфраструктура є потенційною мішенню для противника;

- потенційне обмеження прав людини – надмірне накопичення та використання персональних даних може створювати ризики для свободи пересування та приватності.

Таким чином, система «Аркан» є важливим елементом цифрової трансформації ДПСУ, адже вона значно підвищує ефективність контролю та

безпеки, але водночас вона потребує постійного удосконалення механізмів захисту персональних даних, з метою уникнення ризиків витоку інформації та забезпеченням балансу між інтересами держави і правами громадян.

Відповідно до положень Інструкції [43], зазначено, що черговий інформаційно-комунікаційних систем (надалі – черговий ІКС) – це прикордонний наряд у складі одного та більше прикордонників, який призначений для забезпечення цілодобового функціонування та обслуговування технічних засобів електронних комунікацій, програмно-технічних комплексів (надалі – ПТК), автоматизованих робочих місць посадових осіб підрозділу охорони кордону, пункту управління системи оптико-електронного спостереження та інших компонентів інформаційно-комунікаційних систем.

Варто зазначити, що черговий ІКС, повинен знати склад, призначення, тактико-технічні характеристики, будову, правила експлуатації, функціональні можливості і принцип роботи технічних засобів електронних комунікацій, ПТК інформаційно-комунікаційних систем, установлених на об’єктах інформаційної інфраструктури, порядок надання доступу до інформації, що обробляється в інформаційно-комунікаційних системах.

Також в даній Інструкції зазначається, що під час виконання завдань черговий ІКС зобов’язаний:

- здійснювати постійний моніторинг стану баз даних ПТК, виконувати функції адміністрування ПТК та компонентів локальної обчислювальної мережі об’єкта інформаційної інфраструктури (у частині, що їх стосується);

- підтримувати технічні засоби електронних комунікацій та ПТК інформаційно-комунікаційних систем у робочому стані;

- надавати доступ до роботи на відповідних автоматизованих робочих місцях складу зміни прикордонного наряду та визначеним посадовим особам;

- здійснювати контроль за дотриманням посадовими особами – користувачами ПТК правил експлуатації автоматизованих робочих місць та периферійного обладнання;

- здійснювати організаційно-технічні заходи із реагування на різні види подій у кіберпросторі;

- вести облік роботи технічних засобів електронних комунікацій та ПТК інформаційно-комунікаційних систем;

- суворо дотримуватись вимог щодо забезпечення передачі документальних повідомлень, обміну інформації, правил техніки безпеки, технічного захисту інформації, заходів пожежної безпеки.

У службовій діяльності черговий ІКС, керується нормативно-правовими актами та актами організаційно-розпорядчого характеру, що регламентують використання технічних засобів електронних комунікацій, інформаційно-комунікаційних систем та організацію оперативно-технічної служби на вузлах зв'язку у ДПСУ.

Варто зауважити, що забезпечення цілодобового функціонування ІКС прикордонними нарядами є важливим елементом ефективної діяльності ДПСУ. Черговий ІКС відповідає за підтримання технічних засобів у робочому стані, адміністрування програмно-технічних комплексів, моніторинг баз даних та реагування на кіберінциденти. Така діяльність гарантує безперервність здійснення прикордонного контролю та підвищує рівень захисту інформації, зокрема персональних даних, що обробляються в системах ДПСУ.

Таким чином, ІІКС «ГАРТ» та «Аркан» є важливими інструментами ДПСУ для здійснення ефективного прикордонного контролю у сфері охорони державного кордону України, оскільки вони забезпечують автоматизовану перевірку осіб і транспортних засобів, формування баз даних із персональними даними, а також комплексний захист інформації у сфері прикордонної безпеки, як аспекту національної безпеки загалом. Їх використання підвищує рівень забезпечення національної безпеки та протидії незаконній міграції, проте водночас створює ризики для конфіденційності персональних даних, що потребує постійного вдосконалення механізмів їх захисту.

2.3. Адміністративно-правові механізми запобігання порушенням щодо захисту персональних даних в умовах гібридного збройного конфлікту

Початок третього тисячоліття ознаменувався бурхливим розвитком інформаційних технологій (надалі – ІТ). Проте такий розвиток має, окрім позитивного впливу на суспільне життя, ще й негативний – інформаційна безпека опинилася під загрозою. Вказані процеси створили більші можливості для збору, обробки та використання персональних даних. Інформація використовується як інструмент скоєння правопорушень, також активно використовується в політиці і ведені інформаційних війн.

На сьогодні саме персональні дані та інформація є об'єктом ведення гібридного збройного конфлікту Російської Федерації (надалі – РФ) проти нашої держави. Як зазначає О. М. Бойко, ефективність системи захисту персональних даних та взагалі інформаційної безпеки забезпечується правовими інструментами, зокрема імплементації міжнародних та європейських стандартів захисту персональних та діяльністю уповноважених органів у цій сфері. Окрім цього, не менш важливим фактором інформаційної безпеки є рівень правової культури та обізнаність громадян у цих питаннях [44, С. 57].

Т. О. Гуржій зазначає, що досконала правова база оптимізує та зміцнює сферу інформаційних відносин, роблячи її толерантною до внутрішніх і зовнішніх загроз, оскільки рік у рік зростає кількість випадків несанкціонованого доступу та використання конфіденційної інформації, зокрема персональних даних [45, С. 60].

В умовах гібридного збройного конфлікту безпека персональних даних стає особливо важливою, оскільки кібератаки, фішингові схеми, викрадення особистих даних та фінансових ресурсів – усе це частина гібридної війни, яка загрожує не лише державним установам, а й громадянам, волонтерам, журналістам і громадському сектору загалом.

За численними повідомленнями в засобах масової інформації громадяни України постійно піддаються хакерським атакам з боку ворожих кіберзловмисників. Як зазначає Уповноважений Верховної Ради з прав людини

(надалі – Уповноважений) мають місце надсилання електронних листів, повідомлень у месенджерах від начебто державних органів, банків, служби безпеки тощо з рекомендаціями перейти за вказаними в листах / повідомленнях посиланнями. Після завантаження вкладеного файлу зловмисники мають змогу отримати доступ до персональних даних, що містяться на електронному пристрої користувача (контактів телефонної книги, файлів персонального комп'ютера тощо) [46].

Наприклад, під час здійснення контролю за додержанням законодавства про захист персональних даних Уповноваженим виявлено факти шахрайських дій під виглядом виплати грошової допомоги українцям під час воєнного стану.

Такий вид шахрайства як «фішинг в Інтернеті», який полягає у крадіжці персональних даних за допомогою підставних веб-сайтів, залишається актуальною проблемою в умовах воєнного стану. Суть фішингу полягає в тому, що ошукана особа повідомляє дані про себе добровільно. Разом із тим, зловмисник у цьому випадку відіграє роль уповноваженої особи державного органу або благодійного фонду тощо. Тепер під виглядом надання державних виплат зловмисники виманюють гроші у громадян також шляхом направлення повідомлень.

Зловмисники здійснюють розсилку електронних листів, повідомлень у месенджерах (Viber, Telegram, WhatsApp), повідомлень в соціальних мережах (Facebook), sms-повідомлень, де інформують про виплату матеріальної допомоги вимушеним переселенцям.

Такі повідомлення містять заклик перейти за наданим гіперпосиланням на певний веб-сайт та заповнити форму персональних даних (ПІБ, телефон, електронну адресу, реквізити банківських карток тощо) для отримання грошової допомоги. Після цього шахраї отримують передані особою персональні дані та привласнюються собі кошти. Щоб не стати жертвою зловмисників необхідно уважно ставитись до отриманих повідомлень і не розголошувати свої персональні дані на сумнівних, неперевірених веб-сайтах [47].

У дослідженні «Української правди» описано такі механізми викрадення персональних даних: «до прикладу, ще в 2017 році, за даними Служби безпеки України (надалі – СБУ) менеджмент компанії «Яндекс Україна» незаконно збирав, накопичував та передавав спецслужбам Російської Федерації (надалі – РФ) персональні дані українських громадян, а саме: особисті дані, рід занять, спосіб життя, місця перебування, проживання, роботи, дозвілля, джерела та розміри доходів, номери телефонів, електронних адрес та акаунтів у соціальних мережах.

Зокрема, передавались дані співробітників правоохоронних та спеціальних органів, військовослужбовців Збройних Сил України (надалі – ЗСУ), інших підрозділів, які беруть участь в антитерористичній операції на сході України, працівники органів державної влади та управління.

Відповідна інформація передавалася для планування, організації та проведення розвідувальних, диверсійних, інформаційно-підривних операцій в нашій країні на шкоду суверенітетові України, територіальній цілісності та недоторканості» [48].

У червні 2022 року СБУ на своєму офіційному сайті повідомила, що провела багатоетапну спецоперацію, щоб знешкодити агентурну мережу ФСБ, яка вела розвідувально-підривну діяльність в органах державної влади України. У результаті цієї операції затримано осіб, які займали посади – завідувача відділу Секретаріату Кабінету Міністрів України та керівника однієї з дирекцій Торгово-промислової палати. Ці посадовці передавали до країни-агресора інформацію: від стану обороноздатності до облаштування держкордону та персональних даних українських правоохоронців. Вони робили це не безкоштовно, їм платили за інформацію від 2 до 15 тисяч доларів за завдання. Суми залежали від рівня таємності й важливості зібраних даних. Секретні документи зловмисник роздруковував, фотографував і зберігав на флеш-накопичувачах. Для передачі файлів домовлявся через закритий телеграм-канал про зустріч зі своїм «зв’язковим» - одним з працівників Торгово-промислової палати. За даними слідства урядовець передавав файли через зашифровані канали зв’язку [49].

У червні 2023 року Державне бюро розслідувань (надалі – ДБР) повідомило про підозру працівнику органу правопорядку в Тернопільській області, який незаконно збирав персональні дані добровольців Сил територіальної оборони Збройних Сил України та членів їхніх сімей. Згодом ця інформація була оприлюднена на одному з російських ресурсів. Підозрюваний систематизував і зберігав імена військових, дати їх народження, місце реєстрації та проживання, наявність у власності рухомого та нерухомого майна, вогнепальної зброї та спецзасобів, контактні номери телефонів родичів. ДБР не зазначило, з якою метою збиралися ці дані та як надалі використовувалися, зокрема як потрапили до російських пропагандистів, але сам факт несанкціонованої обробки може мати значні наслідки [50].

На нашу думку, щоб не стати жертвою кіберзловмисників необхідно уважно ставитись до електронних листів від незнайомих адресатів, повідомлень у месенджерах (Viber, Telegram, WhatsApp) з невідомих номерів телефону, а також повідомлень в соціальних мережах (Facebook) від незнайомих користувачів. У разі їх надходження не відкривати підозрілі посилання та не завантажувати вкладені файли. Відкриття таких посилань або файлів може спричинити завантаження шкідливого програмного забезпечення на пристрій і отримання доступу до персональних даних.

Представники Національної команди реагування на кіберінциденти, кібератаки та кіберзагрози (надалі – CERT-UA) рекомендують користуватись перевіреними джерелами інформації – наразі це офіційні сторінки державних органів України, які оприлюднюють інформацію та посилання на сервіси щодо знаходження прихистку, розшуку зниклих, отримання допомоги, проведення евакуації тощо. Щоб вберегти свої персональні дані рекомендується зробити резервні копії документів, фото, телефонної книги, які необхідно зберігати у надійному місці. Також доцільно виписати номери телефонів найближчих членів родини. Це допоможе не втратити зв’язок з найдорожчими навіть якщо буде втрачено контроль над пристроєм [51].

У контексті випадків з витоками персональних даних потрібно також згадати про створення єдиного державного реєстру призовників, військовозобов'язаних та резервістів, який наповнюється шляхом взаємодії з іншими системами, базами даних про громадян [52], з метою прискорення процесу актуалізації даних про призовників, військовозобов'язаних і резервістів.

Зокрема, Кабінет Міністрів України (надалі – КМУ) постановою [53] передбачив проведення звірки персональних даних про фізичних осіб. Для цього було доручено провести верифікацію інформації про осіб на підставі даних, що обробляються в державних інформаційних ресурсах, а саме:

- Єдиному державному демографічному реєстрі;
- Державному реєстрі фізичних осіб - платників податків;
- Державному реєстрі актів цивільного стану громадян;
- реєстрі застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування;
- Єдиній інформаційній базі даних про внутрішньо переміщених осіб;
- відомчій інформаційній системі Державної міграційної служби.

Така інформаційна взаємодія між різними відомствами є необхідним заходом для організації мобілізаційних питань та обороноздатності країни. Проте також важливо наголосити, що при ухваленні подібних рішень обов'язково потрібно враховувати чинне законодавство України з питань захисту персональних даних, наявну систему державного контролю в цій сфері, стан інформаційної безпеки державних систем й організацію роботи з конфіденційною інформацією загалом, зокрема широкий спектр ризиків, які існують сьогодні [54, С. 27].

В умовах ведення гібридного збройного конфлікту збільшується кількість правопорушень у сфері персональних даних, оскільки РФ використовує сьогодні технології ШІ та тестує нейромережі, здатні в реальному часі генерувати фейкові новини, імітувати голоси українських військових і створювати deepfake-відео «свідчень» для вкидів через соцмережі [55].

Фейки, створені за допомогою технологій ШІ, стали потужною зброєю, яка використовується для дезорієнтації, маніпуляцій і підриву довіри до правдивої інформації. Російські пропагандисти за допомогою ШІ створюють фейкові новини, що виглядають достовірно, але насправді вони не відповідають дійсності, наприклад, повідомлення про «масові втрати» чи «здачу позицій» українських військових [56].

Технології ШІ також дозволяють створювати [56] deepfake-фото, відео чи аудіо, що створюється за допомогою алгоритмів машинного навчання, і повністю відтворює зображення чи відеозображення людини, фактично створює фейковий матеріал [57]. Це можуть бути підроблені відео, на яких нібито українські лідери закликають до капітуляції або роблять інші заяви, або зображення з «доказами» певних подій, яких насправді не було. Це можуть бути кадри за підготовленим сценарієм або повністю згенеровані фото, які використовують для дискредитації української армії чи волонтерів. Такі матеріали можуть викликати паніку серед населення [56].

До прикладу, показовою є ситуація коли мери Берліна, Відня, Мадрида, Будапешта та Варшави провели дзвінок із неправомірним використанням зображення мера Києва В. Кличка, створивши тим самим діпфейкове відео з недостовірною інформацією. Зловмисники створили віртуального двійника мера Києва за допомогою технології deepfake, а перед цим самостійно домовились про дзвінок. Мер Берліна Франциска Ґіффай в ході розмови відключилась, бо через дивні прохання мера запідозрила, що з ним щось не так. А от Міхаель Людвіг бургомістр австрійської столиці не зрозумів, що з ним вів розмову не справжній В. Кличко, і одразу після розмови написав про неї у соціальних мережах [57].

Фейкові новини про поразки України чи вигадані злочини поширюються з метою, щоб зламати бойовий дух українців та деморалізувати суспільство, адже через велику кількість фейків люди можуть почати сумніватися навіть у реальних подіях, а це може підривати єдність суспільства.

З метою дезінформації міжнародної спільноти РФ використовує фейки створені за допомогою технологій ШІ, щоб переконати інші країни у своїй

правоті та виправдати свої злочини. Оскільки збройний конфлікт – це не лише боротьба на полі бою, а й комплексна інформаційно-психологічна операція, саме тому РФ активно використовує інформаційні маніпуляції, щоб заплутати українців і міжнародну спільноту, поширюються фейки, які викликають недовіру до ЗСУ, уряду або волонтерів [58].

Варто зауважити, що ШІ в епоху цифровізації людства широко впроваджується всюди: від побуду, користувацького досвіду в мережі Інтернет й електронної комерції до забезпечення правопорядку, правосуддя, оборонної сфери та навіть дипломатії. Так, Урядом України поставлена мета створити цифрову державу, де штучний інтелект – важлива частина цього завдання [59].

Водночас, враховуючи чітку вірогідність ризиків, пов'язаних з цифровими аватарами, наприклад, широке поняття кризи згоди, яке теж відноситься до необхідності надання однозначно закріпленої згоди людини на обробку її зображення (біометричних даних), а також можливість створення цифрової підробки аватара та поширення дезінформації серед суспільства. Саме тому уряд передбачає загрози і закріплює за аватаром QR-код. З іншого боку, в такому випадку повинна впроваджуватися обізнаність серед населення щодо перевірки ШІ-технологій, які використовує влада [60, С. 49].

Інший український інноваційний продукт на базі ШІ – приклад біометричної ідентифікації через сервіс, який за системи стеження за очима веб-камери ідентифікує, аналізує та записує процес читання [61]. Однак, ай-трекінг, як технологія аналізу поведінки людини, що лежить в основі програми, може створювати окремі ризики для приватності персональних даних, які система використовує [60, С. 49]. Зокрема йдеться про можливість надмірного збору біометричних та поведінкових характеристик, що дозволяють відтворювати індивідуальний профіль користувача, адже така інформація може бути використана не лише для освітніх чи дослідницьких цілей, але й для комерційного таргетингу або навіть маніпуляцій у сфері інформаційної безпеки.

Оскільки персональні дані являються важливим інструментом роботи технологій ШІ й об'єктом особливої правової охорони, то наразі виникає

необхідність правового врегулювання ШІ таким чином, щоб в основі забезпечення розвитку технології стояла перш за все гнучкість, етика, прозорість та безпека.

У 2021 році ЮНЕСКО прийняло Рекомендацію [62] щодо етики використання ШІ за одинадцятьма сферами стратегічної дії, одна з яких політика даних, і саме цей сектор містить вимоги щодо захисту конфіденційності у системі штучного інтелекту. Одними з таких вимог є: прозорість, гарантії конфіденційності, належний рівень захисту, підзвітність, можливість видалення персональних даних, узгодженість із законодавством про захист даних та ефективний незалежний нагляд.

Україна прийняла цю Рекомендацію і поступово впроваджує її через Дорожню карту з регулювання ШІ, яка має підготувати компанії та громадян до майбутнього закону-аналога Акту ЄС про ШІ через наступні позазаконодавчі заходи: регуляторна пісочниця як контрольований простір для компаній-розробників ШІ створити безпечний продукт; оцінка ризиків, добровільне маркування систем ШІ, Біла книга, кодекси поведінки тощо. Можливі труднощі, які можуть виникнути при їхньому впровадженні, обумовлюються недостатнім фінансуванням, людським та організаційним ресурсом, що пов’язано в основному з воєнним конфліктом, а також динамічністю суспільних відносин, які постає необхідність врегулювати у сфері ШІ [63, С. 16].

Оскільки збільшується число оскільки кібератак РФ на державні установи України, фішингових схем, викрадення особистих даних, розвиток технологій штучного інтелекту, отже зростає кількість правопорушень у сфері охорони персональних даних, то значної актуальності набувають адміністративно-правові механізми запобігання порушенням щодо охорони персональних даних, особливо в умовах ведення нинішньої гібридної війни.

На думку дослідників, збільшення обсягів інформації вимагає запровадження ефективного механізму правового регулювання суспільних відносин у сфері охорони персональних даних, адже це відповідає вимогам сучасності.

Захист персональних даних станом на сьогодні є однією з основних сфер юридичної діяльності, яка має на меті захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, пов'язаного з обробкою [64, С. 190] та використанням персональних даних.

Вирішення питання забезпечення безпеки приватності персональних даних в усіх сферах життєдіяльності людини, а особливо у сфері охорони державного кордону України, суспільства і держави в умовах гібридного збройного конфлікту та євроінтеграції України постає одним із найважливіших чинників становлення та розвитку правової системи України [65].

Органи державної влади, органи місцевого самоврядування, підприємства, установи і організації усіх форм власності, фізичні особи – підприємці, фізичні особи, що провадять незалежну професійну діяльність, які обробляють персональні дані, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. Варто зауважити, що використання персональних даних здійснюється у разі створення умов для захисту цих даних.

Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом [66, С. 4].

Також відповідно до «Типового порядку обробки персональних даних» [67] (надалі – Типовий порядок), затвердженого наказом Уповноваженого Верховної Ради України з прав людини (надалі – Уповноважений), володільці, розпорядники персональних даних самостійно визначають порядок обробки персональних даних, враховуючи специфіку обробки персональних даних у

різних сферах, відповідно до вимог, визначених Законом [68] України «Про захист персональних даних» та Типовим порядком.

Обов’язково мають бути вжиті заходи щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Володільці, розпорядники персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних та інформаційної безпеки.

Організаційні заходи мають охоплювати:

- визначення порядку доступу до персональних даних працівників володільця/розпорядника;

- визначення порядку ведення обліку операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них;

- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

- регулярне навчання співробітників, які працюють з персональними даними [67].

Працівники, які мають доступ до персональних даних, мають надати письмове зобов’язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв’язку з виконанням професійних чи службових або трудових обов’язків. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

З метою забезпечення безпеки обробки персональних даних володільцями, розпорядниками мають вживатися спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних. Отже, у разі здійснення обробки персональних даних необхідно створити належні умови для їх захисту.

Серед правових підстав для обробки персональних даних, які визначені у частині першій статті 11 Закону України «Про захист персональних даних» [68], у даному випадку необхідно виділити: згоду суб'єкта персональних даних на обробку його персональних даних (пункт 1), укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних (пункт 3) та захист життєво важливих інтересів суб'єкта персональних даних (пункт 4).

По своїй суті така підстава для обробки персональних даних як захист життєво важливих інтересів суб'єкта персональних даних може застосовуватись у виключних випадках за умови об'єктивної неспроможності особи надати згоду на обробку персональних даних (наприклад, перебування без свідомості) у поєднанні з необхідністю надати їй допомогу для захисту її життєво важливих інтересів.

Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим. Згода суб'єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

У сфері охорони державного кордону України згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки.

Враховуючи викладене, згода на обробку персональних даних має відповідати таким вимогам:

- добровільність – означає відсутність прямого або опосередкованого примусу при її наданні;

- поінформованість – означає, що перед наданням згоди суб'єкт повинен отримати достовірну інформацію про те, ким, з якою метою будуть оброблятися його персональні дані, кому будуть передаватися, які саме дані, а також про права, визначені Законом;

- форма надання згоди може бути будь-якою – означає, що умови згоди на обробку персональних даних можуть бути викладені у формі єдиного письмового документа, викладеного доступною для суб'єкта персональних даних мовою, що підписується ним особисто або його законним представником, у електронній формі проставивши відмітку про надання згоди, або ж навіть усно.

Водночас надана згода не повинна викликати сумнівів в її однозначності і володілець повинен мати змогу підтвердити її наявність упродовж усього часу здійснення обробки персональних даних. Разом з тим необхідно враховувати пропорційність обсягу персональних даних суб'єкта. Оброблятися повинні лише ті дані, обробка яких необхідна для досягнення мети. Все залежить від критеріїв, за якими відбувається надання матеріальної чи іншої благодійної/гуманітарної допомоги (категорії суб'єкта, стану здоров'я, матеріального забезпечення, сімейного статусу, кількості дітей тощо).

Таким чином, в умовах гібридного збройного конфлікту, захист персональних даних від випадкової втрати, незаконної обробки та незаконного знищення чи доступу до них є вкрай важливими, адже обробка персональних даних має здійснюватися з урахуванням викладених вище положень законодавства України. Така обробка має бути пропорційною та здійснюватися для конкретних і законних цілей [66, С. 4].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 2:

1. Правове забезпечення розвитку технологій цифрової економіки та суспільства: колективна монографія / за ред. О. В. Шаповалової, К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2023. 292 С.

2. Король М. Упровадження цифровізації процесів адміністративно-юрисдикційної діяльності у Державній прикордонній службі України. *Migration & Law.* 2025. № 5 (2). С. 87–102. URL: http://doi.org/10.32752/2786-5185-2025-5-3-87-102

3. Сидоренко Н., Пакулова Т., Наумик А. Теоретичний та прикладний підхід до реформування системи адміністративних послуг як ключовий фактор переходу України до реалізації концепції «сервісної держави». *Грааль науки.* 2023. № 31. С. 64–67. URL: https://doi.org/10.36074/grail-of-science.15.09.2023.09

4. Зигрій О. Правові виклики цифровізації: український досвід у світовому контексті. *Dictum factum.* 2025. № 1 (17). С. 58–64. URL: https://doi.org/10.32703/2663-6352/2025-1-17-58-64

5. Сандул Я. М. Цифровізація в умовах воєнного стану. Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI ст.: синергія наукових, освітніх та технологічних рішень: у 2 т.: матеріали міжнар. наук. практ. конф. (Одеса, 19 травня 2023р.). 2023. Одеса: Вид-во «Юридика». Т. 2. 828 С.

6. Вжешневська О. М. Поняття та ознаки цифровізації як правової категорії. *Юридичний науковий електронний журнал.*2023. № 6. С. 813–815. URL: DOI https://doi.org/10.32782/2524-0374/2023-6/195

7. Про Національну програму інформатизації: Закон України від 01 грудня 2022 року № 2807-IX. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2807-20#n191 (дата звернення: 24.07.2025).

8. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки: Розпорядження Кабінету Міністрів України від 17 січня 2018 року № 67-р. *Офіційний сайт Верховної Ради України*. URL:

https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#n13 (дата звернення: 24.07.2025).

9. Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 7–18. URL: DOI 10.37772/2518-1718-2022-2(38)-1

10. Шульженко Ф. П., Гришко О. М. Права людини в умовах цифрової трансформації суспільства: теоретико-правовий аналіз. *Київський часопис права.* 2021. № 1. С. 5–10. URL: https://doi.org/10.32782/klj/2021.1.1

11. Череп А., Воронкова В., Череп О. Цифрова трансформація суспільства як необхідна умова його інноваційного розвитку. *Теорія і практика інтелектуальної власності.* № 2. 2022. С. 68–73. URL: https://doi.org/10.33731/22022.259745

12. Перунова О. М. Вплив цифровізації цивільного судочинства на процесуальну форму. *Юридичний науковий електронний журнал.* № 1. 2025. С. 164–166. URL: https://doi.org/10.32782/2524-0374/2025-1/34

13. Маркевич К. Цифровізація: переваги та шляхи подолання викликів. *Разумков центр.* 2021. URL: https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv (дата звернення: 25.07.2025).

14. Україна 2030Е–країна з розвинутою цифровою економікою. *Український інститут майбутнього.* URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення: 25.07.2025).

15. Mehdi Khosrow-Pour. Encyclopedia of Information Science and Technology, Fourth Edition (10 Volumes). IGI Global, june, 2017. P. 8104.

16. Руденко М. В. Цифровізація: категоріальні особливості та специфіка трактування. *Економічний форум.* 2021. № 4. С. 3–13. URL: https://doi.org/10.36910/6775-2308-8559-2021-4-1

17. Сиротін В. Д. Сутність та особливості цифровізації у сфера публічного управління. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2023. № 8. URL: https://doi.org/10.54929/2786-5746-2023-8-02-05

18. Пищуліна О. Цифрова економіка: тренди, ризик та соціальні детермінанти: доповідь. *Центр Разумкова*. 2020. Київ: Видавництво «Заповіт». 274 С. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf (дата звернення: 25.07.2025).

19. Никон О. З. Цифровізація (діджиталізація) системи правосуддя в Україні: теоретико-правові засади: дис. … док-ра філос. юрид. наук. Львів, 2025. 269 С.

20. Дубина М., Козлянченко О. Концептуальні аспекти дослідження сутності діджиталізації та її ролі у розвитку сучасного суспільства. *Проблеми і перспективи економіки та управління.* 2019. № 3 (19). С. 21–32. URL: DOI: 10.25140/2411-5215-2019-3(19)-21-32

21. Кравченко К. В. До питання діджиталізації інституту апеляційного провадження. *Прикарпатський юридичний вісник.*2019. № 4 (29). Т. 2. С. 112–115. URL: https://doi.org/10.32837/pyuv.v2i4(29).445

22. Шлапко Т. В., Старинський М. В., Миргород-Карпова В. В., Висоцький А. І., Шеін Д. С. Правове забезпечення трансформації сфери охорони здоров'я у світлі медичної реформи з огляду на євроінтеграційні процеси. *Аналітично-порівняльне правознавство.* 2021. № 3. С. 141–147. URL: https://doi.org/10.24144/2788-6018.2021.03.27

23. Положення про Міністерство цифрової трансформації України: Постанова Кабінету Міністрів України від 18 вересня 2019 року № 856. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text (дата звернення: 26.07.2025).

24. Державні послуги онлайн. *Офіційний веб-сайт сервісу Дія.* URL: https://diia.gov.ua/ (дата звернення: 26.07.2025).

25. Положення про Єдиний державний вебпортал електронних послуг: постанова Кабінету Міністрів України від 04 грудня 2019 року № 1137. *Офіційний сайт Верховної Ради України*. URL:

https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF/ed20230915#n15 (дата звернення: 26.07.2025).

26. Соколова Г. Б. Деякі аспекти розвитку цифрової економіки в Україні. *Економічний вісник Донбасу*. 2018. № 1 (51). С. 92–96.

27. Visit Ukraine Today. The EES system has been launched in Europe: what Ukrainians need to know before entering the EU. URL: https://visitukraine.today/uk/blog/7008/the-ees-system-has-been-launched-in-europe-what-ukrainians-need-to-know-before-entering-the-eu (дата звернення: 26.07.2025).

28. З 12 жовтня ЄС розпочинає впроваджувати нову біометричну систему контролю EES. *Офіційний сайт Державної прикордонної служби України*. URL: https://dpsu.gov.ua/uk/news/48703-z-12-zhovtnya-yes-rozpochinaye-vprovadzhuvati-novu-biometrichnu-sistemu-kontrolyu-ees (дата звернення: 26.07.2025).

29. На українсько-польському кордоні стартує проєкт eCherha. *Офіційний сайт Кабінету Міністрів України*. URL: https://www.kmu.gov.ua/news/na-ukrainsko-polskomu-kordoni-startuie-proekt-iecherha (дата звернення: 28.07.2025).

30. eCherha. *Офіційний сайт електронної черги на кордоні України***.** URL: https://echerha.gov.ua/ (дата звернення: 28.07.2025).

31. Про затвердження Інструкції з діловодства в Державній прикордонній службі України: Наказ Адміністрації Державної прикордонної служби України від 21 грудня 2020 року № 144.

32. Морохов О. Організаційно-правові засади електронного документообігу інформації з обмеженим доступом. *Migration & Law*. 2024. № 4 (3). С. 74–83. URL: http://doi.org/10.32752/2786-5185-2024-4-3-74-83

33. Литвин М. М. Науково-методологічне забезпечення поетапного реформування системи охорони державного кордону: монографія. Хмельницький: Вид-во НАДПСУ, 2009. 316 С.

34. Шадська У. Захист персональних даних під час війни. Харківська правозахисна група. URL: https://umdpl.info/wp-content/uploads/2023/11/ZPD-v-umovah-vijny.pdf (дата звернення: 09.12.2024).

35. Петрів Ю. П. Інформаційно-аналітичне забезпечення діяльності підрозділів Державної прикордонної служби України *KELM (Knowledge, Education, Law, and Management).* 2019. № 26 (2). С. 171–183. URL: DOI 10.5281/zenodo.35885605

36. Басараб О., Басараб О. Деякі підходи підвищення ефективності функціонування інформаційно-комунікаційної системи Державної прикордонної служби України. *Збірник наукових праць НАДПСУ – Migration & Law.* 2022. С. 63–73.

37. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України: Наказ Адміністрації Державної прикордонної служби України від 30 вересня 2009 року № 810. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/z1086-08#Text (дата звернення: 13.12.2024).

38. Мелінчук Н. Глобальна автоматизована інформаційна система «Гарт» у сфері захисту державного кордону України та Словаччини. *Вісник Львівського університету. Серія: Міжнародні відносини.* 2018. № 44. С. 163–170. URL: http://dx.doi.org/10.30970/vir.2018.44.0.9450

39. Литвин М. М., Єрошин Б. Ф. Методика вибору раціональних значень параметрів прикордонного контролю. *Збірник наукових праць.* 2008. № 42. Ч. II. Хмельницький: Вид-во НАДПСУ. С. 26–30.

40. Про прикордонний контроль: Закон України від 05 листопада 2009 року № 1710-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1710-17#Text (дата звернення: 15.12.2024).

41. Про затвердження Правил перетинання державного кордону громадянами України: Постанова Кабінету Міністрів України від 27 січня 1995 року № 57. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/57-95-%D0%BF#Text (дата звернення: 16.12.2024).

42. Про затвердження Положення про інтегровану міжвідомчу інформаційно-комунікаційну систему щодо контролю осіб, транспортних

засобів та вантажів, які перетинають державний кордон: Постанова Кабінету Міністрів України від 11 лютого 2025 року № 148. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/148-2025-%D0%BF#Text (дата звернення: 12.02.2025).

43. Про затвердження Інструкції про службу прикордонних нарядів Державної прикордонної служби України: Наказ Міністерства внутрішніх справ України від 19 жовтня 2015 року № 1261. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/z1391-15#Text (дата звернення: 12.02.2025).

44. Бойко О. М. Збір персональних даних та інформаційна безпека: адміністративно-правовий аспект. *Європейські перспективи.* 2021. № 2. С. 56–62. URL: DOI 10.32782/EP.2021.2.10

45. Гуржій Т. О. Правовий захист персональних даних: монографія / Гуржій Т. О., Петрицький А. Л. – Київ: Київ. нац. Торг.-екон. ун-т, 2019. 216 С.

46. Щодо захисту персональних даних в умовах воєнного стану (роз'яснення та рекомендації Уповноваженого Верховної Ради України з прав людини). *Інформація і право.* 2023. № 1 (44). С. 193–198.

47. ZMINA. Кібератаки, фішинг, дезінформація: правозахисники зафіксували масштабне зростання загроз у цифровому просторі України. URL: https://zmina.info/news/kiberataky-fishyng-dezinformacziya-pravozahysnyky-zafiksuvaly-masshtabne-zrostannya-zagroz-u-czyfrovomu-prostori-ukrayiny/ (дата звернення: 22.05.2026).

48. Українська правда. СБУ: «Яндекс» передавав персональні дані українців спецслужбам РФ. URL: https://www.pravda.com.ua/news/2017/05/29/7145337/ (дата звернення: 14.02.2025).

49. АрміяInform. СБУ викрила російську агентуру, до якої входили посадовці Кабміну і Торгово-промислової палати України. URL: https://armyinform.com.ua/2022/06/21/sbu-vykryla-rosijsku-agenturu-do-yakoyi-

vhodyly-posadovczi-kabminu-i-torgovo-promyslovoyi-palaty-ukrayiny/ (дата звернення: 18.02.2025).

50. Державне бюро розслідувань. ДБР викрило правоохоронця на незаконному збиранні персональних даних тернопільських тероборонівців, які потім з'явились на російських ресурсах. *Офіційний сайт Державного бюро розслідувань*. URL: https://dbr.gov.ua/news/dbr-vikrilo-pravoohoroncya-na-nezakonnomu-zbirani-personalnih-danih-ternopilskih-teroboronivciv-yaki-potim-zyavilis-na-rosijskih-resursah (дата звернення: 22.02.2025).

51. CERT-UA (Національна команда реагування на комп'ютерні інциденти України). Рекомендації щодо користування перевіреними джерелами інформації та захисту персональних даних. *Офіційний сайт CERT-UA*. URL: https://cert.gov.ua (дата звернення: 22.02.2025).

52. Мамченко Н. В Україні автоматизують і прискорять збір актуальних даних про призовників, військовозобов'язаних і резервістів. URL: https://sud.ua/uk/news/publication/258417-v-ukraine-avtomatiziruyut-i-uskoryat-sbor-aktualnykh-dannykh-o-prizyvnikakh-voennoobyazannykh-i-rezervistakh (дата звернення: 22.02.2025).

53. Про проведення верифікації деяких реєстрових даних: Постанова Кабінету Міністрів України від 30 грудня 2022 року № 1493. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1493-2022-%D0%BF#Text (дата звернення: 01.03.2025).

54. Шадська У. Захист персональних даних в умовах війни. Харківська правозахисна група. URL: https://umdpl.info/wp-content/uploads/2023/11/ZPD-v-umovah-vijny.pdf (дата звернення: 01.03.2025).

55. Коваленко А. Як ШІ змінює інформаційну війну: уроки з України, Китаю та Росії. URL: https://www.liga.net/ua/politics/opinion/shtuchnyy-intelekt-ta-informatsiyna-viyna-maybutnoho (дата звернення: 03.03.2025).

56. Путивльська громада. Як штучний інтелект створює фейки та впливає на війну в Україні. URL: https://putivlska-gromada.gov.ua/news/1737997351/ (дата звернення: 05.03.2025).

57. Петрів О. Дезінформація та штучний інтелект: (не)видима загроза сучасності. URL: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/ (дата звернення: 08.03.2025).

58. Центр протидії дезінформації. ШІ та дипфейки як зброя: рф таргетує дезінформацію під аудиторії. URL: https://cpd.gov.ua/international-direction/yevropa/shi-ta-dypfejky-yak-zbroya-rf-targetuye-dezinformacziyu-pid-audytoriyi/ (дата звернення: 08.06.2026).

59. МЗС України призначило цифрову особу для інформування щодо консульських питань. *Офіційний сайт Міністерства закордонних справ України*. URL: https://mfa.gov.ua/news/mzs-ukrayini-priznachilo-cifrovu-osobu-dlya-informuvannya-shchodo-konsulskih-pitan (дата звернення: 11.03.2025).

60. Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету.* 2024. № 85 (3). С. 47–53. URL: https://doi.org/10.24144/2307-3322.2024.85.3.7

61. EUkraine. Українці створили сервіс, що дозволяє зрозуміти, дочитують чи текст. URL: https://eukraine.org.ua/ua/news/ukrayinci-stvorili-servis-shcho-dozvolyaye-zrozumiti-dochituyut-chi-teksti (дата звернення: 15.03.2025).

62. Рекомендація ЮНЕСКО щодо штучного інтелекту. 43 С. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата звернення: 20.03.2025).

63. Регулювання штучного інтелекту в Україні: бачення Мінцифри: аналітичний матеріал. 2024. 30 С. URL: https://storage.thedigital.gov.ua/files/d/9d/0bbc3a705c821a197bedfcdfe00899d9.pdf

64. Пристай Р. Адміністративно-правовий організаційний механізм захисту персональних даних в ЄС. *Вісник Львівського університету. Серія юридична.* 2024. № 78. С. 190–202. URL: DOI: http://dx.doi.org/10.30970/vla.2024.78.190

65. Пилипчук В. Г., Брижко В. М., Баранов О. А., Мельник К. С. Становлення і розвиток правових основ та системи захисту персональних даних

в Україні: монографія / за ред. Брижка В. М., Пилипчука В. Г. Київ: ТОВ «Видавничий дім АртЕк», 2017. 226 С.

66. Уповноважений Верховної Ради України з прав людини. Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році. *Офіційний сайт Уповноваженого ВРУ з прав людини*. URL: https://ombudsman.gov.ua/storage/app/media/.pdf (дата звернення: 22.03.2025).

67. Про затвердження документів у сфері захисту персональних даних: Наказ Уповноваженого Верховної Ради з прав людини від 08 січня 2014 року № 1/02-14. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 27.03.2025).

68. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 28.03.2025).

РОЗДІЛ 3. УДОСКОНАЛЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

3.1. Сучасні виклики системі захисту персональних даних особи в Україні

У сучасних умовах стрімкої цифровізації суспільства, впровадження штучного інтелекту (надалі – ШІ), питання захисту персональних даних набуває вкрай важливого значення. Стрімкий розвиток інформаційних технологій (надалі – ІТ) не лише відкриває нові можливості для обміну інформацією, автоматизації процесів та підвищення ефективності комунікацій, але й породжує серйозні загрози у сфері інформації. Зокрема, зростає ризик несанкціонованого доступу до конфіденційної інформації, кібератак, шахрайства та неправомірного використання персональних даних, що вимагає впровадження ефективних механізмів їхнього захисту на державному та приватному рівнях.

Забезпечення захисту персональних даних залишається актуальною проблемою сьогодення, адже дедалі більше людей користуються мережею Інтернет, проходять авторизацію на різних ресурсах, використовуючи для цього свої персональні дані, а також дедалі більше різних установ створюють своєрідні бази даних, не завжди дбаючи про їх достатню охорону. Недостатня міра забезпечення безпеки персональних даних у кіберпросторі призводить до надмірної активності кібератак та вчинення різних махінацій із персональними даними [1, С. 252].

З появою всесвітньої мережі, яка є невід’ємною частиною життя багатьох українців, з’явились і проблеми захисту інформації в ній, адже Інтернет та інформаційна безпека несумісні за своєю природою. Відомо, що чим легший доступ в мережу, тим гіршою є її інформаційна безпека. Користувач може навіть не дізнатися, що його дані були скопійовані, змінені або навіть зіпсовані [2, С. 62] чи викрадені.

Технічний та технологічний прогреси створили умови для становлення і розвитку нової формації – інформаційного суспільства, а в подальшому суспільства знань. Динамічний розвиток та впровадження нових інформаційно-

комунікаційних технологій спровокував суттєві соціальні та цифрові трансформації [3, С. 22].

З кожним роком кіберзлочинність стає дедалі складнішою, а методи хакерів усе більш винахідливими [4], оскільки нові загрози у кіберпросторі виникають ледве не щотижня. Стрімкий розвиток технологій ШІ виводить проблему на цілком інший рівень: у недобрих руках ШІ може наробити величезної шкоди та завдати критичних збитків будь-якій організації чи державній установі, оскільки може застосовуватись для найрізноманітніших злочинів: від автоматизованих DDoS-атак, до складного фішингу і соціальної інженерії [5].

Як приклад варто зазначити, що в Україні одна з найбільших кібератак в історії країни сталася 19 грудня 2024 року. Тоді хакери атакували реєстри Міністерства юстиції, перервавши роботу таких важливих інформаційних систем, як Єдиний державний реєстр юридичних осіб, реєстр актів цивільного стану, мобільний застосунок «Дія», державні програми «єОселя» та «єВідновлення», призупинилося бронювання працівників. Це достатньо серйозна атака, адже, за даними дослідження Data Driven, понад 60% українських громадян користуються державними цифровими послугами [6].

Встановлено, що напад був організований російськими хакерами з метою порушення функціонування ключових державних сервісів [7], а саме найбільш активним російським хакерським угрупуванням – групою UAC-0010, яка за даними дослідження Data Driven, пов’язана з Федеральною Службою Безпеки Російської Федерації (надалі – ФСБ РФ) та здійснює близько 15 атак проти України щомісяця, використовуючи в своїй діяльності ШІ [6].

Однак, попри те, що ШІ активно використовується у кібератаках, варто зазначити, що він також допомагає аналізувати величезні обсяги даних, виявляти аномалії, передбачати можливі атаки та швидко реагувати на загрози. До ключових аспектів використання ШІ у боротьбі з кіберзлочинністю варто віднести:

- аналіз великих даних: ШІ здатний аналізувати величезні обсяги даних в режимі реального часу, а це дозволяє йому виявляти підозрілу активність, яку людина могла б пропустити через масштаб інформації;

- автоматизація процесів: ШІ може автоматично реагувати на кіберзагрози без втручання людини, значно скорочуючи час реакції на потенційні атаки;

- виявлення аномалій: ШІ ефективно виявляє незвичну поведінку в мережах, що може свідчити про спроби вторгнення чи хакерської атаки, адже це важливо для запобігання злому систем на ранніх стадіях [4].

Таким чином ШІ відкриває нові можливості в сфері кібербезпеки, забезпечуючи більшу ефективність захисту персональних даних та зменшення часу реагування на кіберзагрози [8].

У контексті глобалізації та становлення цифрової особистості, взаємодія людини з глобальною мережею Інтернет набуває все більшого значення, і протягом останніх десятиліть кількість користувачів істотно збільшилася. Працюючи в середовищі онлайн, особа отримує значну кількість інформації, але при цьому іноді несвідомо стає об’єктом ризику для своїх персональних даних. У сучасному світі захист персональних даних виявляється надзвичайно актуальним питанням, зокрема в контексті їхнього потрапляння до Інтернет мережі та забезпечення їхньої інформаційної безпеки [9, С. 107].

Саме поняття інформаційної безпеки означає стан інформації, при якому система нормально функціонує та забезпечується цілісність, конфіденційність та захищеність персональних даних, а також забезпечення доступу до них [2, С. 62].

Варто виділити три основні принципи, які відносяться до інформаційної безпеки:

- цілісність – запобігання несанкціонованій або незаконній модифікації інформації;

- конфіденційність – стан поводження з інформацією, при якому доступ до неї отримують тільки суб’єкти, які мають на це право;

- доступність інформації означає, що при виникненні потреби авторизованим користувачам може бути забезпечений доступ до певних ресурсів, на яких розміщена ця інформація.

Заходи забезпечення цілісності, конфіденційності персональних даних є важливим елементом у сфері інформаційної безпеки, оскільки Інтернет мережа стала найбільш поширеним джерелом загроз для персональних даних. У сучасному світі практично кожна людина має електронну пошту та, іноді, декілька акаунтів, включаючи особисті та робочі електронні скриньки, а також профілі у соціальних мережах, включаючи професійні. Зламані акаунти можуть призвести до втрати особистих даних, які розміщені на сторінках профілю або передаються через сервіси, включаючи навіть таку важливу інформацію, як паспортні дані.

Захист персональних даних в мережі Інтернет набуває особливої актуальності при врахуванні розвитку електронної комерції, де онлайн-покупки стали поширеним явищем для більшості користувачів [9, С. 107], адже недостатня міра забезпечення безпеки розробниками різних інтернет-ресурсів, відсутність необхідного рівня обізнаності користувачів та навпаки обізнаність шахраїв стають прямими передумовами порушення безпеки персональних даних користувачів [1, С. 254].

В нинішніх умовах питання охорони персональних даних набуває все більшої актуальності, особливо в частині готовності державних структур до захисту величезного обсягу інформації стосовно громадян, яку було зібрано на виконання функцій держави [10, С. 33].

До прикладу, викликом для органів державної влади стало створення в Україні Єдиного державного вебпорталу електронних послуг під назвою «Дія». Згідно із Положенням [11] завданнями його запровадження було зокрема надання громадянам електронних публічних послуг, забезпечення доступу до отримання фінансових послуг та забезпечення через електронний кабінет користувача доступу до інформації з національних електронних інформаційних ресурсів.

На сьогоднішній день кабінет користувача порталу «Дія» фактично виступає агрегатором досить суттєвого обсягу даних щодо громадян України, які отримуються через портал із загальнодержавних реєстрів персональних даних. Ці ризики помножено на дуже велику кількість користувачів – більше 13 млн. з них користуються мобільним додатком, ця цифра стоїть окремо від такої ж кількості користувачів, що взаємодіють з ресурсом через веб-портал [12].

Однак, як запевняв міністр цифрової трансформації М. Федоров у тому, що «Дія» не збирає та не зберігає особисту інформацію про українців, а лише відображає дані, що містяться у державних реєстрах [13] ознайомлення зі змістом веб-ресурсу «Дії», на якому з дотриманням вимог чинного законодавства оприлюднено повідомлення про обробку персональних даних, дозволяє зробити висновок про протилежне: все таки не тільки прізвище, ім’я та по батькові особи, а і серія та номер паспорта, дата народження, зареєстроване або фактичне місце проживання, реєстраційний номер облікової картки платника податків громадянина України а також адреса електронної пошти та номери контактних телефонів таки потрапляють в обробку, яку безпосередньо здійснює розпорядник даних – державне підприємство «Дія» [14].

Варто зазначити, що потреба в обробці наведених персональних даних є зрозумілою, бо їх наявність дозволяє ідентифікувати конкретного користувача та формувати запит до відповідних державних реєстрів із конкретними пошуковими характеристиками [10, С. 34].

Фахове середовище докладно дослідило зміст ресурсів «Дії» і дійшло висновку, що зазначений масив даних – це лише перша частина того, що зберігається в «Дії», насправді ресурс значно масивніший. У ньому є ще два додаткових архіви: один містить фото різних документів користувачів: паспортів, трудових книжок, свідоцтв про шлюб тощо, інший – слабоструктурована база записів з різноманітними даними: як з основною задекларованою для офіційної обробки персональною інформацією, так і з додатковою, наприклад інформація про запит на отримання батьківської допомоги, до прикладу – комплексна електронна публічна послуга «єМалятко»,

заяви на реєстрацію фізичної особи підприємця (надалі – ФОП) та квитанції про оплату послуг [15].

Такий стан речей, коли висловлювання міністра суперечать даним вебпорталу його ж відомства, а сам портал лише частково відповідає вимогам законодавства щодо прав суб'єктів персональних даних на отримання інформації про їхню обробку, викликає сумніви щодо виправданості довіри громадян до державних онлайн-сервісів та електронних реєстрів, без яких у сучасних умовах обійтися неможливо.

Ця картина цілком корелює із результатами такого ж ставлення до захисту персональних даних і суб'єктів приватного права: час від часу медіапростір розбурхують повідомлення про витік інформації з того чи іншого ресурсу, при чому причиною цих повідомлень стають не зізнання володільців і розпорядників даних, а конкретні пропозиції із продажу величезних масивів інформації на чорному ринку [16], пропозиції із надання нелегальних послуг зі збору даних про конкретну особу через месенджери, або в кращому випадку звіти правоохоронців щодо їх реакції на витоки [17].

Активність протиправних елементів кіберспільноти не оминула і ресурсу «Дія». У січні цього року з'явились повідомлення виставлення на продаж на форумі RAID за $ 15 000 особистих даних двох мільйонів громадян, що зберігались сервісом «Дія». Мова йшла про індивідуальні податкові номери, номери телефонів, дані паспортів та банківських карток, а також фото документів. Крім того, на підтвердження джерела даних було одночасно виставлено на продажу закриту інформацію державного підприємства «Дія» та всі файли структури порталу «Дія» [18]. За повідомленнями IT – середовища ціна цієї бази даних досягла $ 80 000, після чого посилання на продажу стало недійсним, що вірогідно свідчить про успішну угоду [15].

М. Федоров, у відповідь на дану ситуацію, заперечив наявність персональних даних на веб-порталі «Дія» і запевнив, що даний витік пов'язаний із базами даних «одного популярного банку». У якості заходів реагування Міністерство цифрової трансформації вирішило запустити у додатку «Дія»

найближчим часом послугу «єЗахист», завдяки якій кожен користувач зможе дізнатися про базові правила кібербезпеки, а також в яких реєстрах є інформація про нього [12].

Варто зауважити, що фахове ІТ – середовище не поділяє оптимізму міністра стверджуючи, що викладені на продаж дані є автентичними, отже витік найімовірніше стався з ресурсу «Дія» [15].

Не вдаючись до технічних подробиць вразливості ресурсу «Дія», які було виявлено після витоку даних, варто зазначити, що найбільшу помилку було допущено з самого початку – з архітектури ресурсу, який має автоматизовані можливості звернення на запит користувача до численних електронних реєстрів. По факту треба вести мову про штучне об'єднання державних реєстрів, що за твердженням правозахисної організації Privacy International, становить серйозну загрозу безпеці даних [19].

Ситуація, коли за одним незмінюваним ідентифікатором користувачу надається доступ до різних за своєю метою збору ресурсів, є прямим порушенням закріплених законодавством України міжнародних принципів обробки персональних даних і ставить під загрозу не тільки конфіденційність, а і цілісність створених за бюджетні кошти величезних масивів необхідної громадянам, суспільству і державі інформації.

І. П. Касперський зазначає, що прийнятний вихід з даної ситуації – зламати конфігурацію централізованого доступу, коли до кожного ресурсу чи реєстру користувач міг би звернутися лише окремо, використовуючи при цьому змінювані за своїм наповненням різні засоби надійної ідентифікації. Це може незначно ускладнити лише швидкість отримання доступу до конкретного ресурсу, проте убезпечить від одночасного витоку величезних масивів персональних даних [10, С. 36].

У травні 2020 року керівник громадського об'єднання «Електронна демократія» В. Фльонц, зробив сенсаційну заяву, що в мережі з'явився «telegram-бот», який оголосив продаж персональних даних громадян України, а саме: електронні адреси, паролі від соціальних мереж, інформацію з державних

реєстрів, ідентифікаційні податкові коди (ІПН) та навіть інформацію з анкет, які громадяни свого часу заповнювали та надавали банківським установам, а головне в продажі знаходилися фотографії документів громадян України**.**

Дану заяву одразу знову ж таки пов'язали з даними 26 мільйонів українців, зареєстрованих у додатку «Дія». У Нацполіції оперативно відреагували на запит та повідомили про відкриття провадження щодо витоку персональних даних.

Також на дані події оперативно відреагували і в Міністерстві цифрової трансформації. Перевірку щодо даного інциденту провели і в Офісі Уповноваженого Верховної Ради з прав людини України (надалі – Омбудсмен) та спільно з Нацполіцією заявили, що інформація щодо витоку персональних даних громадян із цифрового державного сервісу додатку «Дія» не підтвердилася [20].

Надаючи свої персональні дані, ми покладаємося на принцип «privacy by default» – конфіденційність за замовчуванням, тобто особам, чиї дані обробляються не потрібно вживати жодних дій для захисту своєї конфіденційності, адже це має бути забезпечено за замовчуванням. Але, нажаль, не все так просто, бо не завжди вдається забезпечити належний рівень захисту персональних даних, адже зовнішньою загрозою витоку конфіденційної інформації може бути кібератака [21], а внутрішньою загрозою – неналежне зберігання даних, тобто людський фактор.

Оскільки сьогодні будь-хто може придбати персональні дані українців в анонімному інтернеті (надалі – Darknet), у такому собі паралельному інтернеті, який практично неможливо відстежити ні провайдерам, ані спецслужбам, де можна придбати усе, що знаходиться поза законом.

Виникає питання, як персональні дані із закритих баз потрапляють у чат-боти в телеграм каналах, які ними торгують. Як стверджує фахівець із кібербезпеки М. Книш, «закриту інформацію зливають передовсім працівники державних органів. Як правило, працівники органів внутрішніх справ, приходять і фізично вставляють флешку в сервер, або ж надають віддалений доступ необхідній людині. Ця людина викачує усю необхідну базу даних, отримує свої

гроші, як правило, це біткойн або інша криптовалюта та продає ці первинні дані» [22].

Якщо ми говоримо про те, як потрапляють персональні дані у телеграм-канали, про що нещодавно було декілька скандалів, то не через «Дію». Вони потрапляють напряму з Міністерства внутрішніх справ України (надалі – МВС).

Департамент кіберполіції (надалі – ДКНПУ) запевняє, що приватні та державні структури піклуються про свою внутрішню безпеку, адже будь-який витік конфіденційної інформації – це пляма на репутації.

ДКНПУ співпрацює з департаментом внутрішньої безпеки (надалі – ДВБ Нацполіції). Якщо в їхньому підрозділі є інформація про те, що недбалий поліцейський намагається отримати персональну інформацію з баз даних Нацполіції, то ДКНПУ оперативно включається в розслідування, технічно допомагає задокументувати того чи іншого злочинця і надалі спільно з підрозділом ВБ притягує цих осіб до відповідальності – зазначає перший заступник начальника ДКНПУ Сергій Кропива [22].

Варто зазначити, що перші кібератаки на інформаційні системи державних підприємств та установ України було зафіксовано наприкінці 2013 року. Уже тоді більше 22 підприємств та державних установ України були заражені комп'ютерним вірусом який потім отримав назву «Uroboros». Головною метою його було викрадення конфіденційної інформації, в тому числі персональних даних та паролів доступу до інформаційних ресурсів. Основними об'єктами ураження вірусу «Uroboros» були веб-ресурси органів державної влади, в тому числі силових структур, засобів масової інформації та великих промислових підприємств [23].

Необхідно зазначити, що відповідно до ст. 1 Закону [24] кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних

інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

З кожним днем війна в кіберпросторі стає все більшою, адже Російська Федерація (надалі – РФ) здійснює все більше кібератак на державні установи, зокрема, безпосередньо перед вторгненням РФ в Україну, щонайменше шість хакерських угруповань, пов’язані з РФ, здійснили 237 кібератак проти українських підприємств та державних установ. Підготовка до проведення зазначених кібератак проти України розпочалася ще за рік до повномасштабного вторгнення РФ – у березні 2021 року. Експерти наголошують, що деякі атаки також супроводжувалися широкою шпигунською та розвідувальною діяльністю. Віртуальні напади не лише намагалися деградувати системи інституцій в Україні, а й порушити доступ людей до надійної інформації та критично важливих послуг і спробували похитнути довіру суспільства до керівництва України [25].

В той же час, за повідомленнями СБУ, найбільша кількість російських кібератак на ресурси органів державної влади та військового управління України припала саме у ніч повномасштабної вторгнення РФ. Ворог хотів знищити весь кіберзахист України, проте кіберфахівці виявили та нейтралізували понад 120 потужних кібератак на держресурси. Співробітники СБУ знешкодили всі спроби окупантів паралізувати стратегічно важливі українські електронні ресурси або використати їх для поширення пропагандистських матеріалів [26] та запобігли витоку конфіденційної інформації.

Як повідомляє РБК-Україна з посиланням на розвідку Британії, 12 грудня 2023 року, найбільший оператор мобільного зв’язку в Україні, «Київстар», зазнав кібератаки, яка ймовірно, була однією з найбільших підривних кібератак на українські мережі з початку повномасштабної війни.

Ефект від витівки хакерів тривав щонайменше дві доби, вплинувши на мобільні послуги та послуги передачі даних компанії. Зокрема кібератака залишила користувачів мобільного оператора сигналу й можливості користуватись інтернетом. Водночас компанія запевняє у тому, що жодних особистих даних під час атаки не було зламано [27] та не було жодного витоку персональних даних клієнтів компанії.

Однак, попри протидію кібератакам, кіберзлочинці здійснюють і надалі спроби атакувати оборонні підприємства та українських захисників.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, що діє при Державній службі спеціального зв'язку та захисту інформації України (надалі – ДССЗЗІ), зафіксувала нові кібератаки проти українських оборонних підприємств та сил безпеки й оборони. Атака розпочиналася з фішингових листів, які маскувалися під офіційні повідомлення від Українського союзу промисловців і підприємців. У них йшлося про запрошення на конференцію, присвячену переходу продукції вітчизняних підприємств оборонно-промислового комплексу на технічні стандарти НАТО, що проходила 5 грудня 2024 року в Києві.

У листі містилося гіперпосилання «Вкладення містить важливу інформацію для вашої участі». Перехід за цим посиланням та подальше відкриття вкладених файлів могли призвести до інфікування комп'ютера [28] та спричинити виток конфіденційної інформації, а саме персональних даних.

Протягом березня 2025 року у месенджері «Signal» виявлено факти розповсюдження повідомлень з архівами, в яких, нібито, міститься звіт з результатами наради. При цьому, в деяких випадках для підвищення довіри відправка повідомлень може здійснюватися від осіб зі списку існуючих контактів, чиї облікові записи було заздалегідь скомпрометовано.

Використання популярних месенджерів, як на мобільних пристроях, так і на комп'ютерах, значно розширює поверхню атаки, в тому числі за рахунок створення неконтрольованих (в контексті засобів захисту) каналів обміну інформацією.

Таким чином шпигунство за оборонно-промисловим комплексом продовжується й надалі, адже фіксуються непоодинокі випадки здійснення цільових кібератак як у відношенні співробітників підприємств оборонно-промислового комплексу, так й окремих представників Сил оборони України [29].

До сучасних викликів системі охорони персональних даних особи в Україні, окрім вище згаданих викликів для державних структур, а саме кібератак, варто також звернути особливу увагу на соціальну інженерію. Соціальна інженерія стала невід'ємною частиною діяльності кібершахраїв, яка допомагає зловмисникам отримати необхідну інформацію, в тому числі й персональні дані.

Державні установи та оборонні підприємства створюють системи кіберзахисту, орієнтуючись насамперед на технічні вектори атак. Такі системи можуть мати високий рівень захищеності і здаватися надійними, але при цьому залишатися уразливими для однієї з найнебезпечніших загроз – соціальної інженерії, заснованої на маніпуляціях людською свідомістю. За статистикою, сьогодні соціальна інженерія так чи інакше застосовується в 97% націлених атак, при цьому технічні вектори часом взагалі не використовуються або використовуються мінімально [30, С. 46].

Соціальна інженерія – це комплекс заходів спрямованих на маніпулювання користувачами обчислювальної системи, яка може бути використана для отримання несанкціонованого доступу до інформаційної системи [31], з метою розкриття конфіденційної інформації.

Варто зазначити, що згідно ст. 21 Закону [32] конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень та може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, передбачених законом.

В діяльності Державної прикордонної служби України (надалі – ДПСУ) інформація, яка була отримана в процесі здійснення прикордонного контролю,

контррозвідувальної та розвідувальної діяльності, вважається конфіденційною, адже вона має критичне значення для забезпечення національної безпеки та охорони державного кордону України. При цьому саме Законом [32], а не особою визначається, яка саме інформація про фізичну особу, обмежена в доступі, є конфіденційною: дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Оскільки конфіденційна інформація містить дані про оперативно-розшукові заходи, агентурну мережу, технічні засоби розвідки, аналіз загроз та стратегічні рішення, то розкриття такої інформації може становити загрозу прикордонній безпеці та національній безпеці загалом.

За допомогою соціальної інженерії зловмисники можуть підмінювати, викрадати або руйнувати інформацію. В основі соціальної інженерії лежать психологічні методи, які використовуються для того, щоб вплинути на поведінку людей та отримати від них інформацію.

Цей метод досить ефективний, оскільки він спирається на людські слабкості та вразливості.

Соціальна інженерія може проявлятися дуже по-різному. Прикладом атаки, що використовує соціальну інженерію, може бути відправлення електронного листа, який нагадує лист від банку, з проханням вказати свої особисті дані, такі як номер кредитної карти, пароль або іншу конфіденційну інформацію. Ця форма соціальної інженерії називається фішинг.

Іншим випадком соціальної інженерії може бути використання соціальних мереж для отримання інформації про користувачів. Зловмисники можуть створювати фальшиві профілі, щоб отримати доступ до особистих даних користувачів або маскуватися у спілкуванні під колегу чи знайомого.

Іноді зловмисники можуть намагатися використовувати соціальну інженерію, щоб отримати доступ до паролів або іншої конфіденційної інформації для різних деструктивних дій.

Іще одним прикладом соціальної інженерії є підміна особистості – використання інформації про людину, щоб здійснити злочин. Зловмисники

можуть використовувати ім’я, фотографії та інші персональні дані для того, щоб видатися кимось іншим та отримати доступ до персональних даних.

Щоб захистити себе від соціальної інженерії, важливо бути обережним та не довіряти підозрілим повідомленням, електронним листам або іншим формам зв’язку, які містять запити на введення конфіденційної інформації [33].

На нашу думку, сучасні виклики у сфері охорони персональних даних в Україні вимагають комплексного підходу до їх вирішення. Окрім кіберзагроз, значну небезпеку становить соціальна інженерія, яка є потужним інструментом маніпулювання свідомістю користувачів та сприяє витоку конфіденційної інформації. Незважаючи на високий рівень технічного захисту, державні установи та оборонні підприємства залишаються вразливими до цього виду атак.

3.2. Міжнародний досвід правового регулювання захисту персональних даних

У сучасний період суспільство розвивається під впливом інтеграційних, глобалізаційних та інших процесів, до яких варто віднести і інформаційний, а в останнє п’ятиріччя інформаційна сфера стала важливим чинником впливу на розвиток суспільства, а інформатизація всіх сфер суспільної діяльності є основним напрямом державної політики й імперативом розвитку суспільства [34, С. 76], економіки та прикордонної безпеки як аспекту національної безпеки загалом.

Сучасні виклики та загрози пов’язані з нелегальною міграцією, незаконним перетином державного кордону України, контрабандою та іншими загрозами, особливо в умовах глобальної інформатизації, питання охорони та захисту персональних даних набувають особливо важливого значення, зокрема, і у сфері охорони державного кордону України.

Інтенсивний розвиток засобів збору, обробки, зберігання, передачі різних видів інформації, із глобальним наступом віртуального простору, розвитком потужних мереж інформаційно-комунікаційних систем (надалі – ІКС), які здійснюють транскордонні передачі відомостей та коли збільшуються

можливості несанкціонованого доступу до інформації про особу та інших видів інформації, використання якої може завдати шкоду, зокрема, законним інтересам конкретної людини, все більш актуальною стає проблема необхідності захисту конфіденційної інформації про фізичну особу [35, С. 71], а саме її персональних даних.

Захист персональних даних, зокрема міжнародно-правовий досвід у цій сфері, поступово стає предметом широко наукового аналізу. Значна увага приділяється дослідженню правового регулювання персональних даних у Європейському Союзі (надалі – ЄС), що знайшло відображення у численних працях українських правників. У науковому дискурсі розглядаються питання відповідності законодавства України нормам ЄС, а також розглядається практика Суду ЄС щодо принципів захисту персональних даних. На нашу думку, міжнародно-правовий досвід захисту персональних даних посідає важливе місце у сучасних дослідженнях, формуючи ґрунтовну базу для подальшого розвитку національного законодавства.

Однак, у світлі постійного розвитку інформаційних технологій (надалі – ІТ) та розвитку засобів обробки та поширення персональних даних, що впливає на оновлення нормативно-правового регулювання їх захисту, обумовлює подальші дослідження у згаданій сфері [36, С. 644], адже особливої актуальності набувають питання забезпечення балансу між ефективним використанням сучасних технологій та дотримання прав і свобод людини.

Як зазначають науковці П. М. Дуравкін та І. І. Гафич, захист персональних даних вимагає спільних зусиль та співпраці між державними органами, приватним сектором та громадянським суспільством. Важливим кроком на шляху до створення єдиного набору принципів та стандартів, спрямованих на захист персональних даних є розробка міжнародних стандартів та правових норм [37, С. 89] в цій сфері.

У зв’язку із глобалізацією, цифровізацією та розвитком новітніх ІТ, охорона та захист персональних даних стала однією з ключових тем сучасної правової системи. У багатьох країнах приймаються нові закони, або адаптуються

існуючі для захисту персональних даних. Зокрема, ЄС ухвалив Загальний регламент захисту даних (General Data Protection Regulation), який встановлює жорсткі стандарти для захисту персональних даних. Відповідні правила встановлюються не лише в межах ЄС, але й для інших держав, що обробляють персональні дані громадян ЄС. Водночас, Сполучені Штати Америки (надалі – США), Канада та Україна мають різні підходи до регулювання цієї сфери [38, С. 289].

Забезпечення Україною належного рівня захисту персональних даних, відповідно до найвищих європейських та міжнародних стандартів, у цій сфері, безпосередньо впливає на вступ нашою державою до ЄС [39, С. 138].

Станом на початок 2026 року Україна має статус кандидата на вступ до Європейського Союзу. Цей статус був наданий 23 червня 2022 року Європейською радою. Україна офіційно подала заявку на членство у ЄС 28 лютого, на п’ятий день повномасштабного вторгнення Росії.

Президент України Володимир Зеленський заявляє, що метою країни є вступ до Євросоюзу вже до 2027 року, хоча канцлер Німеччини Фрідріх Мерц вважає, що це малоймовірно через тривалість процесу інтеграції.

Отже, наразі Україна має статус кандидата, і тривають підготовчі процеси для повномасштабного членства, яке може відбутися у найближчі кілька років, але точна дата поки ще не визначена.

Враховуючи євроінтеграційний напрямок розвитку України, важливим для нашої країни є досвід правового регулювання функціонування інституту захисту персональних даних саме на європейському континенті [40, С. 58], адже значний досвід провідних країн ЄС, становить практичну цінність для імплементації європейських стандартів охорони та захисту персональних даних у національне законодавство.

На нелегкому та тривалому шляху України до ЄС, 1 червня 2010 року Верховною Радою України (надалі – ВРУ) було ухвалено Закон України «Про захист персональних даних» [41], який набрав чинності 1 січня 2011 року. Його прийняття сприяло Україні ратифікувати Конвенцію Ради Європи «Про захист

прав осіб у зв'язку з автоматизованою обробкою персональних даних» (надалі – Конвенція Ради Європи № 108) [42] та Додатковий протокол до неї (надалі – Додатковий протокол) [43].

Зазначена Конвенція Ради Європи як зазначає В. М. Брижко, є першим у світі, головним та єдиним правовим актом, який визначає основоположні, уніфіковані принципи створення національного законодавства країн світу у сфері захисту персональних даних [44, С. 21]. Відповідно до її положень держава-член Ради Європи має право визначати види персональних даних, які підлягають захисту. В статті 4 зазначено, що кожна Сторона коригує національне законодавство у частині втілення її основних принципів та поставленої мети забезпечення на території держави-члена поваги до прав та основних свобод кожної особи незалежно від її громадянства або місця проживання [42].

Варто зазначити, що вона застосовується до будь-якого процесу обробки даних, що здійснюється як у приватному, так і у державному секторах, зокрема, до обробки персональних даних судовими і правоохоронними органами та захищає особу від зловживань, які можуть виникати при збиранні та обробці персональних даних, її другим завданням є регулювання транскордонної передачі персональних даних.

Що стосується принципів збирання та обробки персональних даних, то Конвенція Ради Європи № 108 [42] вимагає відкритого і законного збирання та автоматизованої обробки персональних даних, які зберігаються для визначених і законних цілей та не використовуються у спосіб, не сумісний із цими цілями, а також не зберігаються довше, ніж це необхідно. А також її принципи стосуються якості даних, зокрема, передбачають, що такі дані повинні бути адекватними, відповідними та не надмірними (пропорційними), а також точними.

Положеннями її статей 5–7 зазначають певні вимоги до захисту персональних даних, а саме:

- їх отримання та обробка мають здійснюватися законним шляхом;

- вони повинні зберігатися та використовуватися у визначених та законних цілях, бути точними та поновлюваними, допускати ідентифікацію особи;

- персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство країни не забезпечує відповідних гарантій (це правило також застосовується до персональних даних, що стосуються засудження у кримінальному порядку);

- засоби та заходи, що застосовують до таких даних, повинні передбачати безпеку персональних даних від випадкового та несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження чи випадкової втрати.

Необхідно заначити, що відповідно до зазначених в ній гарантій, що стосуються збору та обробки персональних даних, Конвенція Ради Європи № 108 [42] забороняє за відсутності відповідних правових гарантій здійснювати обробку чутливих даних, які стосуються расової належності, політичних переконань, здоров'я, релігії, статевого життя або засудження в кримінальному порядку.

Також важливими положеннями її ст. ст. 8, 13 є й ті, що стосуються використання персональних даних, а саме в яких зазначено, що збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, дані про яку обробляються, а також право отримувати відповідні дані без затримки та у зрозумілій формі.

Виходячи з інтересів держави, Конвенція Ради Європи № 108 відповідно до положень ст. 9, допускає обмеження у правах фізичних осіб, якщо це стосується державної чи суспільної безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та основних свобод інших осіб.

Таким чином, Конвенція Ради Європи № 108 стала відправною точкою закріплення регулювання охорони та захисту персональних даних та виокремлення їх у самостійний вид діяльності, оскільки містить основні принципи захисту від неправомірного збирання, обробки, зберігання, поширення персональних даних та базові норми щодо транскордонної передачі даних.

З метою урегулювання та деталізації її положень в частині, що стосується транскордонної передачі даних, 8 листопада 2001 року було прийнято Додатковий протокол [43], який містив нові положення щодо необхідності створення Сторонами Конвенції наглядового органу, який би здійснював контроль за додержанням законодавства про захист персональних даних:

- кожна Сторона призначає один або більше органів нагляду, відповідальний за забезпечення принципів, які містяться у її внутрішньодержавному праві, що втілюють принципи, викладені у Розділах Конвенції та в цьому Протоколі;

- з цією метою вищезазначений орган нагляду має, зокрема, повноваження щодо розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентні судові органи про порушення умов внутрішньодержавного права, що втілюють принципи, викладені у пункті 1 статті цього Протоколу;

- кожний орган нагляду розглядає та приймає рішення щодо заяв будь-якої особи відносно захисту його/її прав і основоположних свобод відносно обробки персональних даних, в межах своєї компетенції;

- органи нагляду виконують свої функції у повній незалежності;

- рішення органу нагляду можна оскаржити у суді у разі, якщо вони викликали скарги;

- відповідно до положень Розділу IV та не впливаючи на положення статті 13 Конвенції Ради Європи № 108, органи нагляду співробітничають між собою в тій мірі, наскільки це необхідно для виконання їхніх обов’язків, зокрема, шляхом обміну будь-якою корисною інформацією.

Оскільки Конвенція Ради Європи № 108 зобов’язує кожну державу-члена призначити один або більше Уповноважених органів нагляду та направити відповідне повідомлення Генеральному секретарю Ради Європи, то завданням інституту Уповноваженого є створення належного організаційно-правового регулювання діяльності щодо захисту персональних даних в країні. Нині

Уповноважені органи з питань захисту персональних даних діють у понад ста країн світу.

Україна, як підписант згаданих Конвенції та Додаткового протоколу до неї зобов'язалася керуватися їх положеннями при розгляді питань, пов'язаних із захистом персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному так і у приватному секторах.

За поданням тодішнього Президента України Віктора Януковича проєкту Закону України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» [45], Верховною Радою України було ратифіковано згадані документи.

З огляду на нові виклики, зокрема пов'язані зі швидким розвитком ІТ, Комітет міністрів Ради Європи у 2011 році ухвалив рішення про початок роботи над оновленням [46, С. 88] Конвенції Ради Європи № 108. Спочатку ця робота була доручена консультативному комітету, а згодом спеціально створеному міжурядовому комітету CAHDATA (англ. ad hoc Committee on Data Protection), який розпочав свою роботу у 2013 році. По завершенню роботи у 2016 році її результати були передані на розгляд Комітету міністрів Ради Європи.

10 травня 2018 року Комітетом Міністрів Ради Європи була ухвалена модернізована Конвенція Ради Європи № 108, яка отримала назву Конвенція 108+ та спрямована на вирішення проблем недоторканості приватного життя, що виникають у зв'язку з використанням нових інформаційно-комунікаційних технологій (надалі – ІКТ), і на зміцнення механізму виконання положень [47].

Вона розповсюджується як на автоматизовану, так і на неавтоматизовану обробку, однак вона не розповсюджується на обробку фізичними особами для власних потреб, адже в ній інтегровано такі принципи як прозорість, пропорційність, підзвітність, мінімізація даних та конфіденційність за дизайном (privacy by design).

Конвенція 108+ [47] розширила права суб'єктів даних, зокрема право на доступ до своїх даних, право на виправлення або видалення неточних даних, право на обмеження обробки та право на переносимість даних. Також вона зобов'язує держав-учасниць упроваджувати ефективні заходи захисту даних і забезпечувати відповідальність контролерів даних.

На нашу думку, ухвалення Конвенції 108+ стало інноваційним, свого часу, адже в ній зазначалося підвищення вимог до міжнародної передачі даних, оскільки вона установлює, що передача даних до третіх країн можлива лише за умови наявності адекватного рівня захисту даних у країні отримувача.

Також варто звернути увагу ще на один нормативно-правовий акт, який пов'язаний із регулюванням сфери захисту персональних даних, а саме на Хартію основоположних прав ЄС [48] (надалі – Хартія), яка була проголошена 7 червня 2016 року. Відповідно до положень ст. 8 Хартії кожному гарантується право на захист своїх персональних даних, а також вона визначає, що дані мають оброблятися чесно, для конкретних цілей і за згодою особи або на іншій законній основі, установленій законом. Це включає зобов'язання забезпечення конфіденційності та безпеки даних під час їхньої обробки. Хартія також передбачає, що кожен має право доступу до зібраних даних, що стосуються його особисто, та право на виправлення таких даних. Це положення підсилює права суб'єктів даних на прозорість та контроль своїх персональних даних, а також констатує, що Хартія є фундаментом для встановлення високих стандартів захисту персональних даних в ЄС.

Подальша імплементація та практична реалізація закріплених у Конвенції Ради Європи № 108 [42] та Хартії [48] принципів зумовили необхідність деталізації у нормативно-правових актах вторинного права ЄС, спрямованих на уніфікацію підходів до обробки персональних даних і забезпечення належного рівня їх захисту.

Слід зауважити, що на рівні ЄС принципи Конвенції Ради Європи № 108 та Хартії були конкретизовані у Директиві 95/46/ЄС Європейського парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та вільним

обігом цих даних» (надалі – Директива 95/46/ЄС) [49], яка була ухвалена 24 жовтня 1995 року. Серед найбільш важливих положень Директиви 95/46/ЄС варто виділити наступні:

- обробка персональних даних має здійснюватися лише за згодою зацікавленої фізичної особи. Під обробкою персональних даних вважаються будь-які дії, чи сукупність дій, які здійснюють чи не здійснюють за допомогою автоматизованих систем, вона включає збирання, реєстрацію, накопичення, зберігання, модифікацію, комбінування, компіляцію, поширення та будь-яку іншу форму дій, що дозволяє мати доступ до персональних даних, а також їх блокування та знищення на носіях інформації;

- положення Директиви 95/46/ЄС застосовують до обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів, а також до обробки неавтоматизованими засобами персональних даних, що є частиною картотеки чи призначені для внесення до картотеки (вона не застосовується якщо обробка персональних даних проводиться фізичною особою під час її діяльності виключно особистого чи побутового характеру);

- фізична особа має бути повідомлена про факт обробки, про передачу її персональних даних третім особам, а також має право на точну та повну інформацію про обставини такої передачі;

- кожній особі гарантується право отримати від контролера підтвердження того, обробляються дані чи ні, які його стосуються, і інформацію, принаймні, про цілі обробки, категорії даних і про одержувачів чи категорії одержувачів, яким надаються дані;

- суб’єкт даних має право заперечувати у будь-який час проти обробки його даних, пов’язаних з конкретною ситуацією, за винятком випадків коли інше передбачено національним законодавством;

- кожна особа має право на те, щоб стосовно неї не приймалося рішення, яке ґрунтується винятково на автоматизованій обробці даних;

- захист персональних даних передбачає використання технічних та організаційних засобів з моменту створення системи їх обробки;

- наглядовий орган повинен вести реєстр операцій із обробки персональних даних;

- кожній людині передбачено право на судовий захист від будь-якого порушення прав, гарантованих національним законодавством, що застосовується до відповідної обробки;

- на одержання компенсації за завдану шкоду та ін.

Загалом цими положеннями Директиви 95/46/ЄС закріплено умови та межі обробки персональних даних, гарантії прав суб'єктів даних, вимоги до автоматизованої обробки й неавтоматизованої обробки, а також обов'язки контролерів і наглядових органів, включно з правом на судовий захист і компенсацію шкоди.

Також необхідно зазначити, що Директива 95/46/ЄС вимагає від держав-членів гарантувати право осіб на недоторканість приватного життя та вимагає забезпечити вільний потік особистих даних в рамках Співтовариства.

Однак, попри те, що Директива 95/46/ЄС була одним із найпрогресивніших документів у сфері захисту персональних даних у світі, IT прогрес та зростання обсягів автоматизованої обробки персональних даних зумовили виникнення нових викликів та вирішення проблем у цій сфері, які потребували додаткової правової регламентації [50, С. 13].

Епохальним документом у сфері захисту персональних даних став «Загальний регламент із захисту персональних даних» (General Data Protection Regulation (EU) 2016/679) (надалі – GDPR) [51], який був прийнятий 26 квітня 2016 року та встановлює правила обробки та вільного руху персональних даних і застосовується до всіх доменів публічного та приватного секторів. Цим регламентом було скасовано Директиву 95/46/ЄС, але були оновлені та модернізовані принципи, закріплені в цій Директиві.

Незважаючи на те, що Україна ще не є державою-учасницею ЄС, правила закріплені в положеннях GDPR, можуть стосуватися безпосередньо суб'єктів, що належать до її юрисдикції. Оскільки відповідно до його положень статті 3 зазначено, що територіальна дія GDPR має екстратериторіальну дію, то його

норми поширюються не лише на держави-члени ЄС, а й на фізичних та юридичних осіб інших країн у конкретних випадках, передбачених GDPR [51].

Варто зауважити, що державам-членам ЄС не потрібно приймати додаткове національне законодавство відповідно до Договору про функціонування ЄС. GDPR є безпрецедентним у світі, адже встановлює дуже посилені вимоги щодо захисту персональних даних, а також встановлює сувору відповідальність за його порушення та право на компенсацію за виявлені порушення [52, С. 204].

Нововведеннями у сфері захисту персональних даних фізичних осіб у ЄС, які були закладені GDPR відповідно до його положень стали:

- право отримувати чітку та зрозумілу інформацію про те, хто обробляє персональні дані, які дані обробляються та чому вони обробляються;

- право доступу до персональних даних, якими володіє суб'єкт даних про фізичну особу;

- право на забуття – фізична особа може вимагати видалення персональних даних, якщо вона не бажає їх подальшої обробки, а суб'єкт даних не має обґрунтованих причин зберігати їх;

- суб'єкт даних у випадках крадіжки або втрати персональних даних повинен повідомити фізичну особу та відповідний орган нагляду за захистом даних, а у випадку невиконання цього положення суб'єкт даних може бути оштрафований;

- посилення захисту дітей в Інтернеті, тощо.

Також варто відмітити, що GDPR закріпив поняття спеціальної категорії персональних даних, а саме «чутливих даних», до яких належать персональні дані, що розкривають расове чи етнічне походження, політичні переконання, релігійні чи філософські переконання чи членство в профспілках, дані про стан здоров'я, дані щодо статевого життя чи сексуальної орієнтації фізичної особи, генетичні дані та обробка біометричних даних з метою ідентифікації фізичної особи.

З іншого боку GDPR встановлює ряд вимог, які застосовуються до суб'єктів даних, а саме:

- суб'єкти даних, які обробляють великі дані у великих масштабах або чиєю основною діяльністю є обробка спеціальної категорії персональних даних, наприклад, даних про здоров'я мають призначити особу, відповідальну за захист даних;

- суб'єктам даних доведеться проводити оцінку впливу, коли обробка даних може призвести до високого ризику для прав і свобод осіб.

Також GDPR пропонуються різні інструменти для передачі даних за межі ЄС, включаючи рішення щодо відповідності, прийняті Європейською комісією, коли країна, що не входить до складу ЄС, пропонує адекватний рівень захисту, попередньо схвалені (стандартні) договірні положення, обов'язкові корпоративні права та кодекси поведінки.

Таким чином GDPR є комплексним і безпрецедентним нормативно-правовим актом, який установлює уніфіковані та посилені стандарти захисту персональних даних, розширює права суб'єктів даних і запроваджує ефективні механізми відповідальності за порушення.

На додаток до GDPR Європейський парламент і Рада 27 квітня 2016 року затвердили Директиву (ЄС) 2016/680 «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця, злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних» (надалі – Директива 2016/680) [53], а також Директиву (ЄС) 2016/681 «Про використання даних записів реєстрації пасажирів (PNP) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» (надалі – Директива 2016/681) [54].

Як зазначає Г. А. Прохазка згадані Директиви, підкреслюючи права громадян на приватність, разом із тим визначають напрями обмеження цього права у зв'язку із потребами захисту інтересів суспільства від злочинних дій [55, С. 153].

У свою чергу О. С. Дяковський зазначає, що в контексті поліцейської діяльності Директива 2016/680 регулює збір, обробку та зберігання персональної інформації, а також вимагає від правоохоронних органів проводити оцінку впливу на захист персональних даних, щоб проаналізувати можливі ризики, оскільки в своїй діяльності правоохоронці широко використовують ІТ [56, С. 268].

Варто зауважити, що положення статті 1 Директиви 2016/680 визначає сферу її застосування, що є вирішальним для чіткого розмежування між нею та GDPR. Для того щоб вона була застосована, обробка персональних даних повинна здійснюватися компетентним органом з метою запобігання, розслідування, виявлення та переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз громадській безпеці і запобігання таким [57].

Щоразу, коли офіцер поліції обробляє дані для цілей, не пов’язаних із правоохоронними органами, і, як один із прикладів, кадрові дані або інформацію, яка підлягає архівації, застосовуватиметься GDPR.

Проте в деяких сферах, де правоохоронні органи мають право обробляти персональні дані, розмежування між Директивою 2016/680 та GDPR не є таким очевидним. До прикладу, це може мати місце в ситуаціях, коли офіцери поліції обробляють персональні дані з метою ідентифікації або перевірки у сфері міграції та прикордонного контролю. Особа, яка незаконно перетинає кордони Шенгенського простору, може бути перевірена офіцерами поліції, і в тих державах-членах, де незаконний перетин кордонів кваліфікується як кримінальний злочин, офіцер поліції може змінити мету обробки персональних даних залежно від того, чи вона здійснюється для міграційних цілей або для кримінального переслідування.

Однак, як тільки нелегальний мігрант подає заяву про надання притулку, розгляд його заяви підпадає під дію GDPR, незважаючи на розпочате кримінальне провадження. Це в свою чергу демонструє складність застосування

компетентними органами двох різних правових режимів залежно від мети обробки персональних даних [57].

Таким чином Директива 2016/680 не передбачає таких прав, які містяться в GDPR, які в першу чергу були розроблені для здійснення комерційної діяльності, таких як право бути забутим або право на переносимість даних, що викликає також складність в реалізації норм вказаних двох джерел права у сфері персональних даних на практиці та утворює проблемні питання у даному напрямі [57].

Необхідно також згадати і Директиву 2002/58/ЄС Європейського Парламенту та Ради щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (надалі – Директива 2002/58/ЄС) [58] яка доповнюючи Директиву 95/46/ЄС [49] та діючи у взаємозв'язку із GDPR [51] і Директивою 2016/680 [53] встановила спеціальні правила щодо конфіденційності комунікацій, використання фалів «cookies», обробки даних трафіку та місцезнаходження, а також обмеження небажаної електронної пошти.

Директива 2002/58/ЄС [58] поширюється як на фізичних, так і на юридичних осіб та зобов'язує постачальників послуг зв'язку дотримуватися суворих стандартів:

- конфіденційність зв'язку – держави члени ЄС повинні заборонити будь-яке несанкціоноване прослуховування, перехоплення чи зберігання телефонних розмов, повідомлень та супутнього трафіку без згоди користувачів;

- правило «cookie law» – веб-сайти зобов'язані інформувати користувачів та отримувати їхню чітку попередню згоду перед збереженням або зчитуванням файлів «cookie» чи іншої інформації на їхніх пристроях;

- захист від спаму – забороняється використання електронної пошти, sms-повідомлень та автоматизованих систем дзвінків для прямого маркетингу без попередньої згоди отримувача;

- безпека послуг – провайдери та оператори повинні вживати технічних заходів для захисту своїх мереж і повідомляти користувачів про специфічні загрози, таких як DoS та DDoS-атаки, а також вірусні атаки;

- дані про місцезнаходження та трафік – дані трафіку мають бути видалені або анонімізовані після завершення сеансу зв'язку, окрім випадків, необхідних для тарифікації чи за згодою клієнта.

На нашу думку, перелічені положення демонструють, що Директива 2002/58/ЄС [58] встановлює комплекс спеціальних гарантій у сфері електронних комунікацій, які охоплюють як технічні, так і організаційні аспекти захисту персональних даних.

Таким чином, хоча Директива 2002/58/ЄС [58] і має спеціалізовану сферу застосування, але разом із GDPR [51] та Директивою 2016/680 [53] формує багаторівневу систему адміністративно-правового регулювання захисту персональних даних.

У цьому контексті важливим є звернення до актів Ради Європи, які деталізують правила захисту персональних даних у спеціалізованих секторах, зокрема у сфері правоохоронної діяльності.

Варто також звернути увагу і на рекомендації № R (87) Комітету Міністрів Ради Європи «Про захист персональних даних у секторі поліції» 1987 року (надалі – Рекомендації № R (87)) [59], які визначають основні положення щодо захисту персональних даних, котрі входять до відання правоохоронних органів, зокрема:

- дотримання принципу контролю за обробкою персональних даних правоохоронними органами, який має здійснюватися незалежним органом державної влади, діяльність якого не пов'язана з діяльністю поліції, на цей же наглядовий орган може бути покладена функція реєстрації файлів (масивів) персональних даних, що будуть оброблятися поліцією;

- дотримання принципу меж збору персональних даних, у національному законодавстві повинні бути введені детальні правила і гарантії від зловживань, особлива увага повинна приділятися обробці даних, що розкривають расову або

етнічну приналежність, релігійні переконання, політичні погляди або сексуальне поводження; відомості про сексуальне поводження можуть збиратися лише для розслідування вже зроблених злочинів;

- дотримання принципу класифікації даних отриманих з надійних джерел, від ненадійних; про зроблені злочини; про підготовку до здійснення злочинів; ці дані повинні зберігатися окремо від даних, зібраних для адміністративних цілей, у тому числі і про адміністративні правопорушення;

- необхідності використання даних лише в поліцейських цілях, тобто для запобігання або припинення злочинів або підтримки суспільного порядку;

- необхідності регламентації права на ознайомлення і виправлення помилкових даних по відповідній процедурі;

- необхідності знищення використаних персональних у кримінальному судочинстві;

- необхідності встановлення вимог забезпечення захисту даних від незаконної обробки як унаслідок необережності, так і навмисних дій.

Таким чином Рекомендації № R (87) закладають комплексну систему принципів захисту персональних даних у діяльності правоохоронних органів, спрямовану на забезпечення законності, пропорційності та цільового характеру їх обробки, що в подальшому знайшло свій розвиток та інституційне закріплення у праві ЄС.

Зокрема, еволюція підходів до охорони та захисту персональних даних зумовила формування спеціалізованих механізмів нагляду та координації їх на відповідному рівні.

Підсумовуючи, зазначимо, що також важливим суб’єктом у сфері захисту персональних даних є Європейська рада із захисту персональних даних (надалі – Європейська рада), яка заснована на підставі положень статті 68 GDPR [51]. Вона складається з голови одного наглядового органу кожної держави-члена та Єврпейського інспектора із захисту даних або їхніх відповідних представників.

Завдання Європейської ради передбачені положенням статті 70 GDPR та включають, зокрема, моніторинг правильного застосування його положень,

надання консультацій Комісії з будь-якого питання, пов’язаного із захистом персональних даних у ЄС, порад щодо відповідних питань, висновків, рекомендацій, окреслення найкращих практик і підходів щодо різноманітних питань, тощо.

Окремо також варто звернути увагу і на суміжні країни ЄС, а саме на Польщу, Румунію, Німеччину та Чеську Республіку які ратифікували Конвенцію Ради Європи № 108 [42] та імплементували Директиву 95/46/ЄС [49] у своє національне законодавство про захист персональних даних.

Як член ЄС, Польща імплементувала Директиву ЄС про захист даних 95/46/ЄС [49] у Законі про захист персональних даних від 29 серпня 1997 року (зведений текст: Збірник законів за 2016 рік, позиція 922) (надалі – попередній PDPA).

Що стосується GDPR [51], то 12 вересня 2017 року в Польщі було опубліковано два законопроєкти про захист персональних даних. Перший з них був прийнятий 25 травня 2018 року як новий «Закон про захист персональних даних» від 10 травня 2018 року (Збірник законів від 2019 року, ст. 1781) (надалі – ЗЗПД), а тоді як другий був прийнятий 4 травня 2019 року як «Закон про внесення змін до галузевих актів, що супроводжують GDPR», від 21 лютого 2019 року, що містить зміни до понад 160 галузевих нормативних актів, включаючи банківське, страхове та трудове законодавство (Збірник законів від 2019 року, ст. 730) (надалі – Закон про впровадження).

Ці два нові законодавчі акти спрямовані безпосередньо на імплементацію GDPR у польський правопорядок, а також на регулювання питань, у яких він залишає певну свободу для держав-членів ЄС. Новий ЗЗПД створює новий наглядовий орган, а саме – Голову Управління захисту персональних даних (надалі - Польський УЗПД), який має набагато ширший спектр повноважень, аніж попередній УЗПД (Генеральний інспектор захисту персональних даних) (надалі - Генеральний інспектор).

Також варто відмітити ряд положень «Закону про електронний зв’язок» від 12 липня 2024 року (надалі – Закон про електронний зв’язок), що застосовуються

до обробки персональних даних постачальником послуг електронного зв'язку, підприємством електронного зв'язку та підприємством телекомунікацій, а ряд галузевих законів, що стосуються, серед іншого, трудових та банківських питань, також містять конкретні правила щодо обробки персональних даних.

Кілька положень закону «Про клінічні випробування лікарських засобів для людини» від 9 березня 2023 року (Вісник законів 2023 р., позиція 605) також застосовуються до обробки персональних даних. Під час проведення клінічних випробувань, що є науковим дослідженнями, дозволяється обмежувати застосування положень статей 15, 16, 18 та 21 GDPR.

Ці обмеження можуть бути запроваджені, якщо є ймовірність, що права, викладені у вищезазначених положеннях, перешкоджатимуть або серйозно перешкоджатимуть досягненню цілей клінічного випробування, яке є науковим дослідженням, і якщо ці обмеження необхідні для досягнення цих цілей.

Також за даними Польської ради праці Кодексу, роботодавець може запровадити тести на тверезість для працівників, якщо це необхідно для забезпечення захисту життя та здоров'я працівників чи інших осіб або захисту майна. Таким чином роботодавець обробляє інформацію про дату та точний час тесту на тверезість та його результат лише у випадку, якщо це необхідно для забезпечення захисту майна та зберігає цю інформацію в особовій справі працівника протягом терміну, що не перевищує одного року з дати її збору [60].

В Румунії Закон № 190/2018 «Про заходи щодо застосування Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради» [61] від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільний рух таких даних, що скасовує Директиву 95/46/ЄС [49] (надалі – Закон № 190/2018) був опублікований в Офіційному віснику № 651/26.07.2018 та набув чинності 31 липня 2018 року. Він регулює, серед іншого, такі види діяльності, окрім надання певних відступів та рамок, пов'язаних із санкціями, що застосовуються до органів державної влади та державних установ:

- обробка генетичних даних, біометричних даних або даних про стан здоров'я;

- обробка національного ідентифікаційного номера;

- обробка персональних даних у контексті трудових відносин;

- обробка персональних даних та спеціальних категорій персональних даних у рамках виконання завдання, що здійснюється в суспільних інтересах.

Також необхідно підсумувати, що Закон № 190/2018 не містить жодних конкретних визначень щодо персональних даних оскільки цей термін вже визначено в GDPR.

Німеччина адаптувала свою правову базу до GDPR, прийнявши новий Федеральний закон про захист даних – «Bundesdatenschutzgesetz» (надалі – BDSG), який набув чинності разом із GDPR 25 травня 2018 року. Метою даного закону є, зокрема, використання численних вступних положень GDPR [51], які дозволяють державам-членам визначати або навіть обмежувати вимоги до обробки даних відповідно до GDPR. Частина 3 BDSG імплементує Директиву 2016/680 [53] про правоохоронну діяльність.

На додаток до BDSG в Німеччині, існує ціла низка правил захисту даних у галузевих законах, наприклад, тих, що регулюють фінансову торгівлю або енергетичний сектор.

Так, станом на 1 грудня 2021 року «Закон про телекомунікаційних даних», перейменований на «Закон про захист даних телекомунікаційних цифрових послуг» від 14 травня 2024 року – «Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz» (надалі – TDDDG). Він передбачає правила захисту даних для постачальників телекомунікаційних та цифрових послуг, які мають на меті усунути давню невизначеність щодо застосування правил захисту даних Закону Німеччини про телекомунікації «Telekommunikationsgesetz» (надалі – TKG) та Закону Німеччини про цифрові послуги «Digitale-Dienste-Gesetz» (надалі – DDG) у взаємодії з GDPR [51]. Також варто підсумувати, що TDDDG імплементує вимогу «згоди на використання файлів cookies» відповідно до статті 5 (3) Директиви про електронну конфіденційність у німецьке законодавство [61].

Новий Закон № 110/2019 Чеської Республіки «Про обробку персональних даних», який є чеським законом про імплементацію GDPR [51], нарешті набув

чинності 24 квітня 2029 року. Цей закон повністю замінив попередній Закон про захист персональних даних (Закон № 101/2000 зі змінами та доповненнями) та регулює обробку персональних даних у рамках Регламенту (ЄС) 2016/679 [51], а також обробку цих даних компетентними органами для запобігання, розшуку та виявлення злочинної діяльності, забезпечення безпеки та громадського порядку, тощо.

Варто зауважити, що він також регулює юрисдикцію Управління із захисту персональних даних та обробки персональних даних під час забезпечення оборони та безпеки Чеської Республіки [63].

Також в умовах стрімкого розвитку та поширення технологій штучного інтелекту (надалі – ШІ) варто звернути увагу на регламент ЄС, який встановлює спільну правову та регуляторну базу для нього в межах ЄС, а саме на акт про штучний інтелект «Artificial Intelligence Act» [64] (надалі – AI Act). Він спрямований на забезпечення безпечного та етичного використання ШІ, враховуючи потенційні ризики для суспільства та прав людини.

О. Петрів зазначає, що AI Act був опублікований в Офіційному журналі ЄС 12 липня 2024 року та набув чинності 1 серпня 2024 року. Його положення впроваджуються поступово протягом 6-36 місяців залежно від конкретних вимог [65]. Він доповнює регламент про захист даних GDPR, не змінюючи його, а також встановлює вимоги до розробників та користувачів ШІ-систем щодо безпеки, прозорості та відповідальності, забезпечуючи захист персональних даних та фундаментальних прав людини. Це включає обов’язкові оцінки ризиків, заходи щодо зниження можливих негативних наслідків та забезпечення підзвітності при використанні ШІ.

AI Act класифікує ШІ-системи за рівнем ризику на чотири категорії, а саме:

- неприйнятний ризик: системи, які заборонені через загрозу для безпеки або прав людей;

- високий ризик: системи, що вимагають суворого контролю та відповідності встановленим стандартам;

- обмежений ризик: системи з обмеженими вимогами щодо прозорості;

- мінімальний ризик: системи, які не підлягають спеціальному регулюванню.

Такий підхід дозволяє адаптувати регуляторні вимоги залежно від потенційного впливу ШІ на суспільство загалом.

Таким чином, AI Act встановлює чіткі правила для розробки та використання ШІ в ЄС, забезпечуючи баланс між інноваціями та захистом прав людини [65], а особливо захисту персональних даних.

Варто підсумувати, що розглянувши нормативно-правові акти, що регулюють сферу захисту персональних даних в ЄС та суміжних країнах, можна прийти до висновку, що законодавство ЄС розвивається та адаптується до умов сьогодення.

3.3. Напрями удосконалення правового регулювання захисту персональних даних у сфері охорони державного кордону України

Як зазначено в Стратегії інтегрованого управління державним кордоном України, в нинішніх умовах гібридного збройного конфлікту та у зв'язку з євроінтеграційним шляхом України, а також з урахуванням впровадження в життя сучасних цифрових інформаційних технологій (надалі – ІТ), від належного удосконалення правового регулювання охорони персональних даних у сфері захисту державного кордону України залежать як національна безпека держави загалом, так і розвиток її економіки та людського потенціалу. Зазначене також сприятиме надійній охороні та захисту кордону від транскордонної незаконної діяльності, стабільності та загальному розвитку держави, розширенню міжнародного співробітництва, збільшенню доходів державного та місцевого бюджетів, туризму та спрощенню інших форм законного переміщення товарів та послуг [66].

Враховуючи зазначене, належне правове регулювання охорони та захисту персональних даних в оперативно-службовій діяльності Державної прикордонної служби України (надалі – ДПСУ) є важливим аспектом

ефективного використання сучасних ІТ із забезпеченням балансу між забезпеченням інтересів національної безпеки та дотриманням прав людини.

На думку І. П. Кушнір і Р. М. Ляшук – постійна зміна характеру загроз на державному кордоні України потребує від ДПСУ адекватного та своєчасного реагування на них, адже наслідком її діяльності є дотримання загальнодержавного рівня безпеки (безпеки нації, суспільства та окремого громадянина) в частині недоторканості державного кордону України, недопущення зміни лінії державного кордону, збереження територіальної цілісності держави та реалізації права безперешкодного перетинання державного кордону України [67, С. 158].

З огляду на зазначене, охорона та захист державного кордону України має розглядатися не лише як сукупність оперативно-службових заходів, а як цілісна система забезпечення прикордонної безпеки, що поєднує правові, організаційні та інформаційні інструменти протидії сучасним викликам і загрозам. В умовах гібридного збройного конфлікту дедалі більшого значення набуває інформаційна складова прикордонної безпеки, адже вона пов’язана зі збором, обробкою та використанням персональних даних осіб, які перетинають державний кордон України.

Як зазначає І. П. Кушнір, безпека державного кордону України, а саме прикордонна безпека є важливою складовою національної безпеки, що забезпечується комплексом різноманітних заходів спрямованих на забезпечення захисту інтересів особи, громадянина, суспільства та держави у цій сфері. Елементом сучасної прикордонної безпеки є її інформаційна складова, а одним із її [68, С. 375] аспектів є охорона персональних даних у сфері захисту державного кордону України.

На нашу думку, для забезпечення прикордонної безпеки держави, а також з метою сприяння транскордонному співробітництву з країнами-членами Європейського Союзу (надалі – ЄС) у сфері охорони державного кордону та з урахуванням існуючих загроз, актуалізується потреба у впровадженні комплексних підходів до управління прикордонною сферою. Йдеться про

інтеграцію правових, організаційних та технологічних інструментів, що дозволяють гармонізувати національні процедури з європейськими практиками та забезпечити ефективну координацію між державними органами та міжнародними партнерами.

Окрім цього, також важливого значення набуває формування та впровадження інтегрованої моделі управління державним кордоном України, що ґрунтується на міжвідомчій координації та обміні інформацією з використанням ІТ, які здатні забезпечити ефективне реагування на наявні та потенційні загрози, особливо в умовах гібридного збройного конфлікту.

У зв'язку з інтенсивним розвитком ІТ, інформатизацією публічної та приватної сфери, упровадження електронних засобів ідентифікації особи, що відбувається з урахуванням європейської інтеграції [68, С. 375] та з метою забезпечення розвитку зовнішньоекономічних зв'язків та міжнародної торгівлі, сприяння переміщенню осіб і товарів через державний кордон України та належного його захисту, Кабінетом Міністрів України (надалі – КМУ) було схвалено «Стратегію інтегрованого управління кордонами на період до 2025 року» [69] (надалі – Стратегія).

Її прийняття стало важливим кроком держави щодо необхідності здійснення комплексної модернізації системи управління державним кордоном України, а також щодо її відповідності сучасним безпековим вимогам та стандартам ЄС у сфері прикордонної безпеки.

Схвалена Стратегія визначає напрями та пріоритети розвитку інституційної спроможності суб'єктів інтегрованого управління кордонами та удосконалення нормативно-правового забезпечення діяльності ДПСУ з впровадженням інноваційних ІТ в оперативно-службову діяльність підрозділів з охорони державного кордону України.

Стратегія спрямована на запровадження ефективних інструментів співпраці та координації на внутрішньовідомчому, міжвідомчому, міжнародному рівнях, а також з приватним сектором. Зважаючи на європейську та євроатлантичну інтеграцію України, ключовим результатом Стратегії є

готовність та спроможність до охорони зовнішніх кордонів із ЄС, в межах державного кордону, після набуття Україною повноправного членства в ЄС.

Для імплементації європейських компонентів прикордонної безпеки Стратегією враховуються національно адаптовані стратегічні цілі інтегрованого управління державним кордоном, передбачені відповідними європейськими документами [70, 71, 72] які визначають концептуальні засади формування в Україні цілісної моделі інтегрованого управління кордонами, що ґрунтується на стандартах ЄС та принципах багаторівневої координації та поєднанні безпекових функцій держави.

Відповідно до положень Стратегії, інтегроване управління кордонами – це скоординована діяльність компетентних органів України та військових формувань, спрямована на створення та підтримання балансу між забезпеченням належного рівня прикордонної безпеки і збереженням відкритості державного кордону України для законного транскордонного співробітництва, а також для осіб, які подорожують.

Її реалізація потребує чітко визначеного механізму координації, який має забезпечити та узгодити дії усіх суб’єктів інтегрованого управління кордонами на стратегічному та тактичному рівнях. Також для реалізації Стратегії необхідно забезпечити розвиток і запровадження сучасних ІТ, адже це сприятиме забезпеченню внутрішньої і зовнішньої безпеки держави.

Координацію інтегрованого управління державним кордоном здійснює міжвідомча робоча група з питань координації інтегрованого управління державним кордоном, яка була створена постановою Кабінету Міністрів України [73] та яка є його тимчасовим консультативно-дорадчим органом.

Необхідно зазначити, що з метою підвищення ефективності міжвідомчої взаємодії та оперативності прийняття рішень у сфері інтегрованого управління кордонами, було передбачено створення спеціалізованих координаційних механізмів. Так, з метою комплексного залучення суб’єктів для забезпечення системного підходу до організації та проведення ефективного моніторингу обстановки на державному кордоні України, проведення аналізу ризиків,

посилення комунікаційних спроможностей, постановою Кабінету Міністрів України [74] був утворений та функціонує координаційний центр інтегрованого управління державним кордоном. Його діяльність спрямована на координацію взаємодії між суб'єктами інтегрованого управління кордонами, узагальнення та аналіз інформації про стан безпекового середовища на державному кордоні України та безпосередньо пов'язана із реалізацією положень Стратегії.

Як зазначає О. Б. Ганьба норми Стратегії сприяють інтенсифікації розвитку інтеграційних відносин у сфері колективної прикордонної безпеки згідно з принципами та засадами ЄС, а також відносин міжнародної взаємодії в інтересах прикордонної співпраці суміжних держав тощо [75, С. 388]. Однак, попри те, що Стратегія є чинною, вона потребує оновлення, адже прикордонне безпекове середовище перебуває в постійній динаміці, що актуалізує необхідність його регулярного моніторингу і вивчення. Її оновлення зумовлене постійною зміною безпекового середовища на державному кордоні України та постійним розвитком і впровадженням європейського законодавства в національне, а також із необхідністю посилення охорони державного кордону. У зв'язку з цим, Адміністрацією ДПСУ (надалі – АДПСУ) розробляється проєкт Стратегії в якій вперше виокремлено окрему ціль 13 «Дотримання прав і свобод людини, забезпечення інклюзивності для вразливих груп населення», а це в свою чергу, відповідає європейським стандартам і створює можливості для розвитку безбар'єрного середовища, рівного доступу до послуг і посилення довіри до державних інституцій [76].

Варто зазначити, що такий підхід, а саме у виокремленні окремої цілі в проєкті Стратегії, свідчить про поступове переосмислення ролі та важливості прав людини в системі інтегрованого управління кордонами, а також демонструє прагнення України адаптувати національне законодавство у прикордонній сфері, до кращих європейських стандартів, обравши для цього людиноцентристський вектор.

З огляду на постійну динаміку безпекового середовища, зростання як зовнішніх так і внутрішніх загроз на державному кордоні України, в умовах

повномасштабного військового вторгнення Російської Федерації (надалі – РФ) в Україну, впровадження та реалізація проєкту Стратегії набуває особливої актуальності та необхідності.

В цих умовах, відбулася й переорієнтація пасажирського та транспортного потоків, яка призвела до зростання навантаження на пункти пропуску на кордоні з державами-членами ЄС та Республікою Молдова. Це негативно впливає на безпеку державного кордону України та підвищує рівень соціальної напруги, а також знижує комфорт для осіб, які подорожують [66].

Збільшення часу очікування, нерівномірність навантаження інфраструктуру пунктів пропуску, а також обмеженість їх пропускної спроможності, зумовили необхідність запровадження додаткових організаційно-управлінських механізмів, спрямованих на впорядкування руху транспортних засобів та мінімізацію корупційних ризиків.

З огляду на зазначене, постановою Кабінету Міністрів України [77] з грудня 2022 року розпочато реалізацію експериментального проєкту з керування чергами автомобільних транспортних засобів перед міжнародними пунктами пропуску через державний кордон України для автомобільного сполучення за допомогою «єЧерга».

А вже 05 грудня 2024 року постановою Кабінету Міністрів України [78] подовжено реалізацію «єЧерга» на наступні два роки, що безперечно дає змогу мінімізувати утворення фізичних черг на під'їзних шляхах до пунктів пропуску. Зазначимо, що цифровізація процесів управління черговістю прибуття транспортних засобів є лише одним із елементів комплексного реформування прикордонної інфраструктури та процедур контролю, які потребують подальшої оптимізації відповідно до стандартів ЄС.

Варто заначити, що запровадження спільного прикордонного контролю з країнами-членами ЄС надасть змогу вирішити низку проблемних питань, зокрема щодо облаштування пунктів пропуску, адже більшість пунктів пропуску облаштовано сканувальними системами, запровадження спільного прикордонного контролю суттєво спростить і пришвидшить процедуру

перетинання державного кордону України. Водночас, такий підхід об'єктивно зумовлює необхідність урахування актуальних змін у правовому регулюванні ЄС у сфері управління зовнішніми кордонами з використанням сучасних ІТ-систем контролю перетину державного кордону України.

Необхідно також зазначити, що відповідно до Регламенту Європейського Парламенту та Ради (ЄС) [79] в 2025 році в ЄС запроваджена нова система контролю перетину кордонів – «EES». Мета її запровадження – це пришвидшення проходження кордону, підвищити безпеку та запобігти перевищенню дозволеного терміну перебування в Шенгенській зоні [80]. Досягнення зазначеної мети передбачає створення єдиного інформаційного механізму автоматизованої реєстрації даних про в'їзд та виїзд громадян третіх країн, а також спрощення процедур прикордонного контролю на зовнішніх кордонах ЄС. У зв'язку з цим, нормативне закріплення порядку функціонування системи «EES» має принципово-важливе значення для забезпечення її ефективного застосування.

Положенням ст. 10 Регламенту [79] зазначено, що система «EES» повинна функціонувати на зовнішніх кордонах держав-членів, які повністю застосовують Шенгенське acquis та на кордонах держав-членів, які не повністю застосовують Шенгенське acquis у повному обсязі, але для яких перевірка відповідно до застосованої процедури Шенгенської оцінки вже успішно завершена та яким було надано доступ до Візової інформаційної системи «VIS».

Зауважимо, що за розробку та управління «EES» відповідає Європейське агентство з оперативного управління великомасштабними ІТ-системами у сфері свободи, безпеки та юстиції «EU-LISA» [81].

З огляду на те, що функціонування систем «єЧерга» та «EES» передбачає обробку значних масивів персональних та біометричних даних осіб, які перетинають державний кордон України, то особливої актуальності набувають питання належного нормативного забезпечення захисту таких даних, у тому числі гармонізація національного законодавства з європейськими стандартами у сфері приватності та інформаційної безпеки.

Також серед важливих напрямів удосконалення правового регулювання охорони персональних даних, варто звернути увагу і на прийнятий за основу у першому читанні Верховною Радою України 20 листопада 2024 року, законопроєкт № 8153 «Проект Закону про захист персональних даних» [82] (надалі – Законопроєкт 8153). Він пропонує ширші правила автоматизованої обробки персональних даних та має на меті не лише оновити чинне законодавство, але й максимально адаптувати українську систему захисту персональних даних до вимог Загального регламенту із захисту персональних даних – GDPR [51]. Також він може одночасно регулювати технології ШІ.

Законопроєкт 8153 закладає основи для якісного нового підходу до захисту персональних даних в Україні та зокрема передбачає:

- встановлення чітких стандартів і принципів обробки персональних даних, що відповідають сучасним міжнародним вимогам;

- розширення прав суб'єктів даних, зокрема: право на забуття, обмеження обробки, мобільність даних, заперечення проти обробки та захист від автоматизованого прийняття рішень;

- запровадження принципів «Privacy by Design» та «Privacy by Default», які гарантують високий рівень приватності на всіх етапах обробки даних;

- обов'язкове інформування контролюючих органів про витоки персональних даних протягом 72 годин;

- чітке регулювання передачі даних за кордон з дотриманням належного рівня захисту;

- введення ефективних фінансових санкцій за порушення, що забезпечує дієвість законодавства [83].

Варто зауважити, що законопроєкт формує сучасну систему захисту персональних даних в Україні, передбачаючи встановлення міжнародно-узгоджених стандартів обробки даних, розширення прав суб'єктів даних, обов'язкове повідомлення про витоки даних, врегульовує їх транскордонну передачу та запроваджує ефективні фінансові санкції за порушення.

Хоча законопроєкт № 8153 і не містить стандартів для ШІ, у ньому пропонуються нові поняття, пов’язані із автоматизованою обробкою персональних даних, до прикладу «профілювання», що забезпечує автоматизовану обробку персональних даних із застосуванням аналізу індивідуальних характеристик суб’єкта даних. Відповідно до його положень, профілювання – це форма автоматизованої обробки персональних даних, яка полягає у обробці персональних даних з метою оцінки певних індивідуальних характеристик, зокрема, аналізу та передбачення варіантів (моделей) поведінки суб’єкта персональних даних (в тому числі в професійній діяльності), його майнового стану, стану здоров’я, особистих уподобань, інтересів, надійності, місцезнаходження або пересування.

Визначення терміну «профілювання» узгоджується з визначенням, наданим у Загальному Регламенті із захисту персональних даних – GDPR [51]. В Законі AI Act [64] також є визначення «профілювання» відповідно до GDPR. Однак, він накладає додаткові заборони й обмеження на певні практики ШІ, які стосуються профілювання. До забороненого використання, зокрема, входить оцінка або прогнозування ризику вчинення фізичною особою кримінального злочину на основі профілювання.

Як зазначає Д. Бойко, безкоштовні, будь-які системи ШІ, що забезпечують профілювання фізичних осіб у критичній інфраструктурі, освіті, секторі безпеки й оборони, правосудді вважаються системами високого ризику, а розробники таких систем повинні здійснювати управління даними, перевіряти їх релевантність та запроваджувати систему управління ризиками [84].

Таким чином, хоча й законопроєкт № 8153 і не встановлює стандартів для ШІ, однак він запроваджує поняття «профілювання» як форми автоматизованої обробки персональних даних, що передбачає оцінювання індивідуальних характеристик особи. В контексті регулювання ШІ профілювання може підпадати під додаткові обмеження і вимоги щодо управління ризиками, особливо у секторі безпеки й оборони, зокрема в охороні державного кордону України.

У зв’язку з цим, важливим елементом формування ефективної системи контролю та нагляду у сфері захисту персональних даних є інституційне забезпечення відповідної державної політики. Постійне впровадження європейських стандартів та процес наближення до повного членства в ЄС вимагають оновлення українського регулювання захисту персональних даних, а тому варто звернути увагу і на законопроєкт № 6177 «Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» [85] (надалі – законопроєкт № 6177). Він визначає статус, повноваження, засади організації та порядок діяльності Національної комісії з питань захисту персональних даних та доступу до публічної інформації.

Головним завданням законопроєкту № 6177 є приведення нормативного регулювання України в сфері захисту персональних даних у відповідність до нових міжнародних стандартів в цій сфері. Він передбачає:

- приведення термінології сфери захисту персональних даних у відповідність до нових міжнародних стандартів;

- деталізацію та більш зрозуміле формулювання принципів обробки персональних даних;

- більш чітке формулювання підстав обробки персональних даних;

- деталізовані та прозорі вимоги до згоди на обробку персональних даних, які дозволять уникнути зловживань та маніпуляцій;

- розширення прав суб’єктів персональних даних та механізми їх реалізації;

- чітке визначення обов’язків контролера і оператора персональних даних;

- порядок повідомлення про витік персональних даних;

- інститут відповідальної особи з питань захисту персональних даних, її функціональні обов’язки, вимоги та порядок призначення;

- врегулювання передачі персональних даних на територію іноземних держав та міжнародних організацій;

- фінансову відповідальність, адміністративно-господарські санкції, що застосовуються до контролера та/або оператора за порушення права на захист

персональних даних, які дозволяють забезпечити дієвість закону та виконання його вимог.

Окрім вищезазначеного, законопроєкт № 6177 має на меті підвищити рівень захисту конституційного права на повагу до приватного життя через посилення стандартів обробки персональних даних та надати більше прав суб'єкту персональних даних для забезпечення можливості здійснення повноцінного контролю суб'єктом за обробкою його персональних даних.

Таким чином, необхідність його прийняття обумовлена тим, що стан законодавства не в повній мірі забезпечує захист персональних даних в Україні в світлі розвитку міжнародних стандартів у цій сфері.

Створення належного органу, який би здійснював контроль за дотриманням права на захист персональних даних є вимогою Додаткового протоколу [43] до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [42], який було ратифіковано Україною 06.07.2010 року [45].

Оскільки, відповідно до міжнародних стандартів зазначений орган має діяти з абсолютною незалежністю, що має гарантуватися законом, то проєкт Закону України «Про внесення змін до статті 154 Кримінального процесуального кодексу України (щодо гарантії незалежності члена Національної комісії з питань захисту персональних даних та доступу до публічної інформації)» [86] (надалі – законопроєкт № 6178) пов'язаний із законопроєктом № 6177. Метою даного законопроєкту є посилення гарантій незалежності членів Національної комісії з питань захисту персональних даних та доступу до публічної інформації (надалі – Національна комісія) шляхом встановлення особливого порядку застосування такого заходу забезпечення кримінального провадження як відсторонення від займаної посади.

Законопроєктом пропонується внесення змін до статті 154 Кримінального кодексу України [86], якими передбачено, що відсторонення від посади члена Національної комісії здійснюється слідчим суддею на підставі вмотивованого клопотання Генерального прокурора в порядку, встановленому законом.

Таким чином, прийняття законопроєкту № 6178 дозволить привести національне законодавство у відповідність до міжнародних стандартів у сфері доступу до інформації шляхом посилення гарантій незалежності членів Національної комісії.

Поряд із цим, удосконалення національного законодавства та приведення його у відповідність до сучасних суспільно-політичних умов потребує врахування нових викликів, спричинених збройною агресією РФ проти України, а також суспільних запитів громадян, що сформувалися в умовах гібридної війни. У зв'язку з цим, до Верховної Ради України внесено проєкт Закону «Про внесення змін до пункту 12 частини сьомої статті 21 Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» щодо додаткового захисту персональних даних» [87] (надалі – законопроєкт № 7314). Однак, Верховною Радою України законопроєкт № 7314 було відхилено.

Окрім вищезазначеного, підсумовуючи, варто також звернути увагу і на те, що відповідно до актуальної інформації 2026 року, в Україні є наміри впровадження ШІ в систему охорони державного кордону. Зокрема:

- Уряд України у своїй програмі діяльності акцентує увагу на підвищенні технічного захисту інформації та охорони державного кордону, включно з впровадженням ШІ для підвищення ефективності та зниження корупційних ризиків [88];

- існує проєкт Плану заходів на 2026 – 2028 роки щодо реалізації Стратегії інтегрованого управління державним кордоном, де передбачаються інноваційні технології, зокрема ШІ, насамперед його використання з метою захисту персональних даних [89];

- Міністерство оборони України (надалі – МОУ) планує виділити до одного мільйона євро на співпрацю з Центром ШІ, що свідчить про активне залучення ШІ у сферу безпеки, включно з охороною кордонів [88].

Отже, можна стверджувати, що в Україні є чіткі наміри та конкретні кроки щодо впровадження ШІ в систему охорони державного кордону, що має на меті підвищення безпеки, ефективності контролю та зниження корупційних ризиків.

Щодо сфери захисту персональних даних з використанням ШІ в Україні 2026 року планується комплексний підхід, який враховує сучасні вимоги законодавства та міжнародні стандарти. Основні напрямки та заходи включають:

- узгодження національного законодавства з європейським регламентом GDPR та новими нормами, пов'язаними із ШІ (наприклад – Ai Act) дозволить забезпечити високий рівень захисту персональних даних при використанні ШІ;

- впровадження принципів прозорості, відповідальності та контролю за обробкою персональних даних у системах із ШІ, – це включає вимоги до розпізнавання згенерованого контенту, перевірки достовірності інформації та критичної оцінки матеріалів;

- розробка та застосування технологічних рішень для захисту даних, таких як шифрування, анонімізація, а також системи моніторингу і виявлення порушень безпеки;

- підвищення рівня обізнаності користувачів і фахівців щодо ризиків і методів захисту персональних даних у контексті ШІ, що включає освітні кампанії та спеціалізовані заходи;

- проведення фахових обговорень і консультацій між експертами, юристами та розробниками для визначення меж відповідальності та етичних норм у використанні ШІ у правовій сфері та захисті даних [90].

Таким чином, в Україні 2026 року захист персональних даних із застосуванням ШІ розглядається як пріоритетна сфера, де поєднуються законодавчі та технологічні заходи для забезпечення безпеки та прав людини.

За умов впровадження в сучасне життя ІТ та ШІ, а також євроінтеграції України, особливої актуальності набуває розроблення пропозицій щодо удосконалення правового регулювання охорони персональних даних у сфері захисту державного кордону України – концептуально, доктринально та змістовно.

Концептуально:

- гармонізація зі стандартами GDPR: необхідно привести національні норми у відповідність, а саме – законність, прозорість, мінімізація даних, обмеження мети, збереження в межах термінів, права суб'єктів;

- необхідно забезпечити баланс безпеки і прав людини: зробити принцип пропорційності й необхідності центральним при обробці даних у прикордонній сфері;

- принципи «Privacy by Design» та «Privacy by Default»: необхідно інтегрувати захист даних на етапі проєктування прикордонних систем (камери відеоспостереження, біометрія, бази даних).

Доктринально:

- чітке визначення юридичних понять: необхідно закріпити в законі визначення «обробка персональних даних на кордоні, «оператори/розпорядники систем прикордонного контролю», «біометричні дані», «автоматизоване прийняття рішень»;

- нормативи щодо допустимості біометрії: необхідно розробити доктрину застосування біометричних технологій з урахуванням ризиків для приватності й дискримінації;

- пріоритет правової визначеності і судового захисту: необхідно закріпити механізми оскарження дій прикордонних органів у частині обробки даних та доступу до ефективних засобів правового захисту.

Змістовно (конкретні норми й інструменти):

- законодавчі положення про правові підстави: необхідно чітко вказати правову підставу для збору й обробки (наприклад – національна безпека, виконання завдань органів влади) та обмеження за обсягом і термінами;

- обмеження збору і мінімізація: необхідно заборонити збір даних, що не потрібні для прикордонного контролю, і потрібно встановити політику дедалі менших наборів даних;

- оцінка впливу на приватність (надалі – DPIA) (**Додаток Б**): необхідно зробити обов'язковими для всіх нових систем, що обробляють чутливі дані або масові дані (біометрія, відеоспостереження);

- захист чутливих категорій даних: необхідна заборона або суворе регулювання обробки расових, етнічних даних тощо;

- технічні заходи: необхідне обов'язкове шифрування збережених і переданих даних, псевдонімізація, журнали доступу з аудитом;

- контроль доступу і логування: необхідні ролі, принцип найменших привілеїв, регулярні аудити доступу;

- трансграничні передачі: необхідні чіткі правила при передачі даних іншим державам або міжнародним системам, з гарантіями захисту;

- прозорість і інформування: необхідно інформувати осіб про обробку, права і механізми оскарження там, де це не створює загрозу безпеці;

- санкції і відповідальність: необхідно встановити пропорційні адміністративні та кримінальні механізми відповідальності за порушення.

Покрокова імплементація (рекомендовані кроки):

- провести аудит поточних практик обробки даних у прикордонних підрозділах;

- розробити проєкт змін до закону з урахуванням принципів GDPR і національних інтересів;

- впровадити DPIA як обов'язковий інструмент для всіх нових систем;

- впровадити технічні стандарти (шифрування, логування, доступи);

- навчити персонал і провести пілотні проєкти з оцінкою результатів;

- створити механізм незалежного нагляду та регулювання аудитів;

- запровадити прозору політику інформування і процедури подання скарг.

Додаткові елементи, які варто передбачити в законодавстві:

- обов'язкова наявність уповноваженої особи із захисту даних (надалі – DPO) у прикордонних органах;

- обмеження строків зберігання даних і чіткі процедури їх видалення;

- положення про співпрацю зі службами безпеки і про суворий порядок доступу за запитом;

- механізми незалежного контролю – наглядовий орган, омбудсмен або апеляційні інстанції та публічні звіти про практики обробки й інциденти безпеки.

Таким чином, необхідно поєднати стандарти захисту приватності, на кшалт GDPR, із потребами національної безпеки, закріпивши принципи пропорційності, мінімізації та прозорості, а серед практичних кроків необхідно провести аудит, зміни в законі та впровадити DPIA й технічні стандарти, провести навчання персоналу і забезпечити незалежний нагляд за дотриманням законодавства у сфері захисту персональних даних.

Однак для того, щоб визначити реальні напрями удосконалення захисту персональних даних у сфері охорони державного кордону України, необхідно проаналізувати чинне прикордонне законодавство України в частині захисту персональних даних осіб, які перетинають державний кордон.

Такий аналіз дозволяє виявити нормативні прогалини й практичні проблеми прикордонного контролю та оцінити ефективність чинних механізмів, визначивши потребу їх гармонізації з європейськими стандартами.

Українське прикордонне законодавство загалом визнає необхідність збирання та обробку персональних даних під час прикордонного контролю, але робить це переважно через призму безпеки держави, міграційного контролю та запобігання правопорушенням. Із результатів пошуку видно, що ключовими актами є Закон України «Про прикордонний контроль» [91], а також підзаконні акти щодо баз даних осіб, які перетнули державний кордон. Окремо виявлено, що в наукових і практичних матеріалах наголошується на потребі прозорості, законності та обґрунтованості дій прикордонників під час збору інформації.

Водночас, нинішня модель регулювання має певну асиметрію: детально врегульовано сам механізм контролю, але не завжди достатньо чітко визначено межі, гарантії та процедури захисту персональних даних. Це створює ризики надмірного збору інформації, невизначеності строків її зберігання, доступу до неї, передачі іншим органам та захисту від несанкціонованого використання.

Для з’ясування цих проблем необхідно розглядати нормативну базу не лише крізь призму спеціального прикордонного законодавства, а й у взаємозв’язку із загальними актами про захист персональних даних та конституційними гарантіями приватності. Саме таке комплексне бачення дозволяє оцінити, наскільки прикордонний контроль відповідає принципам законності, пропорційності та прав людини.

У цій сфері слід розглядати не лише прикордонне законодавство, а й загальні акти про захист даних. Насамперед це: Закон України «Про прикордонний контроль» [91], Закон України «Про захист персональних даних» [41], Закон України «Про Державну прикордонну службу України» [92], підзаконні акти щодо баз даних, обліку осіб, які перетнули кордон та інформаційної взаємодії між органами влади, конституційні гарантії права на невтручання в особисте і сімейне життя та на захист персональних даних.

Саме поєднання цих актів формує правову основу для того, щоб прикордонний контроль був не лише ефективним, а й сумісним із принципами прав людини.

Разом із тим, аналіз зазначених нормативних джерел виявляє низку суттєвих проблем, які знижують рівень правових гарантій для осіб, які перетинають державний кордон. Ці проблеми стосуються як обсягу та меж збору, так і строків її зберігання, порядку доступу та передачі іншим органам, а також рівня прозорості для самих громадян. Саме вони потребують окремого розгляду й систематизації.

1. Надмірність збору даних: під час перетину кордону можуть збиратися дані, які не завжди є необхідними для досягнення законної мети контролю. Проблема полягає в тому, що законодавство не завжди достатньо чітко встановлює принцип мінімізації даних: збирати лише те, що справді потрібно для ідентифікації, перевірки документів, безпеки та пропуску через кордон.

2. Нечіткість щодо строків зберігання: однією з найбільших чутливих тем є те, як довго зберігаються дані про перетин кордону, хто визначає строк зберігання і коли дані мають бути знищені або знеособлені. Якщо ці питання

врегульовані нечітко, то виникає ризик створення фактично необмежених масивів даних про переміщення осіб.

3. Широке коло доступу до даних: персональні дані осіб, які перетинають кордон, можуть бути цікавими багатьом органам. Але чим ширше коло суб'єктів доступу, тим вищий ризик зловживань. Законодавство має чітко визначити: хто має доступ, з якою метою, на якій правовій підставі, у якому обсязі, чи фіксується кожен факт доступу.

4. Передача даних іншим органам і міжнародний обмін: у прикордонній сфері дані часто передаються іншим державним органам або використовуються в міжнародній співпраці. Тут особливо важливо, щоб передача відбувалася лише: на підставі закону, для конкретної мети, із дотриманням принципу пропорційності, за наявності належних гарантій безпеки.

5. Недостатня прозорість для самих осіб: особа, яка перетинає кордон, не завжди чітко розуміє: які саме її дані збираються, хто є володільцем бази, як довго дані зберігаються, як можна виправити помилку, як оскаржити незаконну обробку.

Це послаблює реальність права на захист персональних даних, навіть якщо формально воно існує.

Водночас, попри недоліки, у законодавстві є й сильні сторони: наявність законної мети обробки даних – забезпечення прикордонної безпеки, формалізація процедур контролю, що зменшує ризик довільних дій, визнання необхідності баз даних для обліку перетину кордону, зв'язок із загальним законом про захист персональних даних, який може застосовуватися як універсальний стандарт, поступове наближення до європейських підходів, де ключовими є законність, пропорційність, обмеження мети та безпека обробки.

Разом ці позитивні риси створюють підґрунтя для подальшого вдосконалення правового регулювання у прикордонній сфері. Вони окреслюють напрям руху до більш збалансованої моделі, яка поєднує потреби державної безпеки з гарантіями прав людини. Проте для досягнення відповідності

європейським стандартам необхідно чітко визначити конкретні кроки та закріпити їх у законодавстві.

У прикордонному законодавстві доцільно прямо передбачити, що збір персональних даних має обмежуватися лише тими відомостями, які є необхідними та достатніми для: ідентифікації особи, перевірки документів, оцінки підстав для пропуску або відмови, забезпечення безпеки.

1. Встановити чіткі строки зберігання: потрібно законодавчо визначити: строки зберігання даних про перетин кордону, підстави для продовження зберігання, порядок знищення або знеособлення даних, окремі правила для даних, пов'язаних із правопорушеннями чи розшуком. У цьому зв'язку важливим є також визначення механізмів та засобів удосконалення прикордонного контролю, які мають базуватися на впроваджених стандартах GDPR, тобто на адаптованих до українських умов процедурах здійснення прикордонного контролю відповідно до вимог Регламенту ЄС про захист даних.

2. Обмежити доступ до баз даних: слід запровадити більш жорсткі правила доступу: доступ лише за службовою необхідністю, персоніфікована авторизація, журналювання всіх дій користувачів, проведення незалежних кібераудитів та стрес-тестів систем баз даних кордону (наприклад, Державною службою спеціального зв'язку та захисту інформації або міжнародними експертами), здійснення менеджменту інцидентів, тобто створення чітких протоколів швидкого реагування на випадок кібератак або компрометації даних пасажирів, а також відповідальність за несанкціоноване використання.

3. Посилити інформування осіб: особи, які перетинають кордон, мають отримувати зрозумілу інформацію про: мету збору даних, правову підставу, володільця та розпорядника даних, строки зберігання, права на доступ, виправлення та оскарження.

4. Впровадити оцінку впливу на захист даних: для нових цифрових систем прикордонного контролю – «EES» та «єЧерга» варто передбачити оцінку впливу на захист персональних даних ще до запуску системи. Це особливо важливо для: автоматизованого контролю, біометричних технологій, інтегрованих баз даних,

міжвідомчого обміну інформацією. У цьому контексті доцільним є також навчання прикордонників протидії фішингу, соціальній інженерії та правилам поводження з носіями інформації, а також застосування інструментів штучного інтелекту для підвищення ефективності оцінки ризиків і забезпечення належного рівня кіберзахисту.

5. Посилити парламентський і незалежний контроль: доцільно передбачити: регулярний моніторинг практики оброки даних, звітування про кількість запитів і передач, перевірки дотримання режимів доступу, участь уповноважених органів із захисту персональних даних. В цих умовах важливим є напрацювання щодо удосконалення здійснення контролю за правоохоронним запитом, зокрема шляхом встановлення та запровадження жорстких судових або адміністративних фільтрів для передачі прикордонних даних іншим відомствам, що забезпечить додаткові гарантії законності та пропорційності у сфері захисту персональних даних.

Запропоновані напрями удосконалення свідчать про необхідність системного реформування правового регулювання у сфері захисту персональних даних на кордоні. Вони окреслюють конкретні кроки, що дозволяють гармонізувати українське законодавство з європейськими стандартами, забезпечити баланс між потребами національної безпеки та правами людини, а також підвищити ефективність і прозорість діяльності прикордонних органів.

Підсумовуючи варто зауважити, що чинне прикордонне законодавство України створює правову основу для обробки персональних даних осіб, які перетинають державний кордон, але потребує подальшого вдосконалення в частині гарантій приватності, прозорості та контролю за обробкою даних. Головна проблема полягає не у відсутності правового регулювання як такого, а в тому, що воно має бути більш конкретним, пропорційним і технологічно адаптованим. Найважливіші напрями реформування: мінімізація збору даних, чіткі строки зберігання, обмеження доступу, прозоре інформування осіб, незалежний контроль, оцінка ризиків для нових цифрових систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 3:

1. Аніщук В. В. Проблема захисту персональних даних в кіберпросторі. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. № 84. Т. 3. С. 252–256. URL: https://doi.org/10.24144/2307-3322.2024.84.3.38

2. Землянська О. В., Праховнік Н. А., Ковтун А. І., Ковтун М. А. Безпека в інтернеті та захист персональних даних. *Всеукраїнська науково-практична конференція «Безпека життя і діяльності людини: теорія та практика»:* матеріали наук.-практ. конф. Полтава, 2022. С. 62–64.

3. Радзієвська О. Г. Інформаційні права та безпека особи в умовах соціальних і цифрових трансформацій. *Соціальна цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали II всеукр. наук.-практ. конф. (Київ, 25 грудня 2022 р.). Київ-Одеса, 2022. С. 22–25.

4. Роль штучного інтелекту у боротьбі з кіберзлочинністю: Чи можуть технології випередити хакерів? URL: https://cripo.com.ua/news/society/rol-shtuchnogo-intelektu-u-borotbi-z-kiberzlochynnistyu-chy-mozhut-tehnologiyi-vyperedyty-hakeriv/ (дата звернення: 01.10.2024).

5. Атаки на основі штучного інтелекту: нові виклики для кібербезпеки. URL: https://it-rating.ua/ataki-na-osnovi-shtuchnogo-intelektu-novi-vikliki-dlya-kiberbezpeki (дата звернення: 02.10.2024).

6. Кібервійна з російськими хакерами. Чи достатньо захищені українські реєстри. URL: https://cripo.com.ua/vojna-s-rf/kibervijna-z-rosijskymy-hakeramy-chy-dostatno-zahyshheni-ukrayinski-reyestry/ (дата звернення: 02.10.2024).

7. Д'яконов І. Наймасштабніша кібератака на державні реєстри України: зупинено роботу систем Мінюсту. URL: https://www.pravda.com.ua/news/2024/12/20/7489933/ (дата звернення: 02.10.2024).

8. Герасименко К. В. Штучний інтелект та кібербезпека. URL: https://www.education.ua/blog/48113/ (дата звернення: 05.10.2024).

9. Думчиков М. О., Бондаренко О. С. Проблемні аспекти захисту персональних даних в мережі інтернет. *Наукові записки Львівського*

університету бізнесу і права. Серія юридична. 2024. Вип. 40. С. 105–110. URL: https://doi.org/10.5281/zenodo.10548017

10. Касперський І. П. Проблеми забезпечення принципів захисту персональних даних у процесах цифрової трансформації. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання:* матеріали II всеукр. наук.-практ. конф. (Київ, 25 грудня 2022 р.). Київ-Одеса, 2022. С. 33–37.

11. Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг: Постанова Кабінету Міністрів України від 04 грудня 2019 року № 1137. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text (дата звернення: 03.10.2024).

12. Telegram-контакт @zedigital message edited Jan 22 at 12:18. URL: https://t.me/zedigital/970 (дата звернення: 03.10.2024).

13. Панасюк В. Майбутнє – за технологіями, сьогодення за «Дією»: інтерв'ю з очільником Мінцифри Михайлом Федоровим. URL: https://kanaldim.tv/budyashhee-za-tehnologiyami-nastoyashhee-za-diyeyu-intervyu-s-glavoj-minczifry-mihailom-fedorovym/ (дата звернення: 06.10.2024).

14. Дія : офіційний вебпортал. Повідомлення про обробку персональних даних порталу «Дія». URL: https://diia.gov.ua/policy (дата звернення: 06.10.2024).

15. Чернишова О. З «Дії» чи ні? Звідки хакери взяли персональні дані 2 млн українців. Розслідування DOU. URL: https://dou.ua/lenta/articles/inquiry-about-diia-data-leak/ (дата звернення: 12.10.2024).

16. Поляковська Т. В інтернеті виявлено велику базу даних українців: омбудсмен Денісова вже звернулася до поліції. URL: https://www.unian.ua/society/v-interneti-viyavleno-veliku-bazu-danih-ukrajinciv-ombudsmen-denisova-vzhe-zvernulasya-do-policiji-novini-ukrajini-11543359.html (дата звернення: 12.10.2024).

17. Українська правда. Мінцифри: «Дія» не зливає дані, незаконними телеграм-каналами займається СБУ. URL:

https://www.pravda.com.ua/news/2020/05/12/7251282/ (дата звернення: 19.10.2024).

18. Департамент кіберполіції Національної поліції України. *Офіційний сайт.* Кіберполіцейські вилучили з незаконного обігу бази персональних даних понад 300 мільйонів осіб. URL: https://cyberpolice.gov.ua/news/kiberpoliczejski-vyluchyly-z-nezakonnogo-obigu-bazy-personalnyx-danyx-ponad--miljoniv-osib-7493/ (дата звернення: 25.10.2024).

19. Пасіка В. Повідомляють про масштабний злив даних користувачів «Дія», Мінцифри це заперечує. URL: https://dou.ua/lenta/news/diia-data-leak-2022/ (дата звернення: 25.10.2024).

20. Жаркова О. Персональні дані на продаж: хто винен і чи буде покараний? URL: https://www.ukrinform.ua/rubric-society/3056669-personalni-dani-na-prodaz-hto-vinen-i-ci-bude-pokaranij.html (дата звернення: 27.10.2024).

21. Малинка А. Про ризики в роботі з персональними даними. URL: https://www.prostir.ua/?blogs=pro-ryzyky-v-roboti-z-personalnymy-danymy (дата звернення: 01.11.2024).

22. Шевченко С. Скільки коштують персональні дані українців і чи легко їх купити? URL: https://www.radiosvoboda.org/a/personalni-dani-na-prodazh/31074560.html (дата звернення: 05.11.2024).

23. Міністерство оборони України. *Офіційний сайт.* Кібератаки Російської Федерації. Хронологія. URL: https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html (дата звернення: 05.11.2024).

24. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 08.11.2024).

25. Інститут масової інформації. Російські хакери ще до початку вторгнення здійснили 237 кібератак на Україну – Microsoft. URL: https://imi.org.ua/NEWS/ROSIJSKI-HAKERY-SHHE-DO-POCHATKU-

VTORGNENNYA-ZDIJSNYLY-237-KIBERATAK-NA-UKRAYINU-MICROSOFT-I45256 (дата звернення: 12.11.2024).

26. Інститут масової інформації. Окупант у ніч повномасштабного вторгнення хотів знищити весь кіберзахист України – СБУ. URL: https://imi.org.ua/NEWS/OKUPANT-U-NICH-POVNOMASSHTABNOGO-VTORGNENNYA-HOTIV-ZNYSHHYTY-VES-KIBERZAHYST-UKRAYINY-SBU-I44798 (дата звернення: 12.11.2024).

27. Пишкін С. Кібератака на «Київстар», ймовірно була наймасштабнішою атакою хакерів з початку війни. URL: https://www.rbc.ua/rus/news/kiberataka-kiyivstar-ymovirno-bula-naymasshtabnishoyu-1702729643.html (дата звернення: 15.11.2024).

28. Державна служба спеціального зв'язку та захисту інформації України. *Офіційний сайт.* Кіберзлочинці здійснили спробу атакувати оборонні підприємства та українських захисників. URL: https://cip.gov.ua/ua/news/cert-ua-warns-of-phishing-attacks-targeting-ukrainian-defense-sector (дата звернення: 22.11.2024).

29. CERT-UA. *Офіційний сайт.* UAC-0200: шпигунство за оборонно-промисловим комплексом за допомогою DarkCrystal RAT (CERT-UA#14045). URL: https://cert.gov.ua/article/6282737 (дата звернення: 26.11.2024).

30. Лаптєв С. О. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. *Електронне фахове видання «Кібербезпека: освіта, наука, техніка».* 2022. № 4 (16). С. 45 – 62. URL: https://doi.org/10.28925/2663-4023.2022.16.4562

31. HackYourMom. Що таке соціальна інженерія: Напади, методи та запобігання. URL: https://hackyourmom.com/KIBERVIJNA/SHHO-TAKE-SOCZIALNA-INZHENERIYA-NAPADY-METODY-TA-ZAPOBIGANNYA/ (дата звернення: 01.12.2024).

32. Про інформацію: Закон України від 02 жовтня 1992 року № 2657-XII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 02.12.2024).

33. NADIYNO. Що таке соціальна інженерія. URL: https://nadiyno.org/shho-take-soczialna-inzheneriya/ (дата звернення: 04.12.2024).

34. Северінова О. Б. Інформаційно-правовий простір: питання розвитку в умовах реформування. *Право і суспільство*. 2019. С. 75–80. URL: https://doi.org/10.32842/2078-3736-2019-6-1-13

35. Шарабурина О. О. Проблеми правового захисту персональних даних як відомостей з обмеженим доступом. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2012. Вип. 4 (16). С. 71–74.

36. Різенко О. В. Європейські правові стандарти захисту персональних даних. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 6. С. 643–648. URL: https://doi.org/10.24144/2788-6018.2024.06.105

37. Дуравкін П. М., Гафич І. І. Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. *Право та інновації*. 2023. № 3 (43). С. 89–100. URL: https://doi.org/10.37772/2518-1718-2023-3(43)-12

38. Головацький Н. Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України. *Науковий вісник УжНУ. Серія Право*. 2024. Вип. 85. Ч. 2. С. 288–292. URL: https://doi.org/10.24144/2307-3322.2024.85.2.42

39. Коваленко Ю. О. Особливості захисту персональних даних у Європейському Союзі та їх вплив на процес євроінтеграційної політики України. *Право та державне управління*. 2023. № 3. С. 138–144. URL: https://doi.org/10.32782/pdu.2023.3.21

40. Кебус А. В. Кримінально-правовий захист персональних даних законодавства України відповідно до держав Європейського Союзу. *Modern scientific journal (Сучасний науковий журнал)*. 2023. № 2 (2). С. 52–60. URL: https://doi.org/10.36994/2786-9008-2023-2-7

41. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 29.07.2025).

42. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: дата набрання чинності для України – 01 січня 2011 року. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 01.08.2025).

43. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних: дата набрання чинності для України – 01 січня 2011 року. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/994_363?lang=en#Text (дата звернення: 01.08.2025).

44. Брижко В. М. Про упорядкування законодавства України із захисту персональних даних. *Правова інформатика*. 2008. № 1 (17) С. 20–34.

45. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Закон України від 06 липня 2010 року № 2438-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2438-17#Text (дата звернення: 03.08.2025).

46. Вишневський В. О. Ретроспектива розвитку європейського законодавства у сфері захисту персональних даних. *Часопис Київського університету права.* 2024. № 3. С. 86–90. URL: https://doi.org/10.36695/2219-5521.3.2024.12

47. Протокол, що вносить зміни до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (CETS № 223). 10.10.2018. URL: https://rm.coe.int/16808ac918 (дата звернення: 03.08.2025).

48. Хартія основних прав Європейського Союзу. URL: https://www.asser.nl/media/798224/hartiya-osnovnyh-prav-yevropejskogo-soyuzu-2.pdf (дата звернення: 03.08.2025).

49. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких

даних» від 24 жовтня 1995 року. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 05.08.2025).

50. Бем М. В., Городинський І. М. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. Рада Європи, 2021. 160 С.

51. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС» від 27 квітня 2016 року. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 06.08.2025).

52. Кебус А. В. Законодавства України та держав Європейського Союзу щодо кримінально-правового захисту персональних даних. *Часопис Київського університету права.* 2023. № 1. С. 202–205. URL: DOI: 10.36695/2219-5521.1.2023.43

53. Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення чи переслідування кримінальних правопорушень чи виконання кримінальних покарань, а також про вільний рух таких даних та про скасування Рамкового рішення Ради 2088/977/JHA. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj (дата звернення: 08.08.2025).

54. Директива Європейського Парламенту і Ради (ЄС) 2016/681 від 27 квітня 2016 року про використання даних запису реєстрації пасажирів (ЗРП) для запобігання, виявлення, розслідування та переслідування терористичних та тяжких злочинів. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_045-16#Text (дата звернення: 10.08.2025).

55. Прохазка Г. А. Захист персональних даних у сучасному світі. *Науковий вісник Ужгородського національного університету.* 2018. Вип. 53. Т. 2. С. 151–155.

56. Дяковський О. С., Кортукова Т. О. Правове регулювання захисту персональних даних в Європейському Союзі. *Юридичний науковий журнал.* 2023. № 7. С. 266–269. URL: https://doi.org/10.32782/2524-0374/2023-7/61

57. Сайфет Ю., Квінтел Т. Директива (ЄС) 2016/680 про захист даних для поліції та органів кримінального правосуддя. 2018. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873 (дата звернення: 13.08.2025).

58. Директива 2002/58/ЄС Європейського Парламенту і Ради «Щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації)» від 12 липня 2002 року. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058 (дата звернення: 21.05.2024).

59. Рекомендації № R (87) Комітету Міністрів Ради Європи про захист персональних даних у секторі поліції 1987 року. URL: https://rm.coe.int/168062dfd4 (дата звернення: 15.08.2025).

60. Закони про захист даних у Польщі. URL: https://www.dlapiperdataprotection.com/?c=PL&t=law (дата звернення: 20.08.2025).

61. Закони про захист даних в Румунії. URL: https://www.dlapiperdataprotection.com/?c=RO&t=law (дата звернення: 22.08.2025).

62. Закони про захист даних в Німеччині. URL: https://www.dlapiperdataprotection.com/?c=DE&t=law (дата звернення: 24.08.2025).

63. Закони про захист даних у Чеській Республіці. URL: https://www.dlapiperdataprotection.com/?c=CZ&t=law (дата звернення: 25.08.2025).

64. Дослідник законів про штучний інтелект. URL: https://artificialintelligenceact.eu/ai-act-explorer/ (дата звернення: 28.08.2025).

65. Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. 2025. URL: https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/ (дата звернення: 01.09.2025).

66. Проєкт Стратегії інтегрованого управління державним кордоном України. *Офіційний сайт Державної прикордонної служби України.* URL: https://dpsu.gov.ua/uk/proyekt-strategiyi-integrovanogo-upravlinnya-derzhavnim-kordonom-ukrayini (дата звернення: 07.02.2026).

67. Кушнір І. П., Ляшук Р. М. Результативність та ефективність в діяльності органів охорони державного кордону України. *Право і суспільство.* 2017. № 5. С. 154–159.

68. Кушнір І. П. Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України : дис. … д-ра юрид. наук : 12.00.07. Київ, 2020. 566 С.

69. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : Розпорядження Кабінету Міністрів України від 24 липня 2019 року № 687-р. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text (дата звернення: 08.02.2026).

70. Регламент Європейського Парламенту і Ради (ЄС) № 2019/1896 від 13 листопада 2019 року «Про Європейську прикордонну і берегову охорону» та скасування Регламенту (ЄС) № 1052/2013 та Регламенту (ЄС) № 2016/1624. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_016-19#Text (дата звернення: 09.02.2026).

71. Рішення Ради Правління № 43/2024 від 21 листопада 2024 року «Про схвалення Технічної та оперативної стратегії Європейського інтегрованого управління кордонами на 2023 – 2027 роки». URL:

https://prd.frontex.europa.eu/document/management-board-decision-30-2023-adopting-the-technical-and-operational-strategy-for-european-integrated-border-management-2023-2027 (дата звернення: 09.02.2026).

72. Регламент Європейського Парламенту і Ради (ЄС) № 2016/399 від 09 березня 2016 року «Про Кодекс Союзу щодо правил, які регулюють рух осіб через кордони та правовими, політичними вимогами ЄС щодо Шенгенського acquis». *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_026-16#Text (дата звернення: 10.02.2026).

73. Про утворення міжвідомчої робочої групи з питань координації інтегрованого управління державним кордоном : Постанова Кабінету Міністрів від 30 січня 2029 року № 83. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/83-2019-%D0%BF#Text (дата звернення: 10.02.2026).

74. Про утворення координаційного центру управління державним кордоном : Постанова Кабінету Міністрів України від 12 квітня 2024 року № 426. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/83-2019-%D0%BF#Text (дата звернення: 11.02.2026).

75. Ганьба О. Б. Правові відносини у сфері прикордонної безпеки України: теоретико-правові засади : дис. … д-ра юрид. наук : 12.00.01. Івано-Франківськ, 2020. 552 С.

76. Білоусов М. Стратегія інтегрованого управління державним кордоном: БФ «Право на захист» дав рекомендації щодо дотримання прав іноземців і біженців. URL: https://r2p.org.ua/page/stratehiia-intehrovanoho-upravlinnia-derzhavnym-kordonom-bf-pravo-na-zakhyst-dav-rekomendatsii-shchodo-dotrymannia-prav-inozemtsiv-i-bizhentsiv (дата звернення: 13.02.2026).

77. Про особливості реалізації експериментального проекту з організації управління чергами автомобільних транспортних засобів перед міжнародними пунктами пропуску через державний кордон України для автомобільного

сполучення за допомогою електронної системи єЧерга : Постанова Кабінету Міністрів України від 02 грудня 2022 року № 1349. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1349-2022-%D0%BF#Text (дата звернення: 13.02.2026).

78. Про реалізацію експериментального проєкту з впорядкування черговості прибуття автомобільних транспортних засобів до міжнародних та міждержавних пунктів пропуску через державний кордон України з використанням електронної системи єЧерга : Постанова Кабінету Міністрів України від 05 грудня 2024 року № 1411. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1411-2024-%D0%BF#Text (дата звернення: 13.02.2026).

79. Про створення Системи в'їзду/виїзду (СВВ) для реєстрації даних про в'їзд та виїзд, а також даних про відмову у в'їзді громадян третіх країн, які перетинають зовнішні кордони держав-членів та про визначення умов доступу до СВВ для цілей правоохоронної діяльності, а також про внесення змін до Конвенції про імплементацію Шенгенської угоди та Регламентів (ЄС) № 767/2008 та (ЄС) № 1077/2011 : Регламент Європейського Парламенту та Ради (ЄС) 2017/2226 від 30 листопада 2017 року. URL: https://eur-lex.europa.eu/eli/reg/2017/2226/oj/eng (дата звернення: 13.02.2026).

80. Система в'їзду/виїзду до ЄС (EES). URL: https://www.irishimmigration.ie/uk/at-the-border/eu-entry-exit-system-ees/ (дата звернення: 13.02.2026).

81. ЄС змінює процедуру перетину кордону: чого очікувати. URL: https://eu-ua.kmu.gov.ua/en/news/yes-zminyuye-protseduru-peretynu-kordonu-chogo-ochikuvaty/ (дата звернення: 13.02.2026).

82. Про захист персональних даних : Проект Закону від 25 жовтня 2022 року № 8153. *Офіційний сайт Верховної Ради України*. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення: 13.02.2026).

83. Рада підтримала законопроєкт «Про захист персональних даних» у першому читанні. URL: https://eu4digitalua.eu/uk/news/rada-pidtrymala-

zakonoproyekt-pro-zahyst-personalnyh-danyh-u-pershomu-chytanni/ (дата звернення: 13.02.2026).

84. Д. Бойко. Захист персональних даних і ШІ: Законопроєкт №8153, GDPR та Закон ЄС про ШІ в контексті технологій штучного інтелекту. URL: https://dc.org.ua/news/zahyst-personalnyh-danyh-i-shi-zakonoproekt-8153-gdpr-ta-zakon-es-pro-shi-u-konteksti-tehnologiy-shtuchnogo-intelektu (дата звернення: 13.02.2026).

85. Про національну комісію з питань захисту персональних даних та доступу до публічної інформації : Проект Закону від 18 жовтня 2021 року № 6177. *Офіційний сайт Верховної Ради України*. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27996 (дата звернення: 14.02.2026).

86. Про внесення змін до статті 154 Кримінального процесуального кодексу України (щодо гарантії незалежності члена Національної комісії з питань захисту персональних даних та доступу до публічної інформації) : Проект Закону від 18 жовтня 2021 року № 6178. *Офіційний сайт Верховної Ради України*. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27997 (дата звернення: 14.02.2026).

87. Про внесення змін до пункту 12 частини сьомої статті 21 Закону України «Про єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» щодо додаткового захисту персональних даних : Проект Закону від 25 квітня 2022 року № 7314. *Офіційний сайт Верховної Ради України*. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/39502 (дата звернення: 14.02.2026).

88. Defense AI Center «A1»: Міноборони прискорює впровадження штучного інтелекту у війну. URL: https://mod.gov.ua/news/defense-ai-center-a1-minoboroni-priskoryuye-vprovadzhennya-shtuchnogo-intelektu-u-vijnu (дата звернення: 14.02.2026).

89. Проєкт Плану заходів на 2026–2028 роки щодо реалізації Стратегії інтегрованого управління державним кордоном України. *Офіційний сайт Державної прикордонної служби України.* URL: https://dpsu.gov.ua/uk/plan-

zahodiv-na-2026-2028-roki-shodo-realizaciyi-strategiyi-integrovanogo-upravlinnya-derzhavnim-kordonom-ukrayini (дата звернення: 14.02.2026).

90. Аналітичний дайджест Комітету АПУ з ІТ, медіа та захисту персональних даних: ключові зміни травня 2026 року. URL: https://uba.ua/eng/news/analtichnijj-dajjdzhest-komtetu-apu-z-it-meda-ta-zakhistu-personalnikh-danikh-kljuchov-zmni-travnja-2026-roku (дата звернення: 18.05.2026).

91. Про прикордонний контроль: Закон України від 05 листопада 2009 року № 1710-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1710-17#Text (дата звернення: 14.05.2026).

92. Про Державну прикордонну службу України: Закон України від 03 березня 2003 року № 661-IV. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 14.05.2026).

ВИСНОВКИ

У результаті проведеного дисертаційного дослідження вирішено актуальну наукову задачу, що полягає в удосконаленні адміністративно-правового забезпечення захисту персональних даних у сфері охорони державного кордону України, напрацювання механізмів її синхронізації з нормами європейської системи GDPR. Особливу увагу приділено удосконаленню правовим механізмам обробки та захисту персональних даних осіб, які перетинають державний кордон, а також виявленню прогалин та суперечностей у нормативно-правових актах, що регламентують діяльність Державної прикордонної служби України.

Зазначене дозволило сформулювати наступні основні висновки та пропозиції, що мають важливе теоретичне й практичне значення.

1. У процесі дослідження встановлено, що в сучасних умовах розвитку інформаційних технологій захист персональних даних у сфері охорони державного кордону України є важливим аспектом забезпечення національної безпеки в цілому. Попри різноманітність наукових підходів, сутність персональних даних визначається їх здатністю ідентифікувати фізичну особу, а відсутність єдиного понятійно-категорійного апарату зумовлює необхідність його уніфікації на законодавчому рівні.

2. На підставі проведеного аналізу обґрунтовано доцільність розмежування понять «охорона» та «захист», де охорона має превентивний, статичний характер, а захист – відновлювальний, активний характер. Ефективний захист персональних даних потребує комплексного підходу, який поєднує правові, організаційні та технічні механізми, а також підвищення правової обізнаності населення та вдосконалення національного законодавства. Тим самим, формування цілісної системи захисту персональних даних є необхідною умовою забезпечення балансу між правами людини, інтересами суспільства і держави в цілому.

3. Автором доведено, що персональні дані виступають самостійним предметом адміністративно-правового регулювання, оскільки їх обробка,

зберігання та використання безпосередньо пов’язані з реалізацією та захистом конституційних прав і свобод людини і громадянина. Стаття 32 Конституції України та положення Закону України «Про захист персональних даних» визначають базові гарантії недоторканості приватного життя, закріплюючи правові механізми захисту від неправомірного втручання державних органів чи інших суб’єктів в особисте життя, у зв’язку з обробкою персональних даних.

4. Обґрунтовано, що особливості захисту персональних даних у прикордонній сфері зумовлені специфікою діяльності Державної прикордонної служби України, яка здійснює обробку значних масивів інформації про осіб, які перетинають державний кордон України. Дослідження показало, що нинішня модель регулювання захисту персональних даних має певну асиметрію: детально врегульований механізм здійснення прикордонного контролю, водночас недостатньо чітко визначені гарантії щодо приватності. Виявлено основні проблеми: надмірність збору даних, що суперечить принципу мінімізації; нечіткість строків зберігання, що створює ризик необмежених масивів даних; широке коло доступ до баз даних, що підвищує ризик зловживань та витік інформації; недостатня прозорість здійснення збору даних для осіб, які перетинають кордон. З огляду на зазначене, запропоновано удосконалення чинної моделі захисту персональних даних у прикордонній сфері шляхом гармонізації з європейськими стандартами, визначення чітких строків зберігання та процедур видалення даних, обмеження доступу та забезпечення прозорості для громадян. Окремо підкреслено напрямки, механізми та засоби удосконалення прикордонного контролю, які мають базуватися на впроваджених стандартах GDPR, тобто на адаптованих до українських умов процедурах здійснення прикордонного контролю відповідно до вимог Регламенту ЄС про захист даних.

5. Визначено, що позитивними рисами чинного прикордонного законодавства України в частині захисту персональних даних осіб, які перетинають державний кордон України є законна мета обробки даних, формалізація процедур контролю та поступова гармонізація національного

законодавства з європейськими стандартами, зокрема з Регламентом ЄС 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних». Зазначене дозволить забезпечити належний рівень правових гарантій для осіб, які перетинають державний кордон України, щодо збереження персональних даних та підвищити ефективність та прозорість діяльності Державної прикордонної служби України, зміцнити довіру громадян до прикордонних органів, створити передумови для інтеграції України у європейський правовий простір, мінімізувати ризики неправомірного використання персональних даних в умовах гібридних загроз та кібератак, а також сприяти формуванню високої правової культури й обізнаності суспільства щодо захисту персональних даних.

6. Отримані результати свідчать, що Державна прикордонна служба України є ключовим суб'єктом захисту персональних даних у сфері забезпечення прикордонної безпеки та складової системи національної безпеки. Її правовий статус поєднує ознаки військового формування та правоохоронного органу спеціального призначення, що забезпечує ефективну реалізацію державної політики у сфері охорони державного кордону України та захисту персональних даних.

7. З'ясовано, що Державна прикордонна служба України виконує широкий спектр завдань, зокрема охорону та захист державного кордону України, здійснення прикордонного контролю, протидію незаконній міграції, оперативно-розшукову та контррозвідувальну діяльність, боротьбу з організованою злочинністю на державному кордоні, реагування на гібридні та інформаційні зовнішні загрози, а також забезпечення територіальної цілісності держави, що визначає її як провідного суб'єкта щодо захисту персональних даних.

8. Автором доведено, що цифровізація та діджиталізація є ключовими чинниками нинішньої трансформації суспільства та механізмів регулювання захисту персональних даних. Вони не лише оптимізують управлінські процеси та діяльність державних інституцій, зокрема Державної прикордонної служби України, але й формують нову правову реальність, де захист персональних даних

осіб, які перетинають державний кордон, стає невід'ємною складовою прикордонної безпеки як аспекту національної безпеки загалом.

9. З'ясовано, що цифровізація і діджиталізація, поряд із очевидними перевагами для оптимізації прикордонних процедур, водночас актуалізують потребу у створенні комплексної системи правових та організаційних гарантій захисту персональних даних. Виявлені прогалини у чинному законодавстві свідчать про необхідність розробки чітких правил щодо строків зберігання та процедур видалення даних, а також встановлення обмежень на їх передачу третім сторонам. Доцільно зазначити, що такий підхід дозволить мінімізувати ризики неправомірного використання інформації, забезпечити баланс між інтересами державної безпеки та правами людини, а також сприятиме формуванню сучасної моделі прикордонного контролю, яка відповідатиме європейським стандартам і міжнародним зобов'язанням України.

10. Установлено, що використання Державною прикордонною службою України інтегрованих інформаційно-комунікаційних систем «ГАРТ» та «Аркан» забезпечує здійснення ефективного прикордонного контролю шляхом автоматизації процесів перевірки осіб і транспортних засобів, а також створює умови для захисту значних масивів персональних даних. Водночас акцентовано увагу на тому, що функціонування зазначених систем потребує вдосконалення механізмів інформаційної безпеки, зокрема впровадження незалежних кібераудитів персоніфікованої ідентифікації, системного журналювання доступу, регулярного аудиту та інтеграції з іншими дотичними державними реєстрами, а також проведення стрес-тестів систем баз даних кордону (наприклад, Державною службою спецзв'язку та захисту інформації або міжнародними експертами), здійснення менеджменту інцидентів, тобто створення чітких протоколів швидкого реагування на випадок кібератак або компрометації даних пасажирів.

11. Доведено, що реалізація цих заходів дозволить гарантувати конфіденційність і цілісність даних, мінімізувати ризики їх неправомірного використання, забезпечити відповідність національних процедур європейським

стандартам захисту персональних даних, а також загалом підвищити рівень та ефективність діяльності Державної прикордонної служби України у забезпеченні національної безпеки.

12. Обґрунтовано, що адміністративно-правові механізми запобігання порушенням у сфері охорони персональних даних в умовах гібридного збройного конфлікту мають вкрай важливе значення для забезпечення національної безпеки України. Ефективне їх застосування дозволяє не лише мінімізувати ризики неправомірного доступу до інформації, але й забезпечити стабільність функціонування прикордонних інформаційних систем, які є критично важливими для захисту державного кордону України. У цьому контексті доцільним є напрацювання щодо удосконалення здійснення контролю за правоохоронним запитом, зокрема шляхом встановлення та запровадження жорстких судових або адміністративних фільтрів для передачі прикордонних даних іншим відомствам.

13. Установлено, що в умовах активних кібератак та інформаційних операцій особливого значення набувають превентивні заходи, спрямовані на створення передумов для формування комплексної моделі прикордонної безпеки, де захист персональних даних розглядається як невід'ємна складова національної безпеки, а ефективність адміністративно-правових заходів щодо захисту персональних даних стає ключовим чинником протидії гібридним загрозам.

14. Обґрунтовано, що міжнародний досвід є фундаментальною основою для формування сучасної системи захисту приватності в Україні. Європейський Союз, Рада Європи та інші міжнародні інституції виробили високі стандарти у сфері захисту персональних даних, які стали орієнтиром для національного законодавства. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» та її модернізована версія Конвенція 108+ закріпили базові принципи захисту даних шляхом законності, пропорційності, мінімізації та конфіденційності, а Хартія основоположних прав ЄС та Директива 95/46/ЄС «Про захист фізичних осіб при обробці персональних

даних і про вільне переміщення таких даних», а згодом і Загальний Регламент ЄС 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних» деталізували права суб'єктів даних та обов'язки контролерів, створивши уніфіковану систему захисту в межах Європейського Союзу. Україна, ратифікувавши Конвенцію № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» та Додатковий протокол, ухваливши Закон «Про захист персональних даних», взяла курс на гармонізацію свого законодавства з європейськими стандартами. Міжнародний досвід у згаданій сфері показує, що ефективний захист персональних даних можливий лише за умови співпраці державних органів, приватного сектору та громадянського суспільства, а також створення незалежних органів нагляду.

15. У процесі дослідження, автором вперше запропоновано низку положень, які формують нову якість адміністративно-правового регулювання захисту персональних даних у сфері охорони державного кордону України:

- запровадити обов'язкові оцінки впливу на захист даних (DPIA) для всіх інформаційних систем Державної прикордонної служби України, що дозволить системно управляти ризиками та забезпечити превентивний захист персональних даних;

- запропоновано доцільність введення інституту уповноваженої особи із захисту даних (DPO) у прикордонних органах, яка відповідатиме за дотримання чинного законодавства та реагування на виникаючі при перетині кордону інциденти;

- визначено доцільність встановлення чітких строків зберігання та процедури видалення персональних даних осіб, які перетинають державний кордон України, що забезпечить баланс між потребами державної безпеки та правами людини;

- запропоновано посилення парламентського та громадського контролю за діяльністю прикордонних органів у сфері обробки персональних даних, що сприятиме прозорості та підзвітності;

- обґрунтовано необхідність обмеження транскордонної передачі даних без належних гарантій конфіденційності та безпеки, що відповідає європейським стандартам;

- напрацьовані пропозиції щодо створення спеціальних підзаконних актів та інструкцій для прикордонних органів, які регламентують практичне застосування норм про захист персональних даних;

- доведено важливість підвищення рівня цифрової грамотності працівників Державної прикордонної служби України та впровадження регулярних тренінгів із кібербезпеки: навчання протидії фішингу, соціальній інженерії, правилам поводження з носіями інформації та застосування штучного інтелекту, що забезпечить належний рівень професійної компетентності у сфері інформаційної та кібернетичної безпек.

16. Напрацьовано комплекс адміністративно-правових положень, які спрямовані на формування сучасної моделі захисту персональних даних у прикордонній сфері, що відповідає європейським стандартам та стратегічному курсу України на євроінтеграцію.

Отримані теоретичні висновки та практичні рекомендації можуть бути використані для подальшого вдосконалення концептуальних основ розбудови інформаційного суспільства в Україні, а також для проведення подальших правових досліджень у цьому напрямі.

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Корж І. Ф., Кірієнко В. М. Політико-правова аберація: нігілізм та зброя. *Інформація і право*. 2023. № 1 (44). С. 9–24. URL: https://doi.org/10.37750/2616-6798.2023.1(44)

2. Корж І. Ф., Кірієнко В. М. Дискреція обмеження прав і свобод людини в Україні. *Сучасні аспекти науки*. 2023. С. 77–98. URL: http://perspectives.pp.ua/public/site/mono/mono-31.pdf

3. Кірієнко В. М. Основи прикордонної безпеки України. Organizational and legal fundamentals for the formation of a security environment in Ukraine: Scientific monograph. Riga, Latvia: Baltija Publishing, 2023. 342 p. С. 64–74. http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/386 https://doi.org/10.30525/978-9934-26-363-7-4

4. Кірієнко В. М. Захист персональних даних як аспекту, національної безпеки, в умовах збройного конфлікту. *Юридичний науковий електронний журнал.* 2024. № 1. С. 398–400. URL: https://doi.org/10.32782/2524-0374/2024-1/90

5. Кірієнко В. М. Загрози прикордонній безпеці в умовах збройного конфлікту. *Юридичний науковий електронний журнал*. 2024. № 2. С. 272–274. URL: https://doi.org/10.32782/2524-0374/2024-2/65

які засвідчують апробацію матеріалів дисертації:

1. Корж І. Ф., Кірієнко В. М., Корж Т. І. Дискреція обмеження прав і свобод людини. *Актуальні питання сучасної юриспруденції :* матеріали міжнародної наукової конференції (м. Ченстохова, Республіка Польща, 05–06 квітня 2023 року). Рига : *Baltija Publishing*, 2023. С. 14–18.

2. Кірієнко В. М. Захист персональних даних в умовах воєнного стану. *Актуальні питання юридичної науки :* матеріали всеукраїнської науково-

практичної конференції (м. Київ, 18 травня 2023 року). Одеса : Видавництво “Юридика”, 2023. С. 302–305.

3. Кірієнко В. М. Інформаційна безпека в умовах війни. *Проблеми інформаційно-правового забезпечення децентралізації державної влади та цифрової трансформації в Україні :* матеріали науково-практичної конференції (м. Вінниця, 15 червня 2023 року). Вінниця, 2023. Т.1. С. 88–91.

4. Кірієнко В. М. Охорона державного кордону – як складова сектору безпеки і оборони. *Науковий прогрес: інновації, досягнення та перспективи :* матеріали науково-практичної конференції (м. Мюнхен, Німеччина, 23–25 липня 2023 року). Німеччина : *MDCP Publishing,* 2023. С. 201–205.

5. Кірієнко В. М. Адміністративна відповідальність за порушення зберігання персональних даних. *Європейський науковий конгрес :* матеріали міжнародної науково-практичної конференції (м. Мадрид, Іспанія, 07–09 серпня 2023 року). Іспанія : *Barca Academy Publishing,* 2023. С. 170–175.

6. Кірієнко В. М. Захищеність персональних даних військовослужбовців Державної прикордонної служби України. *Європейський науковий конгрес :* матеріали міжнародної науково-практичної конференції (м. Мадрид, Іспанія, 04–09 вересня 2023 року). Іспанія : *Barca Academy Publishing,* 2023. С. 239–241.

7. Кірієнко В. М. Протидія інформаційній агресії та інформаційній пропаганді. *Нормативно-правова інформація і парламентський контроль :* матеріали науково-практичної конференції (м. Київ, 21 вересня 2023 року) / наук. керівник конф.: Д. В. Ланде; упоряд.: В. М. Фурашев, А. І. Нижник, С. О. Дорогих. Київ, 2023. С. 88–90.

8. Кірієнко В. М. Виклики та загрози прикордонній безпеці від впровадження в сучасне життя цифрових технологій. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання :* матеріали всеукраїнської науково-практичної конференції (м. Київ, 23 листопада 2023 року) / наук. керівник конф. О. А. Баранов; упоряд.: М. В. Дубняк, С. О. Дорогих. Київ, 2023. С. 108–111.

9. Кірієнко В. М. Протидія терористичним загрозам на державному кордоні України. *Актуальні проблеми протидії злочинності і корупції :* матеріали всеукраїнської науково-практичної конференції (м. Харків, 22 грудня 2023 року). Харків : *Юрайт*, 2023. С. 70–72.

10. Кірієнко В. М. Правові аспекти регулювання прикордонної безпеки. *Теоретичні та практичні проблеми реалізації норм права :* матеріали міжнародно науково-практичної конференції (м. Львів, 22–23 грудня 2023 року). Львів – Торунь : *Liha-Pres,* 2023. С. 200–203.

11. Кірієнко В. М. Захист персональних даних як аспект українсько-європейської співпраці у сфері прикордонної безпеки. *Сучасні виклики науки та освіти :* матеріали міжнародної науково-практичної конференції (м. Берлін, Німеччина, 15–17 січня 2024 року). Німеччина : *MDCP Publishing,* 2024. С. 593–596.

12. Кірієнко В. М. Захист персональних даних військовослужбовців Державної прикордонної служби України*. Сучасні виклики науки та освіти : матеріали міжнародної науково-практичної конференції* (м. Берлін, Німеччина, 12–14 лютого 2024 року). Німеччина *: MDCP Publishing,* 2024. С. 492–496.

13. Кірієнко В. М. Вплив корупції на ефективність діяльності правоохоронних органів в умовах воєнного стану. *Актуальні проблеми протидії корупції в умовах воєнного стану :* матеріали міжнародної науково-практичної конференції (м. Львів, 15 лютого 2024 року). Львів – Торунь : *Liha-Pres,* 2024. С. 65–68.

14. Кірієнко В. М. Методологічні засади удосконалення службової діяльності Державної прикордонної служби України в умовах цифровізації. *Реформування правоохоронних органів в Україні : актуальні питання та перспективи :* матеріали міжнародної науково-практичної конференції (м. Львів, 05 лютого 2026 року). Львів – Торунь : *Liha-Pres,* 2026. С. 81–84.

ДОДАТОК Б

Детальний шаблон DPIA (Оцінка впливу на захист даних) адаптований для прикордонних систем. Він структурований за ключовими розділами, які допоможуть системно оцінити ризики, правові підстави, технічні та організаційні заходи захисту персональних даних у сфері захисту державного кордону України.

DPIA (Оцінка впливу на захист даних) для прикордонних систем.

1. Опис операції обробки персональних даних:

1.1. Назва DPIA: _____

1.2. Дата проведення: _____

1.3. Версія: _____

1.4. Власник системи: _____

1.5. Відповідальна особа із захисту даних (DPO): _____

1.6. Обсяг і межі обробки (пункти пропуску, типи систем, категорії суб'єктів, типи даних): _____

1.7. Опис системи/процесу (що робить система, які дані збираються, як і де обробляються, які рішення приймаються): _____

1.8. Контекст використання (масові потоки, підвищенні ризики, інтеграція з іншими системами): _____

1.9. Типи систем (біометричний контроль, відеоспостереження, профілювання ризиків, обмін даними тощо): _____

1.10. Рівень автоматизації (ручна, напівавтоматична, автоматизована з людським контролем, повністю автоматизована): _____

2. Правові підстави та мета обробки:

2.1. Мета обробки (ідентифікація, верифікація, запобігання правопорушенням державного кордону, розшук, статистика тощо): _____

2.2. Правова підставка (конкретні закони, підзаконні акти, міжнародні договори): _____

2.3. Обмеження використання (заборона повторного використання без додаткової підстави): _____

2.4. Інформування суб’єктів (як і коли повідомляються особи про обробку, винятки): _____

3. Необхідність і пропорційність:

3.1. Обґрунтування необхідності кожної категорії даних: _____

3.2. Альтернативи з меншим втручанням: _____

3.3. Точність і актуальність даних (процедури перевірки, виправлення помилок): _____

3.4. Строки зберігання (терміни, умови видалення): _____

3.5. Модель доступу (хто має доступ, принцип найменших привілеїв, журналювання): _____

3.6. Права суб’єктів (доступ, виправлення, заперечення, право на людський перегляд автоматизованих рішень): _____

4. Карта потоків даних:

4.1. Джерела збору (сканери, камери, мобільні пристрої, API): _____

4.2. Передача даних (кому передаються, канали, міжнародні передачі): ___

4.3. Зберігання (локації, захист, резервні копії): _____

4.4. Доступ (ролі, права, аудит): _____

4.5. Видалення (процедури, відповідальні): _____

5. Оцінка ризиків для прав і свобод суб’єктів:

5.1. Ідентифікація ризиків (помилкова, ідентифікація, дискримінація, надмірний збір, розширення мети, витік даних, ризики передачі): _____

5.2. Оцінка ймовірності і впливу (шкала 1–5 для ймовірності та впливу, розрахунок ризику): _____

5.3. Опис сценаріїв шкоди (що може статися, які права порушуються, які наслідки для особи): _____

6. Заходи зниження ризиків:

6.1. Технічні заходи (шифрування, сегментація мереж, багатофакторна автентифікація, журналювання, псевдонімізація): _____

6.2. Організаційні заходи (політики доступу, навчання персоналу, контроль підрядників, дисциплінарні заходи): _____

6.3. Процедурні заходи (регламенти реагування на інциденти, аудит, тестування систем): _____

6.4. План впровадження заходів (хто відповідає, строки, статус виконання):

7. Залишковий ризик і рішення:

7.1. Опис залишкового ризику (що лишається після заходів, чи прийнятний): _____

7.2. Необхідність консультації з наглядовим органом: _____

7.3. Рішення керівництва (GO, GO з умовами, PAUSE, NO-GO): _____

7.4. Періодичність перегляду DPIA: _____

8. Додатки та доказова база:

8.1. Перелік документів (політики, інструкції, угоди, положення, регламенти, протоколи тестів, аудити): _____

8.2. Відомі інциденти (опис, наслідки, коригувальні дії): _____

8.3. План аудиту та метрики (частота перевірок, показники помилок, час реагування): _____

ДОДАТОК В

Проєкт

Закон України

«Про внесення змін до Закону України “Про прикордонний контроль” щодо захисту персональних даних»

Верховна Рада України постановляє:

І. Внести до Закону України «Про прикордонний контроль» такі зміни:

1. Після статті 2 доповнити Закон новими статтями 2-1, 2-2, 2-3, 2-4, 2-5, 2-6 такого змісту:

«Стаття 2-1. Принципи обробки персональних даних під час прикордонного контролю

1. Обробка персональних даних під час прикордонного контролю здійснюється на засадах законності, цільового призначення, мінімізації даних, точності, обмеження строку зберігання, цілісності та конфіденційності, підзвітності, недискримінації та пропорційності.
2. Збір і обробка персональних даних допускаються лише в обсязі, необхідному для здійснення прикордонного контролю, перевірки документів, встановлення особи, виявлення підстав для відмови у пропуску через державний кордон України та забезпечення національної безпеки.
3. Забороняється обробка персональних даних, яка не має безпосереднього зв’язку з метою прикордонного контролю.

Стаття 2-2. Обсяг персональних даних, що можуть оброблятися

1. Під час прикордонного контролю можуть оброблятися лише персональні дані, необхідні для досягнення мети, визначеної цим Законом.
2. Обробка біометричних даних допускається лише у випадках, прямо передбачених законом.
3. Перелік персональних даних, що можуть оброблятися під час прикордонного контролю, визначається Кабінетом Міністрів України з урахуванням вимог законодавства про захист персональних даних.»

«Стаття 2-3. Інформування осіб про обробку персональних даних

1. Особа, яка перетинає державний кордон України, має право на отримання інформації про мету, правові підстави, обсяг, строки зберігання та порядок обробки її персональних даних.
2. Інформування здійснюється у доступній та зрозумілій формі до або під час обробки персональних даних, якщо інше не передбачено законом.
3. Порядок та форма інформування осіб про обробку персональних даних визначаються Кабінетом Міністрів України.»

Стаття 2-4. Автоматизована обробка персональних даних та використання біометричних технологій

1. Автоматизована обробка персональних даних під час прикордонного контролю допускається за умови забезпечення людського контролю у випадках, коли рішення може істотно вплинути на права та свободи особи.
2. Використання біометричних технологій під час прикордонного контролю здійснюється з дотриманням вимог законодавства про захист персональних даних та інформаційну безпеку.
3. Рішення, що істотно впливає на права та свободи особи, не може ухвалюватися виключно автоматизованими засобами без можливості його перегляду уповноваженою службовою особою.
4. Порядок застосування автоматизованих і біометричних засобів визначається Кабінетом Міністрів України.»

Стаття 2-5. Строки зберігання, знищення та знеособлення персональних даних

1. Персональні дані, отримані під час прикордонного контролю, зберігаються протягом строку, необхідного для досягнення мети їх обробки, якщо інше не встановлено законом.
2. Після спливу строку зберігання персональні дані підлягають знищенню або знеособленню.
3. У разі якщо персональні дані пов’язані з кримінальним, адміністративним або іншим провадженням, строк їх зберігання визначається відповідно до закону.
4. Порядок зберігання, знищення та знеособлення персональних даних визначається Кабінетом Міністрів України.»

Стаття 2-6. Доступ до персональних даних та їх передача

1. Доступ до персональних даних, що обробляються під час прикордонного контролю, надається лише уповноваженим особам у межах їхніх повноважень.
2. Передача персональних даних іншим органам державної влади допускається лише у випадках, передбачених законом.
3. Міжнародна передача персональних даних допускається за наявності правової підстави та належних гарантій захисту персональних даних.
4. Усі дії з доступу до персональних даних підлягають обов'язковому обліку та документуванню.
5. Порядок доступу до персональних даних та їх передачі визначається Кабінетом Міністрів України.»

Стаття 2-7. Оцінка впливу на захист персональних даних

1. Запровадження нових інформаційних систем, технологій або процедур прикордонного контролю, що передбачають обробку персональних даних, здійснюється після проведення оцінки впливу на захист персональних даних.
2. Порядок проведення оцінки впливу на захист персональних даних визначається Кабінетом Міністрів України.»

II. Прикінцеві та перехідні положення

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.
2. Кабінету Міністрів України у шестимісячний строк з дня набрання чинності цим Законом:

– привести свої нормативно-правові акти у відповідність із цим Законом;
– затвердити порядок інформування осіб про обробку персональних даних;
– затвердити порядок застосування автоматизованих і біометричних засобів;
– затвердити порядок проведення оцінки впливу на захист персональних даних;
– затвердити порядок зберігання, знищення та знеособлення персональних даних;
– затвердити порядок доступу до персональних даних та їх передачі.

3. Державній прикордонній службі України у шестимісячний строк з дня набрання чинності цим Законом привести свої внутрішні нормативні акти, регламенти та інформаційні системи у відповідність із цим Законом.

ДОДАТОК Г

ДОВІДКА

про впровадження результатів наукового дослідження

Видана аспіранту Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» Кірієнко Віктору Миколайовичу в тому, що напрацьовану ним у процесі дисертаційного дослідження за темою «Адміністративно-правове забезпечення захисту персональних даних у сфері охорони державного кордону України» методику DPIA (Оцінка впливу на захист даних), структуровану за ключовими розділами, що дозволяє системно оцінювати ризики, правові підстави, технічні та організаційні заходи захисту персональних даних у сфері охорони державного кордону України вивчено в Адміністрації Державної прикордонної служби України.

Зазначена методика прийнята до уваги і може бути врахована у подальшій службовій діяльності.

Помічник Голови Державної
прикордонної служби України полковник Андрій ПРОСТАКОВ

Заступник начальника Управління
Юридичного забезпечення полковник юстиції Сергій ЛОПАТЮК

«10» червня 2026 року