**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

Кваліфікаційна наукова
праця на правах рукопису

**ЦЬОМЕНКО АЛІНА ВОЛОДИМИРІВНА**

УДК 342.9:347.181:351.746:004.72.056.52(043.3)

**ДИСЕРТАЦІЯ**

# АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН СУБ'ЄКТАМИ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ

**08 –** Право
**081 –** 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
**_____** А.В. Цьоменко

Науковий керівник **– Пашинський Володимир Йосипович,** доктор юридичних наук, доцент

**Київ – 2024**

# АНОТАЦІЯ

**Цьоменко Аліна Володимирівна.** Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації**.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – «Право» – Міністерство освіти і науки України Київський національний університет імені Тараса Шевченка, Київ, 2024.

Дисертаційне дослідження спрямоване на вирішення комплексу теоретичних і практичних проблем адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації.

Дисертаційна робота є одним із перших у вітчизняній адміністративно-правовій науці дослідженням теоретичних і практичних проблем адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації. Проведений аналіз генези нормативно-правового забезпечення захисту персональних даних дозволив нам виділити чотири етапи розвитку та становлення системи нормативно-правового забезпечення захисту персональних даних в Європі та Україні.

Наголошено, що аналіз теоретичних підходів щодо розуміння поняття персональних даних дозволяє зробити таке визначення поняття «персональні дані громадян» як будь-які відомості або дані, в об'єктивізованій формі, що стосуються суб'єкта даних (фізичної особи), який підлягає ідентифікації.

Персональним даним громадян притаманні наступні ознаки: інформаційний зміст персональних даних – відомості або дані про конкретну фізичну особу; ідентифікуючі властивості – дозволяють визначити (ідентифікувати) конкретну фізичну особу; визначена форма фіксації у певному джерелі (носії) персональних даних; не вичерпність; правова форма персональних даних, яка розпочинається із початком сукупності дій пов'язаних із їх обробкою та забезпеченням захисту.

Зазначено, що суб'єкт персональних даних – це конкретна фізична особа, персональні дані якої обробляються, тобто, підлягають збиранню, зміні, зберіганню та захисту з метою ідентифікації цієї особи, у тому числі з використанням інформаційних технологій та штучного інтелекту. При цьому суб'єктів персональних даних класифіковано за наступними критеріями. За рівнем законодавчого регулювання: такі, що підпадають під дію загального законодавства в сфері персональних даних та спеціального законодавства. За сферою суспільних відносин: медична сфера (фізичні особи: пацієнти, медичний персонал), фінансова сфера (фізичні особи: клієнти банків та інших фінансових установ), освітня сфера (фізичні особи: кандидати на вступ, здобувачі освіти, науково-педагогічні кадри, адміністративні працівники освітніх установ), сфера надання публічних послуг (фізичні особи: громадяни, що звертаються за отриманням публічних послуг, державні службовці), сфера реалізації виборчих прав (фізичні особи- виборці) та інші. Запропоновано поділ суб'єктів персональних даних, виходячи з загальної класифікації фізичних осіб, тобто поділ на громадян, не громадяни (іноземці, особи без громадянства та інші).

Вперше визначено поняття «адміністративно-правове забезпечення захисту персональних даних громадян» – це врегульована адміністративними нормами системна діяльність суб'єктів публічної адміністрації щодо адміністративно-правового регулювання, реалізації, охорони та захисту суспільних відносин у сфері персональних даних.

В свою чергу, структура адміністративно-правового забезпечення захисту персональних даних, як окрема група суспільних відносин, враховуючи її специфіку, буде складатися з таких елементів: 1) об'єкт адміністративно-правового забезпечення персональних даних; 2) суб'єкт адміністративно-правового забезпечення персональних даних; 3) норми адміністративного права щодо забезпечення захисту персональних даних; 4) адміністративно-правові відносини в сфері забезпечення захисту персональних даних та їх зміст;

5) гарантії адміністративно-правового забезпечення захисту персональних даних включають.

Під суб'єктом адміністративно-правового забезпечення захисту персональних даних громадян пропонується розуміти орган публічної адміністрації, який здійснює публічне управління у сфері захисту персональних даних в процесі реалізації прав громадян та надання адміністративних послуг, компетенція якого включає правове регулювання, збір, обробку, зберігання та забезпечення захисту персональних даних.

Суб'єктів адміністративно-правового забезпечення класифіковано за наступними критеріями: 1) за сферами діяльності та повноваженнями: на цивільні та мілітаризовані; 2) за сферами повноважень: публічні та приватні; 3) на суб'єкти забезпечення захисту персональних даних, що забезпечують захист загальних персональних даних та суб'єкти, що забезпечують захист особливо чутливих та конфіденційних персональних даних.

Проведений аналіз нормативно-правового регулювання повноважень суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян дозволяє стверджувати про наявність прогалин у чинному законодавстві та необхідності удосконалення як порядку здійснення повноважень в сфері забезпечення захисту персональних даних, так і розширення змісту та уточнення таких повноважень на рівні законодавчому рівні у відповідності до стандартів ЄС.

Захист персональних даних здійснюється за допомогою інструментів адміністративно-правового забезпечення. Інструменти адміністративно-правового забезпечення захисту персональних даних громадян – це врегульовані нормами адміністративного права зовнішні прояви конкретних дій уповноважених суб'єктів публічної адміністрації, в рамках яких реалізуються і за допомогою яких здійснюються регулюючий вплив на суспільні відносини у сфері обігу персональних даних для забезпечення прав та законних інтересів суб'єктів цих правовідносин. Інструменти адміністративно-правового забезпечення захисту персональних даних

громадян можна поділити на: загальні (універсальні) та локальні (відомчі); нормативно-правові законодавчого та підзаконного характеру, а також нормативно визначені концепції та стратегії забезпечення захисту персональних даних громадян; індивідуальні (адміністративні) акти та фактичні дії; контрольно-наглядові, моніторингові, організаційно-управлінські та технічні інструменти забезпечення захисту персональних даних громадян.

Аналіз досвіду ЄС щодо адміністративно-правового забезпечення персональних даних дає підстави зазначити, що основними завданнями України в контексті євроінтеграції в зазначеній сфері є здійснення правових та організаційних заходів за такими напрямками: а) приведення національного законодавства щодо захисту персональних даних до стандартів ЄС, що визначається нами також як невід'ємна складова європейської інтеграції України; б) визначення на законодавчому рівні системи органів публічного контролю за забезпеченням захисту персональних даних, що відповідає законодавству ЄС. Виконання зазначених завдань вимагає внесення змін до національного законодавства в сфері забезпечення захисту персональних даних, зокрема, створення єдиного окремого органу державної влади, який буде визначати стандарти обробки та безпеки персональних даних, здійснювати контроль за суб'єктами публічної влади щодо забезпечення захисту персональних даних, удосконалювати термінологію та визначення понять «захисту персональних даних», «порушення захисту персональних даних», а також визначатиме коло повноважень органів державної влади та органів місцевого самоврядування щодо забезпечення захисту персональних даних.

Сформульовані у дисертації висновки, пропозиції та практичні рекомендації є основою для удосконалення законодавчих актів з питань адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації, підвищення ефективності діяльності суб'єктів адміністративно-правового забезпечення захисту персональних даних, а також можуть бути використані у законотворчій,

правозастосовній діяльності, в навчальному процесі під час підготовки фахівців в галузі права.

**Ключові слова:** адміністративно-правове забезпечення захисту персональних даних, біометричні дані, види персональних даних, доступ до публічної інформації, захист персональних даних, інструменти адміністративно-правового забезпечення захисту персональних даних, інформація про особу, публічне управління, суб'єкти публічної адміністрації, персональні дані громадян, суб'єкти публічної влади, суб'єкти адміністративно-правового забезпечення персональних даних, суб'єкти персональних даних, штучний інтелект, цифрові технології.

## ABSTRACT

**Alina Tsomenko.** Administrative and legal protection of personal data of citizens by the subjects of public administration. – Qualifying scientific work as a manuscript.

Dissertation for the Doctor of Philosophy degree in specialty 081 - "Law" - Ministry of Education and Science of Ukraine, Taras Shevchenko Kyiv National University, Kyiv, 2024.

This dissertation is aimed at solving a complex of theoretical and practical problems related to the administrative and legal protection of personal data of citizens by the subjects of public administration.

The dissertation is one of the first in the domestic administrative and legal science to study a set of theoretical and practical problems of administrative and legal protection of personal data of citizens by the subjects of public administration. The analysis of the genesis of legal protection of personal data allowed us to identify four stages of development and establishment of the system of legal protection of personal data in Europe and Ukraine.

It is emphasized that the analysis of theoretical approaches to understanding the concept of personal data allows us defining the notion of "personal data of

citizens" as any information or data, in an objectified form, related to the data subject (an individual) that is subject to identification.

Personal data of citizens have the following characteristics: informational content of personal data i.e., information or data on a specific individual; identifying properties i.e., they allow identifying a specific individual; defined form of record in a certain personal data source (medium); inexhaustibility of data; and legal form of personal data, which starts from a number of actions related to their processing and protection.

It is noted that the subject of personal data is a specific individual, whose personal data is processed, i.e., subject to collection, change, storage and protection for the purpose of identifying this person, to include by means of information technologies and artificial intelligence. At the same time, the subjects of personal data are classified according to the following criteria. According to the level of legislative regulation: those, subject to general legislation in the field of personal data, and special legislation. According to the field of public relations: medicine (individuals: patients, medical staff), finances (individuals: banks and other financial institutions clients), education (individuals: candidates for admission, students, scientific and pedagogical personnel, educational institutions administrative staff), public services (individuals: the citizens applying for public services, civil servants), exercise of electoral rights (individuals-voters) etc. It is proposed to divide personal data subjects based on the general classification of individuals i.e., into citizens and non-citizens (foreigners, stateless persons etc.).

For the first time, the concept of "administrative and legal protection of personal data of citizens" was defined as a systemic activity of the subjects of public administration regulated by administrative norms on administrative and legal regulation, implementation, security and protection of public relations in the field of personal data.

In turn, the structure of administrative and legal protection of personal data, as a separate group of social relations, given its specificity, includes the following elements: 1) the object of administrative and legal protection of personal data; 2) the

subject of administrative and legal protection of personal data; 3) norms of administrative law regarding protection of personal data; 4) administrative and legal relations in the field of personal data protection and their content; 5) the guarantees of administrative and legal protection of personal data.

It is proposed to construe the subject of administrative and legal protection of personal data of citizens as a body of public administration that ensures personal data protection in the process of exercising the citizens' rights and providing administrative services, and the competence of which includes legal regulation, collection, processing, storage and protection of personal data.

The subjects of administrative and legal protection are classified according to the following criteria: 1) in terms of activity and powers: civilian and militarized; 2) public and private; 3) those that ensure protection of general personal data and those that ensure protection of particularly sensitive and confidential data.

The analysis of the regulatory and legal governing of powers of the subjects of administrative and legal protection of personal data of citizens allows us saying of the presence of gaps in applicable legislation and the need to improve both the procedure for exercising powers in the field of personal data protection, and expanding the content and clearness of such powers at the legislative level in accordance with the EU standards.

The protection of personal data is carried out with the help of administrative and legal support tools, which, inter alia, include external manifestations of specific actions of the authorized subjects of public administration regulated by the Administrative Law, within the scopes of which regulatory influence on social relations in the field of personal data circulation is implemented, and with the help of which regulatory influence in the field of personal data circulation to ensure rights and lawful interests of the subjects of these legal relationships, is carried out. These tools can be divided into: general (universal) and local (departmental); regulatory - of a legislative and bylaw nature, as well as regulatory defined concepts and strategies for ensuring the protection of personal data of citizens; individual (administrative) measures and actual actions; control and supervision, monitoring, organizational and

management, as well as technical tools for ensuring the protection of personal data of citizens.

The analysis of the EU's practice in the field of administrative and legal protection of personal data allows us noting that the main tasks of Ukraine in the context of European integration in the specified field are implementation of the following legal and organizational measures: a) bringing the national legislation on the personal data protection to the EU standards, which is an integral part of the European integration of Ukraine; b) determination at the legislative level of the system of public controlling bodies for ensuring personal data protection meeting the EU legislation. To fulfil the foregoing, it is requited to amend the national legislation in the field of ensuring personal data protection, in particular, to establish a single and independent state body that will determine the standards for processing and securing personal data, control the activity of public authorities in terms of ensuring personal data protection, improve the terminology and definition of "personal data protection" and "personal data protection breach" concepts, and will determine the scope of powers of state authorities and local self-government bodies to ensure personal data protection.

The findings, proposals and practical recommendations outlined in the dissertation are the basis for the improvement of legislative acts on the administrative and legal protection of personal data of citizens by the subjects of public administration, increasing the efficacy of their activities, and can also be used in law-making, law-enforcement activities, as well as in the educational process to train specialists in the field of law.

**Key words:** administrative and legal protection of personal data, biometric data, types of personal data, access to public information, personal data protection, personal data protection administrative and legal tools, information on a person, public administration, subjects of public administration, personal data of citizens, subjects of public authority, subjects of administrative and legal protection of personal data, personal data subjects, artificial intelligence, digital technologies.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Цьоменко А. В. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 1 (53), 2023. Київ, С. 41-45. URL:https://miljournals.knu.ua/index.php/visnuk/article/view/1028/955 (дата звернення 25.04.2024 р.)

2. Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян : поняття та структура. Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія» ) Випуск № 10(40) 2023. С. 678-688. DOI: https://doi.org/10.52058/2708-7530-2023-10(40)-678-688.

3. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 4 (52), 2022. Київ, С. 50-53. URL:https://miljournals.knu.ua/ index.php/visnuk/article/view/1006/945. (дата звернення 25.07.2023 р.)

4. Pashynskyi Volodymyr, Tsomenko Alina. Administrative-legal support for the protection of citizens personal data: contemporary theoretical approaches. Visegrag journal on human rights № 4 (2023) P. 55 -61.

які засвідчують апробацію матеріалів дисертації:

1. Цьоменко А.В. Захист персональних даних органами публічної влади в умовах війни. Права людини та публічне врядування в сучасних умовах : Матеріали V Міжнародного правничого форуму, 10 червня 2022 р., м. Чернівці

/ Уклад. І.В. Ковбас, І.І. Бабін, О.І. Ющик, І.Ж. Торончук, П.І. Крайній. Чернівці: Технодрук, 2022. С.268-270.

2. Цьоменко А.В. Європейська рада щодо захисту персональних даних, як незалежний орган спеціальної компетенції європейського союзу. Права людини як індикатор розвитку сучасної держави: матеріали Міжнародної науково-практичної конференції (13 грудня 2021 року) / За ред. О. Васильченко; Є. Герасименко, О. Сінькевич, А. Матат. Київський національний університет імені Тараса Шевченка. Київ: «Видавництво Людмила», 2021. С.209-211.

3. Цьоменко А.В. Забезпечення захисту персональних даних військовослужбовців в умовах війни. Адаптація правової системи України до Європейського союзу: теоретичні та практичні аспекти Всеукраїнська науково-практична конференція з нагоди 20-ї річниці заснування Полтавського юридичного інституту Національного юридичного університету імені Ярослава Мудрого (29 вересня 2022 року) Полтава: зб.наук.пр./ укладачі В.М. Божко, П.П. Нога. С. 308-310.

4. Цьоменко А.В. Публічно-правовий контроль за обігом персональних даних як засіб захисту від зловживання правом. Актуальні питання розвитку юридичної науки і практики в умовах воєнного стану та мирної розбудови: матеріали Міжнародної науково-практичної конференції (5 травня 2023 року): ел. збірник. Київ: Київський національний університет імені Тараса Шевченка, 2023., С.241-243.

5. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян у контексті використання програм «штучного інтелекту» VI Міжнародно правовий форму Права людини та публічне врядування в сучасних умовах: матеріали V Міжнародного правничого форуму (10 червня 2022) м. Чернівці/ Уклад. І.В. Ковбас, І.І. Бабін, О.І. Ющик, І.Ж. Торончук, П.І. Крайній,. Чернівці: Технодрук, 2022. С. 237-240.

6. Пашинський В.Й., Цьоменко А.В. Міжнародно-правовій звичай у сфери захісту персональних даних. Актуальні питання державотворення та

захисту прав людини в Україні: зб. наук. пр. / гол. ред. Л. Г. Білий. Хмельницький: Вид-во Хмельниц. ін-ту МАУП, 2024. Вип. 13. 249-255 с.

7. Цьоменко Аліна. Європейські стандарти адміністративно-правового забезпечення захисту персональних даних громадян: Публічна влада: проблеми реалізації повноважень в умовах воєнного стану та відбудовного періоду. Матеріали Міжнародної науково-практичної конференції (22 лютого 2024 року): електр. збірник / Ред. кол.: О. Васильченко; П. Діхтієвський; Т. Коломоєць; А. Мамула; В. Мушенок; В. Пашинський. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 134-139.

8. Цьоменко Аліна, Цьоменко Алла. Публічна інформація як важливий ресурс та результат процесу адміністрування. Матеріали Міжнародної науково-практичної конференції (22 лютого 2024 року): електр. збірник / Ред. кол.: О. Васильченко; П. Діхтієвський; Т. Коломоєць; А. Мамула; В. Мушенок; В. Пашинський. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 371-374.

# ЗМІСТ

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ – Верховна Рада України

GDPR – General Data Protection Regulation (Загальний регламент про захист даних)

Директива 2002/58/ЄС – Директива (ЄС) 2002/58/ЄС Європейського Парламенту і Ради «Щодо обробки персональних даних та захисту конфіденційності в секторі електронних засобів зв'язку»

Директива 2016/681 – Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. «Про використання даних записів реєстрації пасажирів»

ДРФО – Державний реєстр фізичних осіб-платників податків

ЕСОЗ – Електронна система охорони здоров'я

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

ІКС – Інформаційній комунікаційна система

КМУ – Кабінету Міністрів України

МВС України – Міністерство внутрішніх справ України

Мін'юст – Міністерство юстиції України

Мінцифри – Міністерство цифрової трансформації України

ЕМІС – Електронна медична інформаційна система

МОЗ України – Міністерство охорони здоров'я України

МОН України – Міністерство освіти і науки України

МОУ – Міністерство оборони України

НСЗУ – Національної Служби Здоров'я України

Позиція WP 136 – Позиція про концепцію персональних даних від 20 червня 2007 року

СБУ – Служба безпеки України

Уповноважений ВРУ – Уповноважений Верховної Ради України з прав людини

ЦБД – Центральна база даних

# ВСТУП

**Обґрунтування вибору теми дослідження.** Розбудова України як європейської, демократичної, правової держави, де найвищою цінністю є людина і її права, вимагає створення та ефективного функціонування інститутів публічної влади, які забезпечують реалізацію та захист основних прав та свобод громадян. Провідне місце у системі таких прав наразі належить правам пов'язаним з забезпеченням захисту персональних даних громадян, без чого неможлива реалізація конституційних прав і свобод громадян України суб'єктами публічної влади.

Радикальні інновації у сфері інформаційних технологій призводять до поглиблення різноманітних аспектів захисту прав і свобод людини, невід'ємною складовою, яких є обробка і захист персональних даних.

Актуальність теми дисертаційного дослідження пов'язана із швидким запровадженням інформаційних технологій та процесів у всіх сферах публічного адміністрування через створення різноманітних баз даних та доступу органів публічної влади до персональних даних громадян і необхідністю забезпечення їх захисту. Активна розбудова електронного врядування та процеси цифрової трансформації управлінської діяльності в Україні та світі загалом, визначають завдання щодо формування «держави в смартфоні», здійснення «цифровізації економіки» та проведення «цифрових трансформацій» в органах публічної влади. Все це вимагає створення правових механізмів забезпечення захисту персональних даних громадян.

Сучасні темпи розвитку інформаційних технологій та обробки персональних даних в системі публічного адміністрування загострили проблему захисту персональних даних суб'єктами публічної адміністрації. Це вимагає врахування міжнародного досвіду щодо обробки і захисту персональних даних суб'єктами публічної адміністрації, а також врахування національного досвіду щодо діяльності суб'єктів публічної адміністрації в

забезпечені прав і свобод людини, у тому числі права на захист персональних даних.

Особливої актуальності зазначене питання набуло у контексті європейської інтеграції України та заходів щодо імплементації в національне законодавство європейських стандартів та норм, які стосуються обробки та захисту персональних даних.

Становленню ефективної системи адміністративно-правового забезпечення захисту персональних даних в Україні перешкоджають прогалини у законодавчій базі, відсутність системних підходів щодо удосконалення чинного законодавства, в тому числі щодо запровадження правових механізмів обробки та захисту персональних даних. З огляду на це з'являється потреба у напрацюванні пропозицій щодо удосконалення чинного законодавства в частині забезпечення захисту персональних даних громадян. Особлива увага повинна бути приділена створенню надійних механізмів для забезпечення конфіденційності, цілісності та забезпечення захисту персональних даних окремих вразливих категорій громадян.

Особливої актуальності тема адміністративно-правового забезпечення захисту персональних даних громадян набуває в умовах повномасштабної російської збройної агресії проти України, окупації частини її території та необхідністю посилення захисту в цих умовах персональних даних громадян, особливо вразливих категорій. З метою захисту суверенітету та територіальної цілісності в державі було запроваджено адміністративно-правовий режим воєнного стану, що вимагає формування особливих підходів до забезпеченням захисту персональних даних вразливих категорій громадян України, зокрема внутрішніх біженців, переселенців, військовослужбовців, військовозобов'язаних або військовополонених. Відтак є необхідність враховувати специфічні загрози та виклики, які виникають в умовах воєнного стану для вразливих категорій громадян.

**Стан розробки у вітчизняній та зарубіжній науці.** Теоретичні та практичні питання адміністративно-правового забезпечення захисту

персональних даних громадян досліджувалися у працях окремих вітчизняних учених. Зокрема, сутність персональних даних і окремі аспекти забезпечення їх адміністративно-правового захисту досліджували такі вчені як П.В. Діхтієвський, М. Ю. Блохін, В.М. Брижко, Р.В. Ігонін, Н. А. Загребельна, Н.Ю. Задирака, О.А. Заярний, Р.А. Калюжний, А.В. Кучеренко, С.Й. Литвин, П.С. Лютіков, А. М. Мартинова, А. М. Новицький, А.В. Пазюк, В.Й. Пашинський, О.О. Пунда, В.П. Радкевич, М.В. Різак, К.М. Рудой, О. П. Світличний, В.О. Серьогін, І.М. Сопілко, В.І. Теремецький, А.В. Тунік, А.М. Чвалюк, О.О. Шарибурина, М.Я. Швець, Д.В. Цвірюк, Я. Г. Худолєй та інші.

Незважаючи на наявність вагомих напрацювань у зазначеній сфері, більшість теоретичних і практичних питань адміністративно-правового забезпечення захисту персональних даних громадян залишається невирішеними.

Науковцями не були охоплені питання адміністративно-правового забезпечення захисту персональних даних громадян суб’єктами публічної адміністрації, що підтверджує актуальність обраної теми, враховуючи її теоретичну та практичну значимість з огляду на розвиток адміністративного права в правовій системі України, входження країни до Європейського Союзу, сучасних викликів повномасштабної російської агресії.

Водночас, варто підкреслити, що питання комплексного дослідження проблематики адміністративно-правового забезпечення захисту персональних даних громадян суб’єктами публічної адміністрації не розглядалися, а тому є надзвичайно актуальним, що зумовлює доцільність їх розгляду на рівні дисертаційного дослідження.

Відповідно, дослідження правової природи, змісту поняття та видів персональних даних, суб’єктів адміністративно-правових відносин, пов'язаних із персональними даними, інструментів адміністративно-правового забезпечення захисту персональних даних громадян, адміністративно-правового забезпечення захисту персональних даних громадян матиме важливе

наукове й практичне значення, спрямоване на оптимізацію сучасних відносин у сфері персональних даних, відповідно до європейських стандартів та практики.

**Зв'язок роботи з науковими програмами, планами, темами, грантами.**

На виконання основних положень Закону України «Про пріоритетні напрями розвитку науки і техніки» від 11 липня 2001 року № 2623-III; Постанови Кабінету Міністрів України від 7 вересня 2011 р. № 942 «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року»; Постанови Кабінету Міністрів України від 30 січня 2019 № 56 «Деякі питання цифрового розвитку»; п. 13 Розвиток публічного адміністрування в Україні в умовах цифровізації Розділу 1.3., п. 12 Правове забезпечення формування та реалізації державної політики в сфері цифрових технологій з питань захисту персональних даних, охорони інтелектуальної власності, п. 17 Впровадження та розповсюдження Інтернету речей, Великих даних (BigData), вирішення проблем захисту персональних даних, п. 18 Розробка пропозицій щодо вдосконалення державної політики у сфері захисту інформації, формування примірного переліку цифрових прав громадян з урахуванням європейських вимог та рекомендацій Організації Об'єднаних Націй Розділу 1.8. Стратегії розвитку наукових досліджень Національної академії правових наук України на 2021 – 2025 роки, затвердженої Постановою загальних зборів Національної академії правових наук України від 26.03.2021 р. № 12–21 року, а також відповідно до науково-дослідної теми «Розробка системного вчення про основні права людини з метою втілення в Україні європейських правових цінностей у контексті розбудови громадянського суспільства» № 19 БФ 042-01, яка досліджується у Навчально-науковому інституті права Київського національного університету імені Тараса Шевченка та стратегічної теми Наукових досліджень кафедри адміністративного права та процесу «Концептуальні засади розвитку вітчизняного адміністративного та

адміністративного процесуального права в умовах нового часу: виклики, рішення, європейський вектор» затвердженої Вченою радою Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка № 17 від 30 квітня 2024 року.

Тема дисертації затверджена Вченою радою Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка № 4 від 25 жовтня 2021 року.

**Мета і завдання дослідження.** Мета полягає в тому, щоб на основі досягнень юридичної науки, аналізу національного законодавства України та практики його застосування, досвіду Європейського Союзу вирішити комплекс теоретичних і практичних проблем адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації.

Для досягнення поставленої мети були визначені такі наукові дослідницькі завдання:

розглянути генезу становлення та розвитку нормативно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації;

розкрити сутність та окреслити характерні ознаки поняття та видів персональних даних;

визначити суб'єктів адміністративно-правових відносин, пов'язаних із персональними даними;

охарактеризувати поняття та зміст адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації;

розглянути систему та повноваження суб'єктів публічної адміністрації щодо адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації;

охарактеризувати інструменти адміністративно-правового забезпечення захисту персональних даних громадян;

висвітлити європейський досвід адміністративно-правового забезпечення захисту персональних даних суб'єктами публічної адміністрації;

розробити на цій основі пропозиції і рекомендації вдосконалення адміністративно-правового забезпечення захисту персональних даних.

**Об'єктом дослідження** є суспільні відносини у сфері адміністративно-правового забезпечення захисту персональних даних громадян.

**Предметом дослідження** є адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації.

**Методи дослідження.** В ході наукового дослідження використано комплексний підхід та сукупність філософських, загальнонаукових та спеціально-юридичних методів пізнання, що дозволило дослідити проблеми адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації та вирішити поставлені завдання відповідно до мети дослідження.

Застосування діалектичного методу дозволило дослідити правову природу персональних даних, забезпечення захисту персональних даних в їх нерозривному розвитку в системі суспільних відносин у взаємозв'язку з іншими суспільними явищами і процесами та з використанням інших методів наукового дослідження. Такі загально-наукові методи дослідження як аналіз та синтез стали основними інструментами у межах всієї наукової роботи з дослідження наукових поглядів в сфері адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації.

За допомогою формально-логічного та історико-правового методів визначене поняття та досліджено генезу персональних даних як правового інституту (підрозділ 1.1, 1.2). За допомогою аналітичного методу було досліджено систему суб'єктів персональних даних, суб'єктів адміністративно правового забезпечення, сучасний стан законодавства щодо особливостей публічного адміністрування у сфері забезпечення захисту персональних даних та розроблено пропозиції з удосконалення правової бази щодо

адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації (підрозділ 1.2, 1.3, 2.2).

Системно-логічний метод застосовувався при виявленні ознак механізму публічного адміністрування у сфері адміністративно-правового забезпечення захисту персональних даних громадян (підрозділ 2.1). Застосування системного та порівняльно-правового методу дало змогу дослідити систему нормативно-правових актів, що регулюють адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації (підрозділ 2.2, 2.3).

Компаративістський метод був застосований для проведення дослідження та порівняння генези розвитку адміністративно-правового забезпечення захисту персональних даних в ЄС та Україні, суб'єктів персональних даних, суб'єктів адміністративно-правового забезпечення захисту персональних даних та механізмів адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації в європейських країнах (підрозділ 1.1, 1.3, 2.2, 2.4).

Також, статистичний метод застосований для дослідження обсягу обробки та зберігання персональних даних суб'єктами публічної адміністрації та з метою визначення актуальності проблематики щодо забезпечення захисту персональних даних та обґрунтування пропозицій необхідності вдосконалення законодавства щодо забезпечення захисту персональний даних.

Нормативно-правовою основою роботи стали положення Конституції України, Закон України «Про захист персональних даних» та інші нормативно-правові акти України, а також нормативно-правові акти Президента України, Кабінету Міністрів України, центральних органів виконавчої влади України, законодавство зарубіжних країн у досліджуваній сфері.

Емпіричну базу дослідження склали теоретичні напрацювання вітчизняних науковців у сфері забезпечення захисту персональних даних, узагальнення практичної діяльності суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян, статистичні дані офіційних електронних

веб-сайтів, суб'єктів публічного адміністрування в Україні та зарубіжних країн, а також довідкові видання у досліджуваній сфері.

**Наукова новизна.** Дисертаційна робота є одним із перших у вітчизняній адміністративно-правовій науці науковим дослідженням теоретичних і практичних проблем адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації.

Основними положеннями, що обумовлюють наукову новизну та виносяться на захист, є такі:

*вперше:*

– запропоновано визначення поняття «адміністративно-правове забезпечення захисту персональних даних громадян – це врегульована адміністративними нормами системна діяльність суб'єктів публічної адміністрації щодо адміністративно-правового регулювання, реалізації, охорони та захисту суспільних відносин у сфері персональних даних»;

– запропоновано визначення категорії «суб'єкт адміністративно-правового забезпечення захисту персональних даних громадян як орган публічної адміністрації, який здійснює публічне управління у сфері захисту персональних даних в процесі реалізації прав громадян та надання адміністративних послуг компетенція якого включає правове регулювання, збір, обробку, зберігання та забезпечення захисту персональних даних»;

– запропоновано класифікацію суб'єктів адміністративно-правового забезпечення за наступними критеріями: 1) за сферами діяльності: цивільні та мілітаризовані; 2) за сферами повноважень: публічні та приватні; 3) за видами персональних даних: суб'єкти забезпечення захисту загальних персональних даних та суб'єкти забезпечення захисту особливо чутливих та конфіденційних персональних даних;

– критерії для класифікації суб'єктів персональних даних, а саме: за рівнем законодавчого регулювання – такі, що підпадають під дію загального законодавства в сфері персональних даних та спеціального законодавства; за сферою суспільних відносин: медична сфера (фізичні особи: пацієнти,

медичний персонал), фінансова сфера (фізичні особи: клієнти банків та інших фінансових установ), освітня сфера (фізичні особи: кандидати на вступ, здобувачі освіти, науково-педагогічні кадри, адміністративні працівники освітніх установ), сфера надання публічних послуг (фізичні особи: громадяни, що звертаються за отриманням публічних послуг, державні службовці), сфера реалізації виборчих прав (фізичні особи-виборці) та інші; поділ суб'єктів персональних даних, виходячи з загальної класифікації фізичних осіб, тобто поділ на громадян, не громадяни (іноземці, особи без громадянства та інші).

*удосконалено:*

– визначення поняття «персональні дані громадян – це будь-які відомості або дані, в об'єктивізованій формі, що стосуються суб'єкта даних (фізичної особи), який підлягає ідентифікації»;

– визначення поняття «фізична особа, що піддається ідентифікації — це реальна фізична особа, яку можна визначити у прямий чи опосередкований спосіб, зокрема, за допомогою певних відомостей ідентифікуючого характеру, таких як ім'я, прізвище, по-батькові, ідентифікаційний номер, дані про народження, місцезнаходження, онлайновий ідентифікатор, або на один або кілька факторів (їх поєднання), які є специфічними та винятково властивими для соціальної, генетичної, фізичної, фізіологічної, інтелектуальної, майнової, культурної ідентичності цієї особи»;

– визначення поняття «інструменти адміністративно-правового забезпечення захисту персональних даних громадян – це врегульовані нормами адміністративного права зовнішні прояви конкретних дій уповноважених суб'єктів публічної адміністрації, в рамках яких реалізуються і за допомогою яких здійснюються регулюючий вплив на суспільні відносини у сфері обігу персональних даних для забезпечення прав та законних інтересів суб'єктів цих правовідносин» та їх класифікації.

*дістали подальшого розвитку:*

– періодизація нормативно-правового забезпечення захисту персональних даних в Європі та Україні шляхом виділення основних чотирьох етапів становлення з кінця XIX століття до сьогодення;

– підходи до класифікації видів персональних даних, використовуючи критерії їх змісту та рівня визначеної можливості доступу до них: загальні дані про особу, спеціальні дані про особу, а також біометричні дані про особу. При цьому видами біометричних персональних даних громадян виступають генетичні дані про них та відомості, що стосуються їх здоров'я або отриманої медичної допомоги.

– підходи щодо структури адміністративно-правового забезпечення захисту персональних даних громадян: 1) об’єкт адміністративно-правового забезпечення персональних даних; 2) суб’єкт адміністративно-правового забезпечення персональних даних; 3) норми адміністративного права щодо забезпечення захисту персональних даних; 4) адміністративно-правові відносини в сфері забезпечення захисту персональних даних та їх зміст; 5) гарантії адміністративно-правового забезпечення захисту персональних даних включають.

– пропозиції щодо удосконалення чинного законодавства відповідно до стандартів ЄС, щодо створення єдиного окремого органу державної влади, який буде визначати стандарти обробки та безпеки персональних даних, здійснювати контроль за суб’єктами публічної влади щодо забезпечення захисту персональних даних, удосконалення термінології та визначення понять «захисту персональних даних», «порушення захисту персональних даних» та законодавчого визначення повноважень органів державної влади та органів місцевого самоврядування щодо забезпечення захисту персональних даних.

**Практичне значення** одержаних наукових результатів полягає у тому, що сформульовані в дисертації положення та висновки впроваджено та можуть бути використані:

- у нормотворчій діяльності – для розробки пропозицій щодо внесення

змін до законодавчих актів з питань адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації (довідка керівника секретаріату Комітету ВРУ з питань фінансів, податкової та митної політики від 17 квітня 2024 року);

- правозастосовчій діяльності – для підвищення ефективності діяльності суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації;

- у освітній діяльності – в навчальному процесі під час підготовки фахівців у галузі знань 08 Право, зокрема в ході викладання навчальних дисциплін «Адміністративне право України», (акт впровадження результатів дисертаційної роботи Військового інституту Київського національного університету імені Т. Шевченка від 15 квітня 2024, акт впровадження результатів дисертаційного дослідження Київського інституту Національної гвардії України від 22 квітня 2024 року, акт впровадження результатів дисертаційного дослідження Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка від 01 травня 2024 ).

**Особистий внесок здобувача.** Дисертацію виконано здобувачем самостійно. Отримані теоретичні положення та сформульовані на їх основі пропозиції і рекомендації одержані автором особисто. Статті «Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права» (Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 1 (53), 2023. Київ, С 41-45) та «Адміністративно-правове забезпечення захисту персональних даних громадян : поняття та структура» (Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія» ) Випуск № 10(40) 2023. С. 678-688) виконані авторкою самостійно.

У наукових статтях «Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни» (Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 4 (52), 2022. Київ, С. 50-53) та Administrative-legal support for the protection of citizens personal data:

contemporary theoretical approaches. (Visegrad journal on human rights № 4 (2023) P. 55-61) опублікованих спільно з В.Й. Пашинським, авторці належить 60 % дослідження.

**Апробація результатів дисертації.** Основні положення дисертації обговорювалися на кафедрі адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка.

Результати дослідження були оприлюднені на 8 науково-практичних конференціях та круглих столах, зокрема: «V Міжнародному правничому форуму «Права людини та публічне врядування в сучасних умовах» від 10 червня 2022 року, м. Чернівці; «Міжнародній науково-практичній конференції «Права людини як індикатор розвитку сучасної держави» від 13 грудня 2021 року м. Київ; «Всеукраїнській науково-практичній конференції з нагоди 20-ї річниці заснування Полтавського юридичного інституту «Адаптація правової системи України до Європейського союзу: теоретичні та практичні аспекти» від 29 вересня 2022 року, м. Полтава; «Міжнародній науково-практичній конференції «Актуальні питання розвитку юридичної науки і практики в умовах воєнного стану та мирної розбудови» від 05 травня 2023 року, м. Київ; «VI Міжнародному правовому форуму «Права людини та публічне врядування в сучасних умовах» від 10 червня 2022 року, м. Чернівці; VI Всеукраїнській науково-практичній конференції Актуальні питання державотворення та захисту прав людини в Україні» Хмельницький інститут імені Блаженнішого Володимира, Митрополита Київського і всієї України ПрАТ «ВНЗ «МАУП» від 29 січня 2024 року, м. Хмельницький, Міжнародній науково-практичній конференції «Публічна влада: проблеми реалізації повноважень в умовах воєнного стану та відбудовного періоду» від 22 лютого 2024 року, м. Київ .

**Публікації.** Основні положення, висновки та пропозиції, сформульовані за результатами дисертаційної роботи, відображено у 3 наукових статтях у наукових виданнях України, визнаних фаховими з юридичних наук, а також у 8 тезах наукових доповідей.

**Структура та обсяг дисертації.** Робота складається із вступу, двох розділів, що містять сім підрозділів, висновків, списку використаних джерел. Загальний обсяг дисертації становить 213 сторінок, з них основний текст –159 сторінок, список використаних джерел – 28 сторінок  та додатки на 12 сторінках.

# РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН

## 1.1 Генеза нормативно-правового забезпечення захисту персональних даних громадян

Розбудова України як європейської, демократичної, правової держави, у якій найвищою цінністю є людина та її права, честь і гідність, недоторканність і безпека, потребує подальшого удосконалення правових механізмів забезпечення захисту основноположних прав і свобод людини. Сучасні темпи розвитку інформаційних технологій та пов'язане з цим активне формування відповідних баз персональних даних в системі суб'єктів публічного адміністрування загострили проблему захисту різних видів інформаційних прав і свобод людини, в тому числі захисту персональних даних громадян.

У сучасному інформаційному суспільстві, яке швидко розвивається, персональні дані громадян набули особливо важливого значення, як самодостатня соціальна цінність, правова категорія та об'єкт адміністративно-правового забезпечення їх захисту, які у глобальному світі потребують єдиних міжнародних стандартів щодо їх регулювання та захисту.

Зрозуміло, що у кожної держави формувалися свої індивідуальні підходи до нормативно-правового регулювання відносин щодо персональних даних. Проте, останні десятиліття спостерігається тенденція до їх глибокої уніфікації на міжнародному рівні. Не є винятком у цьому процесі і Україна, як суб'єкт міжнародного права, що інтегрується в європейський правовий простір та запроваджує стандарти ЄС щодо захисту персональних даних в національне законодавство.

Аналізуючи різноманітні аспекти нормативно-правового регулювання суспільних відносин пов'язаних із адміністративно-правовим забезпеченням захисту персональних даних та етапи формування правової думки в Україні,

нами розглядатиметься цей процес у нерозривній єдності з історичними етапами становлення інституту персональних даних у Європі та світі.

Необхідно зазначити, що інститут персональних даних, за своєю правовою природою, є новим інститутом суспільних відносин. Його становлення та сучасний швидкий розвиток тісно пов'язані з еволюцією прав особи, зокрема, права на приватність та недоторканість особистого життя, а також запровадженням інформаційних технологій в усіх сферах суспільної діяльності.

Правовий інститут персональних даних відзначається наявністю системи власних елементів, які визначають предмет правового регулювання різних галузей права (конституційного, цивільного тощо), але, у першу чергу, – адміністративного права, яке є інструментом діяльності публічної влади, щодо забезпечення прав і свобод людини.

Із зазначених вище причин, сфера захисту персональних даних займає важливе місце в діяльності суб'єктів публічної адміністрації, охоплює відносини між приватними особами та суб'єктами публічної влади, які мають як публічно-правовий так і приватно-правовий характер.

При цьому, на нашу думку, приватно-правовий вплив на захист персональних даних носить субсидіарний (додатковий) характер. Це зумовлено тим, що правовий інститут захисту персональних даних формувався як елемент правового статусу та адміністративно-правового захисту прав людини, зокрема, права на приватність та особисту недоторканість, як невідємної складової концепції «прайвесі» [1]), пов'язаних із захистом особистих прав громадян. Дана концепція була відображена в американській юриспруденції та включала охорону свобод та приватного життя від надмірного та неправомірного втручання держави.

Зміст концепції «прайвесі» був сформульований в кінці XIX століття, як «право дати людині спокій». Англійською мовою усі аспекти особистого життя позначаються єдиним терміном «privacy», який буквально перекладається, як «приватність», проте вживання даного терміну в рамках концепції передбачає

його більш широке тлумачення. Нині цей термін увійшов у правову термінологію і охоплює всі аспекти приватного життя людини, такі як: інтимний світ, сферу особистих стосунків, недоторканність приватного листування, щоденників, свободу думки, релігійних переконань та інші, забезпечення яких безпосередньо пов'язано із захистом персональних даних [2].

Протягом першої половини XX ст. дана концепція «privacy» (або «право на приватність») швидко поширюється і за межами США, в інших демократичних країнах знаходить своє відображення в наукових дослідженнях, в нормах права та американській судовій практиці [2].

Паралельно передумови визнання права на недоторканість особистого життя формуються на теренах України. Відтак, у контексті історичних витоків сучасного національного праворозуміння забезпечення особистісної сфери людини, у тому числі її приватності, від будь-яких форм зовнішнього втручання можна знайти у працях відомого діяча громадівського руху Михайла Драгоманова. Зокрема, у розробленому ним Проекті основ статуту українського товариства «Вільна Спілка» визначається завдання «перетворення цієї держави на засадах політичної свободи» [3].

Під словами політичні свободи М. Драгоманов пропонує також розуміти наявність особистих свобод: недоторканість тіла для принизливих покарань та смертної кари; недоторканість особи, її житла, приватного листування тощо [4]. Але ці ідеї не знайшли реалізації в нормах права, зокрема щодо забезпечення особистих прав людини, недоторканості приватного життя, через історичні обставини, в яких знаходилась наша держава протягом XX століття та носили виключно теоретичний характер.

В подальшому, сформульована у США концепція «privacy» суттєво вплинула на становлення сучасних міжнародних стандартів та системи прав і свобод людини, яка базується на принципі «людиноцентризму», і знайшла своє закріплення у нормах міжнародного права після Другої світової війни. Особлива увага до прав людини пояснюється, в першу чергу, систематичним

порушенням під час війни таких ключових природних прав людини як право на життя, а також право на приватність. На той час, одним із найбільш значимих соціальних питань повоєнного устрою стало забезпечення прав людини, зокрема, особистих прав: недоторканість особистого життя, недоторканість сімейного життя, таємниця кореспонденції. Водночас, питанню забезпечення захисту персональних даних не приділялося достатньої уваги.

У 1948 році право на особисте життя разом із іншими фундаментальними правами і свободами людини закріплюється у Загальній декларації прав людини, зокрема, у ст. 12 встановлювалось, що ніхто не може бути об'єктом свавільного втручання в його особисте та сімейне життя, свавільного посягання на недоторканість [5]. В 1950 році у Конвенції про захист прав людини і основоположних свобод (ст. 8) передбачалося право на повагу до приватного і сімейного життя, а також неможливість втручання органами державної влади у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни; для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі, або для захисту прав і свобод інших осіб [6]. Вищезазначені норми міжнародного права стали основою для забезпечення захисту особистих прав, в тому числі основою для майбутнього розвитку забезпечення захисту персональних даних на національному рівні.

В подальшому право на захист персональних даних знаходить своє закріплення в національному законодавстві різних країн. В США в середнині XX ст. прийнято Privacy Act, у котрому американський Конгрес вперше встановлює зв'язок між правом на приватне життя і персональні дані [7]. Так, § 552a зазначеного акту встановлює кодекс чесної інформаційної практики та регулює питання збору та поширення інформації про особу, яка зберігається органами федеральної влади. Даний законодавчий акт встановлював, що особисте життя людини може зазнавати впливу внаслідок збору, використання та поширення персональної інформації органами державної влади [7].

Разом із тим, право на захист персональних даних набуває своєї актуальності та починає виходити із тіні права на особисте життя і становлення як окремого правового інституту. Прискоренню цих процесів сприяв швидкий розвиток на початку другої половини XX ст. інформаційних технологій, котрі дозволяли значно швидше опрацьовувати більшу кількість інформації та можливості її зберігання у базах даних органів публічної влади. У 60-ті роки XX ст. ці технології стають усе більш доступними, що викликало певне занепокоєння у контексті зберігання, обігу, контролю інформації щодо особи та необхідності захисту її персональних даних.

Так, у 1968 році Парламентська Асамблея Ради Європи приймає рекомендацію №509 Права людини та сучасні наукові і технологічні досягнення, у якій висловлюється стурбованість щодо можливих загроз праву на особисте життя, котрі виникають внаслідок використання нових інформаційних технологій обробки персональних даних. Асамблея доручила Комітету з прав людини дослідити дане питання та надати пропозиції щодо забезпечення захисту персональних даних. Зокрема, йшлося про те, що нові методи, такі як технічні можливості прослуховування телефонів, підслуховування, таємне спостереження, незаконне використання офіційних статистичних та подібних опитувань для отримання приватної інформації, а також підсвідома реклама та пропаганда є загрозою правам і свободам осіб і, зокрема, на права на приватність, яке захищається статтею 8 Конвенції про захист прав людини і основоположних свобод. Зазначений документ сприяв початку досліджень проблематики нормативно-правового регулювання у сфері «data privacy» (захисту персональних даних) в окремих країнах Європи, які згодом і стануть основою для міжнародних стандартів захисту персональних даних, таких як Загальний регламент про захист даних або General Data Protection Regulation (далі - GDPR) в ЄС, який в подальшому створить правову основу для забезпечення захисту персональних даних.

Протягом наступних тридцяти років більшість країн Європи активно продовжували здійснювати правове регулювання та впроваджували

нормативні акти, що стосуються збору, обробки та захисту персональних даних, і закріплювали в них механізми правового регулювання обігу таких даних. Важливим аспектом слід відзначити те, що створення таких законів відбувалося паралельно із розвитком законодавства, спрямованого на захист права на недоторканість особистого життя.

На початкових етапах європейські країни приймали окремі національні закони, які регулювали питання захисту персональних даних. Це дозволило створити базу для подальшого розвитку та уніфікації нормативно-правової бази на рівні Європейського Союзу.

Значущим кроком у сфері розвитку захисту персональних даних стає прийняття перших законів щодо забезпечення захисту персональних даних, першим з яких був прийнятий німецькою землею Гессен у 1970 році. А вже через сім років був ухвалений перший федеральний закон, який регулював питання захисту персональних даних німецьких громадян (Bundesdatenschutzgesetz) [8]. Такий підхід обумовлюється історичними подіями в країні, зокрема, авторитарними режимами: фашистський, комуністичний, які ґрунтувались, серед іншого, на систематичному порушені прав і свобод людини, стеженні за населенням, викликавши велику суспільну потребу у збереженні конфіденційності та захисті персональних даних громадян. Таким чином, прийняття даного закону про захист персональних даних у Німеччині стало важливим кроком в контексті забезпечення захиступерсональних даних, що дозволило безпосередньо забезпечити захист громадян на конфіденційність їхніх персональних даних.

Також, важливе значення для розвитку стандартів у сфері захисту персональних даних стало прийняття у Франції 1978 році Закону про інформатику та громадянські свободи, що було пов'язане з автоматизованою обробкою даних, яка здійснювалась завдяки передовим на той час обчислювальним технологіям [9]. Зазначений закон передбачав створення єдиного реєстру даних за допомогою номерів соціального страхування для ідентифікації громадян, що дозволяло б ідентифікувати будь-якого

громадянина. Стаття, опублікована в газеті Le Monde у 1974 році під назвою «SAFARI ou la chasse aux Français» [10] (САФАРІ або полювання на французів), викликала гучний скандал і призвела до відставки уряду, що в результаті призвело до прийняття зазначеного закону і створення Комісії з інформатики та громадянських свобод. Комісія з інформатики та громадянських свобод в подальшому встановила обмеження щодо обробки персональних даних, визначивши тим самим важливі рамки для забезпечення захисту персональних даних [9].

Таким чином, німецький і французький закони вперше впроваджують регулювання обігу, обробки, механізмів захисту персональних даних та створення спеціальних інституцій, а також дають відчутний імпульс для розвитку та подальшої уніфікації нормативно-правового регулювання захисту персональних даних. На проблему починають звертати увагу усе більше й більше країн, а також міжнародних організацій. Саме у цей час стає відчутною різниця на рівні нормативно-правового забезпечення захисту персональних даних країн західного світу та України (УРСР), яка на той час входила до складу Радянського Союзу.

У цей період радянська конституція 1977 року лише на декларативному рівні гарантувала громадянам недоторканість особистості та житла, а також охорону законом особистого життя, таємниці листування, телефонних розмов і телеграфних повідомлень (ст. 55, 56, 57) [11]. В той же час, прийнята на її основі радянська конституція України (УРСР) 1978 року стала першою і єдиною конституцією на радянському просторі, котра містила окремі стандарти розвинутих європейських країн, зокрема розділ щодо комплексу громадянських, політичних, економічних, соціальних і культурних прав. Громадянам гарантувалась недоторканність особи, недоторканність житла, особисте життя громадян, таємниця листування, телефонних розмов і телеграфних повідомлень [12]. Зрозуміло, що жодним чином про захист персональних даних у цих соціалістичних конституціях не йшлося, хоча самі по собі вони стають значним кроком у контексті демократизації життя

українських громадян радянських часів, незважаючи на декларативний характер положень зазначених конституцій.

У той же час, на теренах нинішнього ЄС продовжується активний розвиток нормативно-правового забезпечення захисту персональних даних у зв’язку зі стрімким розвитком комп’ютерних технологій, та їх використання, в тому числі, в комерційній діяльності. В цьому аспекті важливе значення для нормативно-правового забезпечення захисту персональних даних стає Конвенція Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28.01.1981 р. Зазначена конвенція мала важливе значення для уніфікації і розвитку законодавства європейських країн щодо захисту персональних даних [13]. Зазначена конвенція закріпила гарантії та основні принципи обробки персональних даних, такі як законність, справедливість, пропорційність, точність та конфіденційність. Одним з ключових досягнень Конвенції також стало запровадження поняття «чутливих даних» і встановлення особливих умов для їх обробки.

Конвенція стала основою для прийняття Директиви 95/46/ЄС Європейського Парламенту та Ради Європейського Союзу «Про захист фізичних осіб при обробці персональних даних та вільне переміщення таких даних», яка отримала схвалення 24 жовтня 1995 року. Дана Конвенція започаткувала формування сучасного етапу правового забезпечення захисту персональних даних у ЄС, а також стала першим загальнообов'язковим правовим актом, що заклав основи захисту персональних даних фізичних осіб у ЄС [14]. Також дана Конвенція врегулювала питання захисту фізичних осіб при обробці персональних даних, вільне переміщення таких даних, гарантувала вільний обіг персональних даних відповідно до гармонізованих правил, призначених захистити ключові права і, насамперед, право на повагу до приватного життя.

Наступними кроками стає прийняття нормативних актів у специфічних сферах, які не підпадали під дію Директиви 95/46/ЄС, зокрема, що встановлюють правила обробки персональних даних та захисту

конфіденційності у секторі електронних засобів зв'язку (далі – Директива 2002/58/ЄС) [15], а також створення Європейського агентства з мережевої та інформаційної безпеки (Регламент (ЄС) №406/2004) [16].

Наступним важливим кроком розвитку даного типу суспільних відносин стає закріплення права на захист персональних даних як фундаментального та невід'ємного права людини на рівні первинного права ЄС, а саме: в установчих Договорах ЄС, зокрема у статті 16 Договору про функціонування ЄС [17], у статті 39 Договору про ЄС [18] та у статті 8 Хартії Основних прав ЄС. Мова йде про ч. 3 ст. 8, що «Дотримання цих правил підлягає контролю з боку незалежного органу» [19].

Сучасний етап нормативно-правового забезпечення захисту прав персональних даних пов'язаний із набуттям чинності в 2018 р. на території ЄС Загального Регламенту із захисту даних (далі – Регламент ЄС 2016/679) [20], що замінює та скасовує Директиву 95/46/ЄС, та Директиви (ЄС) 2016/680, яка встановлює правила про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування за кримінальні злочини або виконання кримінальних покарань. На даний час усі країни-члени ЄС імплементували в національне законодавство положення Загального Регламенту із захисту даних (Регламент (ЄС) 2016/679).

Однак, даний Регламент не став кінцевим пунктом законотворчої діяльності ЄС у сфері захисту персональних даних. Обробка персональних даних відповідно до цілей кримінального правосуддя не належить до питань, що урегульовується Регламентом, оскільки потребує встановлення окремого правового режиму. Тому в 2016 році одночасно із GDPR було прийнято Директиву (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.2016 р. “Про використання даних записів реєстрації пасажирів ( далі – Директива PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину” (Директива PNR) [21].

У Європейському Союзі на сучасному етапі продовжується діяльність спрямована на створення ефективного механізму нормативно-правового забезпечення відносин у сфері захисту персональних даних. При цьому є наявною тенденція щодо поширення публічно-правових підходів до нормативно-правового регулювання захисту персональних даних.

В свою чергу, Україна з самого початку прийняла до уваги орієнтири сформовані у нормативних актах ЄС щодо захисту персональних даних для розвитку національного законодавства. Оскільки, обробка персональних даних суб'єктами публічної влади може також бути використана з метою порушення прав людини, включно з правом фізичних осіб на приватність та захист персональних даних. За таких умов, необхідність захисту особистих даних стає обов'язоком суб'єктів публічної влади та невід'ємною складовою всієї системи захисту прав людини. Більше того, забезпечення захисту особистих даних громадян є частиною міжнародних зобов'язань держави, пов'язаних з її європейською інтеграцією, від виконання якого залежить євроінтеграційний курс України [22].

Зазначені вище обставини зумовили прийняття Закону України «Про захист персональних даних» від 01.06.2010 р., де було закріплено поняття «персональних даних» як «відомостей чи сукупності відомостей про фізичну особу» (ст. 2) та поняття «суб'єкт персональних даних» (ч. 1 ст. 2) де розуміється фізична особа, персональні дані якої обробляються, а також передбачено правовий механізм захисту персональних даних [23].

Також, Закон України «Про захист персональних даних» закріплює окремі види персональних даних. Насамперед, слід розрізняти загальні та особливі (так звані чутливі чи вразливі) персональні дані. До останніх належать дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних (ч. 1 ст. 7) [23].

Таким чином, Україна зробила перший надзвичайно важливий крок у процесі нормативно-правового забезпечення обігу та захисту персональних даних у відповідності до європейських стандартів визначених директивами та Регламентом ЄС. Це стало можливим завдяки активному впровадженню у національне законодавство європейських принципів та стандартів щодо забезпечення захисту персональних даних.

Враховуючи тенденції щодо розвитку нормативно-правового забезпечення захисту персональних даних у ЄС, в Україні також були прийняті законодавчі акти, які врегулювали питання захисту персональних даних у різних сферах суспільного життя. У цьому контексті важливим було прийняття Закону України «Про інформацію», який в свою чергу уточнює поняття «персональні дані» як інформація про фізичну особу (ст. 11) [24].

Важливе значення набуває також Закон України «Про державні фінансові гарантії медичного обслуговування населення» в контексті захисту прав персональних даних у сфері охорони здоров'я у зв'язку із запровадженням електронної системи охорони здоров'я – інформаційно-телекомунікаційної системи, що забезпечує автоматизацію ведення обліку медичних послуг (ст. 11) [25]. Закон передбачав, що функціонування електронної системи охорони здоров'я обов'язково повинно здійснюватись з урахуванням вимог законодавства про захист персональних даних [26].

Більше того, персональні дані пацієнта, а саме: відомості про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також відомості, одержані при його медичному обстеженні, охоплюються правом на таємницю про стан здоров'я (ст. 391); відомості про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина підпадають під правовий режим лікарської таємниці.

Слід зазначити, що дія Закону України «Про захист персональних даних» поширюється на всіх суб'єктів правовідносин у медичній сфері не залежно від їх організаційно-правової форми та форми власності. Тобто, не тільки державні заклади охорони здоров'я, але і приватні, а також ті, хто займається приватною

медичною практикою, зобов'язані реєструвати бази персональних даних пацієнтів та забезпечувати їх захист.

В подальшому, нормативно-правове забезпечення захисту персональних даних здійснювалось шляхом внесення змін та доповнень до окремих законів, які запроваджували систему надання адміністративних послуг та здійснення електронної реєстраційної діяльності, яка пов'язана з персональними даними. До числа таких відносяться, зокрема, Закон України «Про адміністративні послуги» [27] та, особливо Закон України «Про особливості надання публічних (електронних публічних) послуг» [28], який визначає механізм захисту персональних даних під час надання електронних публічних послуг та публічних послуг, а також комплексних електронних публічних послуг та автоматичного режиму надання електронних публічних послуг.

Особливо важливим також є Закон України «Про публічні електронні реєстри», який встановлює правові, організаційні і фінансові засади створення та функціонування публічних електронних реєстрів з метою захисту прав та інтересів фізичних та юридичних осіб під час створення, зберігання, оброблення та використання інформації у публічних електронних реєстрах [29]. Закон України «Про публічні електронні реєстри» поширюється на відносини, що виникають у сфері публічних електронних реєстрів під час створення та ведення таких реєстрів, адміністрування, взаємодії, перетворення, модифікації та припинення публічних електронних реєстрів; при використанні реєстрової інформації національних електронних інформаційних ресурсів під час провадження дозвільної діяльності, надання адміністративних, соціальних та інших публічних послуг; провадження іншої управлінської діяльності та державного регулювання, а також поширюється на відносини, що виникають під час створення, ведення, взаємодії, адміністрування Єдиного реєстру адвокатів [29].

Також важливим в контексті захисту персональних даних є здійснення послуг державної реєстрації, пов'язаних з використанням персональних даних. Саме тому виникає необхідність згадати низку інших нормативних актів. Так,

у ст. 4 Закону України «Про державну реєстрацію юридичних осіб та фізичних осіб-підприємців та громадських формувань» державна реєстрація юридичних осіб та фізичних осіб-підприємців та громадських формувань – це засвідчення факту створення або припинення юридичної особи, засвідчення факту набуття або позбавлення статусу підприємця фізичною особою, а також вчинення інших реєстраційних дій, які передбачені цим Законом, шляхом внесення відповідних записів до Єдиного державного реєстру [30].

У Законі України «Про державну реєстрацію актів цивільного стану» поняття такої реєстрації відсутнє, лише вказано, що державна реєстрація актів цивільного стану проводиться з метою забезпечення реалізації прав фізичної особи та офіційного визнання і підтвердження державою фактів народження фізичної особи та її походження, шлюбу, розірвання шлюбу, зміни імені, смерті (ст. 9) [31].

Крім зазначених нормативно-правових актів, що безумовно відносяться до сфери правового забезпечення захисту персональних даних, привертають увагу і окремі положення трудового законодавства. Специфіка захисту персональних даних в трудових правовідносинах обумовлена насамперед ціллю їх обробки і регулюється Кодексом законів про працю України. Варто зазначити, що роботодавець має законні підстави для обробки персональних даних працівника за його згодою, але лише в межах, які необхідні при прийнятті його на роботу та подальшим виконанням ним трудової функції (ч. 2 ст. 24) [32].

Також варто зазначити, що у сфері приватно-правового регулювання до числа нормативно-правових актів, що регулюють захист персональних даних необхідно віднести і ЦК України. Окремі норми ЦК України також передбачають право на особисте життя та його таємницю. З зазначеними нормами безпосередньо пов’язані інші суб’єктивні немайнові права, які в свою чергу на практиці виступають правовими гарантіями забезпечення захисту таємниці особистого життя. До числа таких можна віднести право: на

інформацію (ст. 302), на особисті папери (ст. 303), на таємницю кореспонденції (ст. 306), на недоторканність житла (ст. 311) [33].

Наразі, у національній правовій системі сформувалася правова база нормативно-правового забезпечення суспільних відносин, пов'язаних з захистом персональних даних. В національному законодавстві щодо захисту персональних даних ключову роль відіграють нормативно-правові акти, в переважній більшості – акти адміністративного законодавства.

Зазначені акти визначають механізми захисту персональних даних, систему суб'єктів та їх повноваження. Особливого вагомого значення у цьому контексті набуває запровадження застосунку «Дія», функціонал якого безпосередньо пов'язаний із збиранням, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і передачею персональних даних користувачів зазначеного застосунку при наданні адміністративних послуг в різних сферах суспільного життя, наприклад при отриманні громадянами електронних послуг.

Завершуючи характеристику сучасного етапу нормативно-правового забезпечення захисту прав персональних даних, наголосимо, що російська військова агресія особливо загострила весь спектр проблематики пов'язаної з сферою захисту персональних даних громадян, несанкціонований доступ до яких може загрожувати національній безпеці та безпосередню життю і здоров'ю громадян.

Проблеми захисту персональних даних, поставлені перед суспільством з початком російської збройної агресії, вимагали і вимагають негайного вирішення проблем щодо захисту персональних даних громадян, особливо вразливих категорій, у тому числі на нормативно-правовому та організаційно-управлінському рівнях.

Початком діяльності публічної влади у цьому напрямку став Указ Президента України від 24 лютого 2022 року №64/2022 «Про введення воєнного стану в Україні», який передбачає, що на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і

громадянина щодо: недоторканості житла (ст.30); таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31); втручання в його особисте і сімейне життя (ст.32); свободи пересування, вільного вибору місця проживання, права вільно залишати територію України (ст.33); права на свободу думки і слова, вільного вираження своїх поглядів і переконань ( ст. 34) та інші передбачені Конституцією України, реалізація яких пов'язана із захистом персональних даних громадян [34].

Тимчасові обмеження зазначених прав і законних інтересів юридичних осіб в межах визначених Конституцією та Законами України, необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, основним завданням якого є оборона держави та, як кінцевий результат, охорона і захист конституційних прав людини і громадянина (ст. 8) [34]. Зазначені обмеження конституційних прав здійснюються лише в інтересах національної безпеки і тільки на період дії правового режиму воєнного стану.

Водночас, необхідно зазначити, що в умовах широкомасштабної військової агресії, виникає нагальна потреба одночасно вести мову не лише про встановлення законних обмежень окремих прав і свобод людини і громадянина, але й про впровадження нових правових механізмів їх захисту через діяльність органів публічної влади та окремих інститутів громадянського суспільства. Особливе уваги потребує стан дотримання прав у сфері захисту персональних даних військових, державних службовців, примусово переміщених громадян та інших категорій осіб.

Першими важливим кроком у формуванні нових правових механізмів захисту персональних даних громадян органами публічного адміністрування стала постанова КМУ від 12 березня 2022 р. № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану». Згідно даної постанови на період дії воєнного стану поширюється на міністерства, інші центральні та місцеві органи виконавчої

влади, державні та комунальні підприємства, установи, організації, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами, яких вони є та захисту інформації, яка обробляється в таких реєстрах.

Прикладами таких заходів щодо захисту державних інформаційних ресурсів, можуть бути, зокрема: розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах та/або в центрах обробки даних, які розташовані за межами України; реєстрація доменних імен за доменом gov.ua для здійснення такого розміщення та зупинення, або обмеження роботи таких інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, в тому числі публічних електронних реєстрів [35]. Прийняття зазначеної постанови допомогло на початкових етапах дії правового режиму дії воєнного стану сприяти та забезпечити захист персональних даних громадян та започаткувало подальший розвиток нормативно-правового забезпечення у сфері захисту персональних даних громадян, що особливо важливо для вразливих груп громадян. В першу чергу, мова йде про представників силових (мілітаризованих) структур Збройні Сили України, Національна гвардія України, Служба безпеки України, Національна поліція, Державна прикордонна служба України та ін.

На нашу думку, наразі назріла необхідність розробити окремі інформаційні реєстри щодо зазначених нами вище вразливих категорій громадян з різним ступенем доступу до інформації про них та унормуванням можливості отримання інформації щодо таких суб'єктів, дані яких наявні в цих базах даних або навпаки отримати інформацію про відсутність даних про таких осіб в базах.

Таким чином, перші правові норми щодо захисту персональних даних з'явилися у результаті об'єктивного розвитку суспільних відносин і розглядалися у контексті права на приватність та недоторканість особистого

життя. Проте, в контексті переходу до інформаційного суспільства, який характеризується широким використанням інформаційних технологій, інтенсивним збором та обробкою інформації, включаючи особисту інформацію, виникла нагальна потреба у правовому регулюванні обробки таких персональних даних. Відтак, поширення інформаційних технологій суттєво прискорило потребу нормативно-правового регулювання захисту персональних даних великого кола суб'єктів незалежно від їх державної приналежності на міжнародному та національному рівнях.

Варто зазначити, що в цьому аспекті передовими країнами стали країни Західної Європи, оскільки саме ними були прийняті спеціальні закони про захист персональних даних. Доцільно акцентувати увагу на тому, що законодавство в сфері захисту персональних даних в європейських країнах і наразі продовжує свій розвиток. Це обумовлюється наявністю нових проблем, що потребують правового регулювання, як, наприклад, транскордонна передача персональних даних, використання біометричних персональних даних та даних медико-генетичного характеру тощо.

Нинішній етап нормативно-правового забезпечення захисту персональних даних пов'язаний з необхідністю врегулювання суспільних відносин щодо використання технологій штучного інтелекту, які безпосередньо впливають на захист прав людини, захист її персональних даних. Окремої уваги в цьому аспекті заслуговує закон, прийнятий Європейським парламентом про штучний інтелект. Цей закон відображає зростаючу увагу до правових аспектів використання штучного інтелекту в сучасному суспільстві. Прийняття такого закону свідчить про необхідність регулювання і контролю за застосуванням штучного інтелекту для запобігання можливих порушень прав людини та захисту її приватності, відображає новий етап у формуванні правової бази, спрямованої на адаптацію законодавства до викликів, які виникають у зв'язку з швидким розвитком штучного інтелекту та необхідністю забезпечення належного захисту особистих даних громадян. Зазначений закон, спрямований на обмеження штучного інтелекту та включає в себе широкий спектр правових

норм та положень, які регулюють використання штучного інтелекту в різних сферах життя. Ці норми стосуються збору, збереження, обробки та передачі персональних даних, визначення відповідальності за автоматизовані рішення, забезпечення прозорості та відповідності алгоритмів штучного інтелекту правовим європейським стандартам, а також захисту прав споживачів та гарантії їхньої безпеки під час використання штучного інтелекту. Такий комплексний підхід дозволяє забезпечити ефективний захист прав і свобод осіб у контексті широкого застосування штучного інтелекту в сучасному інформаційному суспільстві [35].

Наразі можемо виділити чотири етапи розвитку та становлення нормативно-правового забезпечення захисту персональних даних в Європі та Україні. Перший з них пов'язаний з розповсюдженням та інтерпретацією правової концепції «privacy» (або «право на приватність») починаючи з кінця XIX століття і до тридцятих років XX століття та закріплення даної концепції в нормативних актах окремих європейських країн. Натомість в цей період на теренах України відбувається виключно теоретичне формування забезпечення особистих прав людини та її приватності, але такі теоретичні підходи на той час не були безпосередньо відображені в правових нормах, що обумовлено історичними обставинами в яких знаходилась Україна [37, с. 968-969].

Другий етап, нормативно-правового забезпечення персональних даних припадає на другу половину XX століття коли з концепції «privacy» (або «право на приватність») окремо виділяється сфера правового захисту персональних даних та здійснено їх нормативно-правове регулювання на рівні національного законодавства та законодавства ЄС, яке вперше впроваджує регулювання обігу, обробки, механізмів захисту персональних даних та створення спеціальних інституцій, а також дає відчутний імпульс для розвитку та подальшої уніфікації нормативно-правового регулювання захисту персональних даних. В цей час на території України на рівні радянської конституції було визначено особисті права громадянина, хоча це носило виключно декларативний характер і на законодавчому рівні не було правових механізмів їх реалізації [37, с. 968-969].

Третій етап нормативно-правового забезпечення захисту персональних даних, що розпочався з 2016 року і триває наразі, характеризується створенням загальних стандартів ЄС у сфері захисту персональних даних та закріплення їх на законодавчому рівні ЄС, а також характеризується імплементацією цих стандартів у національне законодавство країн-членів ЄС. В свою чергу, Україна, з отриманням незалежності, почала розвиток законодавства у сфері захисту персональних даних у відповідності до європейських стандартів, що безпосередньо пов'язано з євроінтеграційним курсом України. Таким чином, нині в Україні сформувалась розвинута система нормативно-правового забезпечення захисту персональних даних, яка визначає процедури обробки, зберігання та використання персональних даних. Водночас, в умовах повномасштабної війни органи публічної влади мають активізувати зусилля щодо формування ефективної системи захисту інформаційних ресурсів, створення нормативно-правових та організаційно-технічних передумови до захисту персональних даних громадян [37, с. 968-969].

У перспективі українське суспільство очікує на четвертий, новітній етап нормативно-правового забезпечення захисту персональних даних. На нашу думку, безпосередньо цей етап пов'язаний з абсолютно новим для сучасного технологічного розвитку витком розробки інформаційних технологій, таких як штучний інтелект, що спонукає створення окремої нормативно-правової бази, яка буде регулювати сферу дії та використання штучного інтелекту та забезпечувати захист персональних даних осіб.

### 1.2 Поняття та види персональних даних

У вітчизняній юридичній науці триває пошук моделі адміністративно-правового забезпечення захисту персональних даних суб'єктами публічної адміністрації, яка узгоджувалася б з міжнародно-правовими стандартами та гарантувала ефективний захист прав і свобод людини та громадянина [38], в умовах стрімкого розвитку цифровізації суспільно важливих сфер життя, що

тісно пов’язане з захистом персональних даних громадян та потребує імплементації у національної правової системи у спільний європейський правовий простір.

Характеризуючи персональні дані як суспільну категорію, в першу чергу, необхідно зробити акцент на їх правовій природі та змісті. Термін «персональні дані», знаходить своє широке закріплення на рівні нормативно-правового регулювання у змісті окремих законодавчих та підзаконних актів, а також знаходить своє широке тлумачення на рівні правової доктрини, як правова наукова категорія.

Розглянемо правову природу та сутність персональних даних з позицій адміністративно-правової науки. У сучасній науково-правовій літературі питанням визначення персональних даних присвячено праці представників різних галузей права (конституційного, адміністративного, трудового, цивільного та інших), проте враховуючи, що у більшості випадків питання обробки, зберігання пов’язане з діяльністю суб’єктів публічної влади, ці відносини регулюються у більшості випадків нормами адміністративного права. Незважаючи на певні особливості, викликані галузевою специфікою досліджень, спільною є позиція щодо взаємозв’язку між категорією «персональні дані» та рівнем розвитку сучасної цивілізації [39], її переходом у у цифрову площину, застосування систем для цифровізації інформації та відповідного зростання значення інформації в цілому, як основного ресурсу [40] в сучасному інформаційному суспільстві.

Виокремлення такої категорії як «персональні дані» з більш поширеної категорії «приватне життя», про що нами наголошувалось у попередньому підрозділі дослідження, пов'язане з появою та використанням автоматизованих систем обробки та зберігання інформації, в першу чергу, комп'ютерних баз даних та мережі Інтернет, до яких є можливість отримати віддалений доступ через технічні канали зв'язку.

Відтак, саме ці системи, по суті, зробили революцію у питаннях структурування, обробки, зберігання та, в тому чилі, пошуку необхідних даних.

Все це створило передумови виникнення проблеми захисту конфіденційних відомостей персонального характеру.

По суті, сучасне інформаційне суспільство — це суспільство, в якому інформація є найціннішим ресурсом, засобом суспільного виробництва, а також головним продуктом, який створює найбільшу додаткову вартість. Такі процеси супроводжуються зростанням кількості інформаційних систем та обсягів даних, в тому числі і персональних, що містяться в таких системах, у процесі здійснення комерційної діяльності та наданні публічних послуг.

Виникнення персональних даних як категорії в цілому в праві та, зокрема, адміністративному праві безпосередньо пов'язане з ідеєю захисту приватного життя, яка в умовах розвитку інформаційного суспільства все частіше стає предметом різного виду загроз.

Відтак, саме забезпечення належного рівня захисту персональних даних особи від інформаційних загроз призвело до появи ідеї контролю за обробкою інформації про індивідів – персональних даних, виокремивши їх у особливий вид інформації, яка потребує захисту суб’єктами публічної влади.

Справа полягає у тому, що з розширенням спектра послуг, що надаються публічним і приватним секторами, зросла автоматизована обробка інформації приватного характеру, яка стосується особи.

Незважаючи на те, що комп'ютеризація передбачає низку соціальних та економічних переваг, такий інформаційно-технологічний розвиток також породжує небезпеку зловживання інформацією, наслідки якої можуть завдати набагато більших збитків індивіду і державі в цілому, ніж при старих методах обробки інформації без застосування комп’ютерних технологій.

Сьогодні у правовій науці сформовано різні теоретичні підходи щодо розуміння персональних даних, які відрізняються галузевою спрямованістю та особливістю предмета правового регулювання. В той же час, більшість науковців єдині в думці, що правова природа персональних даних нерозривно пов’язана з приватністю особи та інформацією про неї.

Так, на думку Н.В. Камінської поняття «персональні дані» у національному законодавстві України розглядається через правову категорію «інформація про особу» та безпосередньо «персональні дані» [38].

При досліджені даної категорії в цивільному праві О.А. Дмитренко розглядає поняття «персональні дані», як інформацію, що стосується фізичної особи, яку можна ідентифікувати, і воно є тотожним поняттю «інформація про особу» [41, с.4].

На думку Р.С. Концевого персональні дані – це конкретні відомості про фізичну особу, які включають: ім'я, вік, освіту, місце проживання, тощо [42].

Водночас, Р.А. Майданик наголошує, що персональні дані в цілому слід розглядати, як інформацію про особу. Перелік такої інформації визначений законодавством України [43, с. 902], яке в тому числі регулює питання захисту персональних даних.

Відштовхуючись від правової природи нематеріальних благ, І.М. Сопілко підкреслює, що ідея захисту особистих прав особи вимагає їх охорони й позитивного регулювання обігу інформації про таку особу [44], тобто персональних даних особи.

З позиції правовідносин щодо захисту персональних даних М.І. Саєнко, під поняттям персональні дані розглядає інформацію про живу особу, котра підлягає ідентифікації на основі цих даних та додаткової інформації [45, с.103].

На думку В. Речицького, персональні дані – це не просто конфіденційна інформація, а конкретний тип, різновид [46, с.25], що безпосередньо пов’язаний з особою та інформацією про неї.

Подібних теоретичних поглядів щодо розуміння правової природи персональних даних, як сукупності інформації щодо особи, також дотримаються інші вчені-правники, які визначають персональні дані, як: окремі відомості про фізичну особу чи сукупність таких відомостей, що ідентифікують її або можуть ідентифікувати [47, с. 168]; сукупність задокументованих відомостей про особу [48, с. 176]; сукупність конкретних відомостей про фізичну особу, яка ідентифікується у визначеному законом порядку [49, с. 55];

до змісту інформації про фізичну особу входять: персональні дані (прізвище, ім’я, дата народження, тощо), інформація про особисте життя людини та інше [50, с. 96–97].

А.В. Кардаш підкреслює, що визначення категорії персональних даних має враховувати інформацію про особу за допомогою якої особу ідентифікують [51].

На думку В. Я. Василюк та С.О. Климчук, персональні дані слід розглядати як зафіксовану на матеріальних носіях дані про конкретну особу. До таких даних можна віднести інформацію про особу, відомості про її професію, соціальний стан, фінансове становище, стан здоров’я тощо [52, с. 117].

О. С. Брель вважає, що наведений вище перелік складових персональних не є вичерпним і не визначає, які саме дані про особу можна віднести до персональних [53, с. 220].

На думку Ю. Д. Бєлової, можна визначити такі складові щодо правової природи персональних даних: 1) персональні дані відносяться до особистих немайнових благ; 2) персональні дані – це різновид інформації про особу. Виходячи з цього, на її думку, персональні дані слід розглядати як відомості, що стосуються фізичної особи і дозволяють її ідентифікувати за умови, що такі відомості було зібрано та оброблено із дотриманням вимог законодавства за допомогою інформаційних (автоматизованих) систем [54].

Аналізуючи наведені вище окремі положення адміністративно-правової наукової доктрини зауважимо, що для відмежування персональних даних від інших видів інформації важливим є використання, як основної ознаки персональних даних, наявності взаємозв'язку між суб'єктом, тобто особою, та змістом відповідної інформації про нього.

Таким чином, зв'язок може бути очевидним через беспосередню вказівку на суб'єкта даних з використанням ідентифікуючої інформації про такого суб’єкта, або він може бути потенційно встановлений. Крім того, як додаткову ознаку персональних даних слід розглядати їх формалізований характер. Тобто,

обумовлений цілями та завданнями обробки в інформаційній системі набір відомостей та їх зв'язок з інформаційною системою.

Термін ідентифікація походить від латинського слова identius –тотожний, той же самий і означає встановлення тотожності за якимись ознаками, властивостями. Процес ідентифікації здійснюється шляхом вивчення і порівняння ознак об’єкта, тобто передбачає вивчення двох чи декількох досліджуваних об’єктів, який буде давати можливість не тільки встановити загальні, тобто об’єднуючі, але й відмінні якості.

Під ознаками розуміється об’єктивне відображення якостей предмета, які дозволяють відрізнити даний предмет від всіх інших. Аналіз відмінностей виключно важливий тому, що, у відповідності з положеннями діалектичної логіки, тотожність об’єкта мінлива, рухома, а тому, розглядаючи тотожність як стан відносної постійності, необхідно завжди з’ясовувати чому появилися наявні зміни. Їхнє вивчення дає можливість встановити ту кількість неспівпадаючих ознак, які не виключають висновку про тотожність об’єкта самому собі. Ці відмінності можуть бути як наслідком дій ряду факторів, так і зміною структури об’єкта та умов його використання, а також можуть бути зроблені навмисно, чи утворились випадково. Навмисно створені зміни виключають ідентифікацію, якщо вони суттєво змінюють індивідуальні ознаки об’єкта, тобто є суттєвими, а якщо не суттєві, то ідентифікація здійснюється тому, що визнані зміни порушили тільки деякі якості об’єкта дослідження, але сам він в цілому залишився без особливих змін. Вирішуючи питання про ідентифікацію необхідно мати на увазі і те, що період ідентифікації залежить від чисельних факторів, коли мова іде про конкретну особи.

Очевидним в сучасній юридичній науці також є розуміння персональних даних як різновиду інформації. Відповідно, визначаючи правову природу персональних даних, важливо також з’ясувати співвідношення правових категорій «інформація», «дані» та «відомості».

В першу чергу, варто розглянути категорію «дані», як сукупність відомостей про особу [55]. У свою чергу, поняття «відомості» тлумачиться як

категорія, що виражає певні знання або уявлення про будь-що [56] (об’єкт, особу, тощо).

Вважаємо, що для правильного з’ясування означеного питання доцільно звернутися до лінгвістичного аспекту визначення понять. З огляду на саме смислове навантаження ми вважаємо, що доцільним є використання саме поняття «дані» у нашому випадку, коли мова йде про ідентифікуючу інформацію про особу, є більш правомірним, ніж вживання вужчого за своїм внутрішнім змістом поняття «відомості».

В той же час, поняття «відомості» має тлумачитись широко та включати будь-яку інформацію про особу. В широкому розумінні це передбачає будь-яку інфрмацію про особу. За характером об’єктивну інформацію, яка не залежить від волі суб’єкта персональних даних та інших осіб суб’єктивну інформацію, яка відобража суб’єктивну точку зору. За змістом, що включають інформацію про особисту сферу і передбачає забезпечення захисту особистих прав; сферу професійної та громадської діяльності особи [54], яка зібрана та передана у будь-який спосіб, перебуває на зберіганні на будь-яких носіях, а також зібрана за допомогою штучного інтелекту.

Словосполучення "відомості чи сукупність відомостей" повинно тлумачитися широко і включати будь-яку інформацію про особу. Ця інформація може бути об’єктивною, тобто незалежною від волі суб'єкта персональних даних та інших осіб, або суб'єктивною, що відображає особисту точку зору, таку як оцінка, характеристика або рецензія. Вона може також охоплювати інформацію про інтимну та особистісну сфери життя особи, а також її громадську, господарську та професійну діяльність. Персональні дані можуть бути текстовими, графічними, звуковими або відео-інформацією, включаючи цифрові дані, та можуть бути збережені на будь-якому носії, такому як папір, електронні пристрої, компактні диски тощо. Крім того, необхідно враховувати, що персональні дані можуть бути неповними, неточними або застарілими, і вони також підпадають під захист.

Важливо пам’ятати, що йдеться про ідентифікуючу інформацію про особу, а тому, з цього погляду, більш виправданим виступає визначення змісту поняття такої ідентифікуючої інформації саме у вигляді даних, а не відомостей про особу, оскільки дані, їх одержання і використання у соціально важливих відносинах за участі певного суб’єкта становлять кінцеву мету правового регулювання.

У процесі публічного управління, у розпорядженні органів публічної влади надходять саме дані про особу, що втілюються у вербальній, графічній, предметній або наглядно-образній формі, стають уже у подальшому, у процесі розумової діяльності та обробки здобутої інформації даними про особу. Отже, саме дані, а не відомості є результатом фіксації інформації про особу.

Виходячи з викладеного розуміння персональних даних, справедливим, на нашу думку, буде таке визначення понять: це результат фіксації ідентифікуючих ознак людини (фізичної особи або громадянина); це інформація у вигляді даних, втілена в певних матеріалах (матеріальних носіях). Таке розуміння повністю відповідає загальноприйнятому визначенню поняття інформації як суспільного явища, яке відображає відомості про навколишній світ та процеси, які відбуваються у ньому та можуть сприймаються особою за допомогою спеціальних пристроїв або безпосередньо [57].

Важливо пам’ятати, що інформація (лат. informatio - обізнаність) – буквально означає свідчення, знання, дані. А відтак, інформація про особу – це фактично і є дані. Поняття інформація позначається не тільки як відомості, що передаються людьми під час спілкування [57], а також відомості, які обробляються та зберігаються.

Крім того, в широкому розумінні інформація – це одна з головних властивостей об’єктивного світу, яка зумовлена наявністю у ньому особливих процесів, що мають назву інформаційні [57], в тому числі, інформація про особу.

На основі такого теоретичного підходу до розуміння персональних даних, перейдемо до аналізу їх нормативно-правового закріплення в національному законодавстві та забезпечення захисту персональних даних.

В Україні суспільні відносини, пов'язані із персональними даними регулюються на рівні законодавчих та підзаконних актів. Беручи за основу такий підхід наголосимо, що на загальному рівні регулювання суспільних відносин щодо захисту персональних даних здійснюється на основі Конституції України, яка регулює основні конституційні права людини, в тому числі особисті права, такі як право особи на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), право на особисте і сімейне життя (ст. 32) [58].

До загальних норм щодо захисту персональних даних також можна віднести положення Закону України «Про звернення громадян», який містить вимоги щодо заборони розголошення одержаних із звернень відомостей про особисте життя громадян без їхньої згоди чи відомостей, що становлять державну або іншу таємницю, яка охороняється законом, та іншої інформації [59]

Стаття 11 Закону України «Про інформацію» прирівнює їх до «інформації про фізичну особу» [24]. Більше того, ст. 8 Закону України «Про захист персональних даних» кваліфікує права суб’єкта персональних даних як особисті немайнові права, однією з ознак яких є їх специфічний об’єкт, тобто те, на що спрямоване дане право [23].

Закони України «Про захист персональних даних» (ст. 2) [23] та «Про інформацію» (ст. 11) [24] закріплюють наступне визначення персональних даних: «персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована».

Суміжними правовими категоріями до поняття персональних даних у вітчизняному спеціальному законодавстві виступають наступні поняття: «інформацію про особисте життя фізичної особи» (ст. 302 ЦК України) [33]; «інформацію про фізичну особу» (ст. 11 Закону України «Про інформацію»)

[24]; «відомості, що дають можливість ідентифікувати фізичну особу» (Закон України «Про доступ до судових рішень» [60]); «відомості, що ідентифікують особу» (Закон України «Про організацію формування та обігу кредитних історій» [61]); «відомості про особисте життя громадян» (Закон України «Про звернення громадян» [59]); «інформація про приватне життя громадянина» (Закон України «Про телебачення і радіомовлення» [62]). З аналізу вище наведених термінів вбачається, що кожен з них цілком може бути замінений поняттям «інформація про фізичну особу» або «інформація про особисте життя фізичної особи».

На рівні судової практики визначення поняття персональних даних міститься і у рішенні Конституційного Суду України від 20.01.2012 р. № 2-рп/2012. Конституційний Суд України тлумачить поняття персональних даних, як: конфіденційну інформацію про фізичну особу; будь-які відомості або їх сукупність про фізичну особу; інформація про особисті майнові та немайнові відносини цієї особи з іншими особами. Зазначена інформація про фізичну особу та її членів сім'ї є конфіденційною і може бути розголошена лише за їхньою згодою, якщо закон не передбачає іншого. Згодом на поширення такої інформації можуть впливати інтереси національної безпеки, економічного добробуту та прав людини, які законом визначено як обґрунтовані. [63].

Таким чином, є очевидна невідповідність між рівнем доктринального визначення, нормативно-правового закріплення та розуміння у правозастосовній діяльності поняття і характеристики персональних даних.

Водночас необхідно підкреслити, що поняття «персональні дані» отримало своє нормативно-правове закріплення у міжнародних нормативно-правових актах. Зокрема, поняття «персональні дані» визначається Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних як будь-яка інформація, що стосується конкретної особи або особи, що може бути конкретно визначеною (ст. 2) [6].

В свою чергу, директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне

переміщення таких даних» визначає персональні дані, як будь-яку інформацію, яка стосується ідентифікованої фізичної особи чи фізичної особи, і яку можна ідентифікувати (ст. 2) [14].

Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення даних надає наступне визначення персональних даних – це відомості про конкретну фізичну особу або дані про неї, які прямо чи опосередковано стосуються фізичної особи (тобто, суб'єкта персональних даних)[20].

Подібний підхід відповідає і головному сучасному орієнтиру в умовах адаптації вітчизняного законодавства – вимогам європейських директив щодо визначення персональних даних та їх складових. У цьому контексті заслуговує на увагу діюча наразі в умовах нового Регламенту (Євросоюзу) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних «Позиція про концепцію персональних даних від 20 червня 2007 року» (далі – Позиція WP 136). Розділ III Позиції WP 136 виділяє в конструкції персональних даних чотири елементи: «будь-яка інформація», «що стосується», «ідентифікованої або здатний бути ідентифікованою», «фізичної особи» .

Варто звернути увагу на два центральні елементи: «що стосується» і «ідентифікованого або здатний бути ідентифікованою», оскільки вони найбільше характеризують бік контролера персональних даних як учасника даних правовідносин [64].

Дані, «що стосуються» суб'єкта, включають не тільки інформацію про самого суб'єкта, але й про належні йому або іншим чином пов'язані з ним об'єкти, тому числі і тварини.

Таким чином, даними, що «що стосується» суб'єкта, є не тільки номер телефону, автомобіля, комп'ютера, банківської картки, фітнес трекера, чіпа тварини, але й інші характеристики цих об'єктів та тварин: ціна, знос, серійні номери, поломки, діагнози, результати аналізів тощо. Позиція WP 136 також

виділяє три елементи, кожен і наявність хоча б одного з таких елеметів відносить будь-яку інформацію, до такої «що стосується» суб'єкта — це зміст, мета та результат [64].

Інформація може відноситися до суб'єкта за своїм змістом, якщо така інформація стосується конкретної фізичної особи, як наприклад, результати тестів на іспиті, номер телефону конкретної особи, профіль певного користувача у соцмережах. Інформація може відноситися до суб'єкта також з мети, якщо вона використовується або, найімовірніше, буде використана з метою оцінки, впливу на статус чи поведінку суб'єкта, прояви певного роду ставлення до суб'єкта.

Наприклад, список відвідуваних співробітниками компанії інтернет сторінок у корпоративній мережі може бути використаний для цілей моніторингу ефективності використання робочого часу кожним співробітником, або для блокування певних сторінок певним співробітникам. Інформація може відноситися до суб'єкта персональних даних, навіть якщо відсутні ознаки «змісту» та «мети», проте є ознаки результату, тобто якщо обробка даних, найімовірніше, вплине на права та інтереси суб'єкта, наприклад, навіть якщо злегка змінить ставлення оточуючих до нього, змусить виділяти його серед інших у співтоваристві.

Ці три елементи відношення даних до суб'єкта застосовуються кожен окремо, але, наявність одного елементу не потребує виявляти інші два, в цьому випадку дані точно відносяться до суб'єкта. Наступна частина конструкції персональних даних «ідентифікований або здатний бути ідентифікованим» відповідно до Позиції WP139 визначає особу як ідентифіковану, якщо вона ще не ідентифікована, але її можливо ідентифікувати прямо. Наприклад, за ім'ям (якщо вона дозволяє виділити суб'єкта з групи) або побічно — за номером паспорта, автомобіля, телефону або комбінації суттєвих критеріїв, що дозволяють виділити суб'єкта із групи (це може бути вік, місце проживання, зовнішній вигляд тощо) [64].

Проте лише гіпотетична ймовірність ідентифікації суб'єкта робить інформацію персональними даними. Якщо можливість ідентифікувати суб'єкта відсутня чи мізерно мала, дані не вважаються персональними. Деякі контролери користуються з цього як аргументу, що в них і в думках не було ідентифікувати когось, що вони лише збирають номери телефонів, автомобілів і деяких карт, що належать суб'єктам. Але ми розуміємо, що ідентифікація за цими номерами можлива в порівнянні з іншою базою даних, наприклад, в рамках міжвідомчого обміну даними, отримання даних, наприклад з дорожніх камер відеоспостереження [64]**.**

Для оцінки ступеня та ймовірності використання можливості ідентифікації суб'єктів контролером або будь-якою третьою особою, яка має доступ до інформації, необхідно визначити розумні зусилля, які потрібно буде здійснити для цієї ідентифікації. Така оцінка включає в себе розгляд таких аспектів, як витрати ресурсів, зокрема – фінансових, часових і людських, які необхідні для проведення такої ідентифікації. Також важливо врахувати наявність технологій, які можуть спростити цей процес та знизити витрати зусиль і ресурсів. Потрібно врахувати, що під «розумними зусиллями» мається на увазі не лише офіційна оголошена мета, але і загальна стратегія обробки даних. Окрім того, варто розглянути потенційні вигоди, які може отримати контролер або третя особа в результаті ідентифікації суб'єктів. Тривалість зберігання даних і можливий технологічний прогрес також слід враховувати, оскільки вони можуть вплинути на можливості ідентифікації у майбутньому [64].

У кожному конкретному випадку необхідно визначати наявність можливості та ресурси контролера, що додаються, для ідентифікації суб'єктів за номером телефону. За наявності можливості, мети, або контекст обробки передбачає ідентифікацію суб'єкта за номером телефону, в цьому випадку номер телефону є персональними даними. Наприклад, номер телефону — є персональними даними, оскільки він залежно від ситуації або є ідентифікатором особи, або є інформацією, що відноситься до «ідентифікованої

або здатний бути ідентифікованою» фізичної особи. Всі інші номери та характеристики об'єктів і живих істот, що належать суб'єкту, в тому чи іншому контексті обробки, також можуть кваліфікуватися як персональні дані. Навіть за відсутності прізвища ім’я або по батькові суб'єкта персональних даних у контролера та будь-якої третьої особи, і навіть за відсутності у них можливості ідентифікувати суб'єкта, вони все ж таки мають можливість порушити його права та інтереси [64]**.**

Контактні дані, такі як номер телефону, електронна пошта, адреса тощо представляють собою важливі елементи особистої інформації, які можуть бути використані зловмисниками для встановлення безпосереднього контакту з особою проти її волі. Це може призвести до серйозних наслідків, таких як загроза життю та безпеці, маніпулювання особою, настирливе привертання уваги, заважання особистому та професійному життю. Враховуючи ці ризики, важливо, щоб суб'єкти персональних даних виявляли розсудливість при наданні своїх контактних даних третім особам. Компроментація такої інформації може спонукати суб'єкта до необхідності зміни свого номера або місця проживання, порушуючи не лише його власні інтереси, але і інтереси третіх осіб, таких як родина суб'єкта. У зв'язку з цим, розробка ефективних заходів захисту особистих даних передбачає удосконалення свідомості суб'єктів щодо ризиків, пов'язаних з розголошенням своїх контактних даних, та прийняття відповідних заходів обережності.

Як вказано вище, навіть при відсутності прямої ідентифікації суб'єкта, за володіння третіми особами контактними даними може тягнути за собою порушення прав особи. Конфіденційність персональних даних, зокрема контактних даних, відіграє значну роль у забезпеченні безпеки життя та здоров'я суб'єкта, його близьких осіб, дозволяє контролювати зовнішні комунікації, знижує доступність для зовнішнього світу, сприяє формуванню особистих меж суб'єкта та захищає його особистий простір. Персональні дані є інформацією, яка може бути пов'язана з конкретним індивідом, тобто, персоніфікованою.

Відтак, можемо констатувати, що визначення персональних даних на рівні національного законодавства в цілому відповідає європейським стандартам, закріпленим у вказаних міжнародних нормативно-правових актах. Із врахуванням того, що визначення персональних даних у національному законодавстві суттєво засноване на Директиві 95/46/ЄС, належить розглянути можливість використання рекомендацій, розроблених робочою групою з захисту фізичних осіб у зв'язку з обробкою персональних даних, як основи для визначення характеристик персональних даних (Позиції WP139) [64].

У сучасному світі важко уникнути ідентифікації особи, однак обмеження зберігання, обробки та використання персональної інформації без згоди суб'єкта є необхідним та важливим. Заходи, спрямовані на забезпечення безпеки та запобігання незаконним діям щодо персональних даних, отримали правове визначення – «захист персональних даних».

Стосовно персональних даних у режимі обмеженого доступу слід вести мову про «правовий режим конфіденційності персональних даних», який має власний зміст і поширюється на випадки обробки персональних даних на умовах дотримання конфіденційності. Конфіденційність персональних даних є встановленою законодавством вимогою, зверненою виключно до оператора, обробника персональних даних, органу захисту персональних даних, працівника оператора, а також іншої особи, тобто конфідентам, які отримали доступ до персональних даних на законній підставі. Конфіденційність, як обов'язкова вимога, виникає з отримання доступу до персональних даних конфіденту, за відсутності у нього законних підстав для обробки їх у режимі загальнодоступної інформації.

З метою усунення колізій, що виникають із співвідношенням правового режиму конфіденційності персональних даних з іншими правовими режимами конфіденційної інформації, такими як: лікарська таємниця, таємниця зв'язку, адвокатська, нотаріальна, банківська таємниці та ін., бажано закріпити в Законі України «Про захист персональних даних» норму, яка б встановила пріоритет вимог режиму конфіденційності персональних даних, які мають бути виконані

конфідентами за умов, коли іншими режимними вимогами передбачається нижчий рівень захищеності інформації.

Для вирішення проблем, що виникають у правозастосовній практиці, важливо запропонувати використання та пряме закріплення в законодавстві положення про «презумпцію конфіденційності персональних даних» як один із принципів, передбачених статтею Законі України «Про захист персональних даних».

Завершуючи характеристику змісту поняття персональних даних наголосимо на важливому публічно-правовому аспекті даного питання. Аналіз законодавства доводить, що у окремих випадках персональні дані можуть носити і неправдивий характер. У цьому разі вони відіграють роль утаємничення справжньої особистості громадянина та заважають його невибірковій ідентифікації. Такими можуть бути персональні дані, які містяться у документах прикриття осіб залучених до спеціальних заходів з протидії злочинності або оперативно-розшукових заходах.

З певних мотивів особа може свідомо перекручувати або змінювати власні персональні дані або «викрадати» та привласнювати дані інших осіб видаючи себе за них у певних правовідносинах та інше. Зазначене знаходить своє відображення у Законі України «Про державний захист працівників суду і правоохоронних органів» як основному нормативно-правовому акті, що регулює правовідносини в сфері державного захисту [65]; Законі України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» [66] та інших нормативно-правових актах, таких як  закони України: «Про оперативно-розшукову діяльність» [67]; «Про розвідку» [68], «Про Службу безпеки України» [69]; «Про Державне бюро розслідувань» [70].

Зазначене дозволяє нам сформулювати видове по відношенню до категорії «персональні дані громадян» поняття «фіктивних персональних даних», визначивши його як відомості чи сукупність відомостей про фізичну особу відображені у документах, що не дають можливості здійснити її невибіркову ідентифікацію та отриманих такою особою у зв’язку з застуванням

щодо неї та членів її сім'ї заходів особистого захисту, або виступають елементом здійснення негласних слідчих дій, оперативно-розшукових, розвідувальних та контррозвідувальних заходів за участі такої особи.

Наразі у правовій науці постає потреба у розробці підходів до класифікації персональних даних із низкою різноманітних критеріїв з метою якомога більш глибокого та системного визначення усіх складових вказаної категорії. Деякі дослідження наголошують на правильності співвідношення персональних даних з іншими суміжними поняттями та категоріями. Це має суттєвий вплив не лише на результати наукових досліджень, але і на практику правозастосування в сфері захисту персональних даних [71]. Персональні дані є структурованим утворенням. Персональні дані, як і будь-яка інша складна система, складаються з численних елементів, які групуються за певними критеріями у відповідні підсистеми, що дозволяє здійснити їх класифікацію.

Саме поняття «класифікація» походить від латинського classis, що означає розряд або клас. Поняття «класифікація» означає поділ сукупності предметів, суспільних явищ, правової категорії за відповідними спільними ознаками з утворенням певних систем, підсистем, класів такої сукупності [72].

Відтак, в юридичній науці під класифікацією слід розуміти харакеристику певного суспільного явища, правової категорії, поняття за певними ознаками, використовувану як засіб для встановлення взаємозв'язків між цими поняттями. Використання певних спільних ознак, притаманних цим поняттям, дозволяє визначити систему, взаємозв'язок та підпорядкованість понять. Таким чином, спільні ознаки виступають основою класифікації і відіграють вирішальну роль для отримання результату класифікації.

Отже, класифікація персональних даних громадян може бути використана для отримання інформації про різноманітні аспекти об'єкта нашого дослідження. У контексті даного дослідження – це масив персональних даних, що характеризують різноманітні змістовні характеристики ідентифікуючих ознак та різного роду процедур та дій з ними пов'язаних.

Класифікація структурних елементів персональних даних, що у своїй сукупності створюють певне правове явище, що сприяє більш цілісному теоретичному та практичному його дослідженню.

З точки зору практики, класифікація персональних даних, сформована і перенесена із теоретичної сфери у сферу реального життя, де відбувається реальний захист персональних даних, допомагає визначати поведінку учасників суспільних відносин, пов'язаних із забезпеченням захисту персональних даних. Наприклад, сформувати різні нормативно-правові та організаційно-правові засади забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації та їх посадовими особами. Поведінка суб'єктів цих відносин у даному випадку буде мати чіткий, нормативно врегульований, системний характер, що безпосередьо впливає на ефективність здійснення забезпечення персональних даних громадян.

Нині, в науковій літературі можемо знайти різні теоретичні підходи та різні варіанти щодо класифікації персональних даних громадян з врахуванням різноманітних критеріїв. Так, наприклад, за ступенем пов'язаності з особою персональні дані поділяють на постійні (антропологічні ознаки, функціональні ознаки, особливості письма) та змінювані (адреса проживання, місце роботи) [73, с. 153].

За особливостями правового регулювання, персональні дані можна класифікувати на: загальні персональні дані про особу (прізвище, ім'я, батькові, дата народження тощо; вразливі персональні дані про особу (дані національність, політичні або релігійні переконання, політичні погляди та участь у політичних партіях і громадських організаціях, дані про притягнення до юридичної відповідальності, дані про стан здоров'я тощо; спеціальні персональні дані про особу (персональні дані, що не входять довище зазначених категорій і межі обігу яких визначаються суб'єктом зазначених даних ) [74, с. 94].

Залежно від того, якими органами чуття сприймаються ідентифікуючі ознаки персональних даних громадян – зорові (зокрема текст, фото) та звукові [41, с. 28].

За співвідношенням із метою використання запропоновано поділ персональних даних громадян на повні, неповні та надмірні (виходячи з тлумачення ст. 6 Закону «Про захист персональних даних»). Якщо повні дані дають можливість з високою ймовірністю ідентифікувати особу, то неповні відображають лише певну складові (наприклад, місце проживання або лише номер телефону). Надмірні персональні дані можуть включати в себе як певну ідентифікуючу інформацію так і інші відомості, що можуть бути корисними для суб'єкта їх використання (наприклад, художні або кулінарні смаки).

Також є інші критерії та способи поділу персональних даних за різними критеріями: за змістом – біометричні та не біометричні; за ступенем доступу – конфіденційні та ті, що знаходяться в загальному доступі.

Також, персональні дані громадян можна класифікувати за іншими критеріями, такі як: предмет відносин (біометричні, біографічні тощо); ступенем неконтрольованого обігу (вразливі, звичайні); можливостями ідентифікації (прямо ідентифікуючі, опосередковано ідентифікуючі); за метою використання (надмірні дані, повні дані, неповні дані); повнотою відображення дійсності (достовірні дані, недостовірні дані) тощо [41, с. 9].

Зазначені вище теоретичні підходи та критерії щодо класифікації персональних даних не є вичерпними та можуть бути розширені. Відтак, підхід щодо вибору критеріїв класифікації повинен мати наукове підґрунття та враховувати необхідність застосування на практиці для ефективного забезпечення захисту персональних даних. У контексті нашого дослідження доцільно підходити до класифікації персональних даних, вибору відповідних критеріїв, таким чином, щоб відобразити їх спільні ознаки та харатерні відмінності для вдосконалення правового регулювання суспільних відносин у сфері персональних даних.

Виходячи із зазначеного, ми пропонуємо класифікувати персональні дані громадян, виходячи із критеріїв їх змістового наповнення та рівня доступності, на такі групи: загальнодоступні (загальні), спеціальні та біометричні.

До загальних даних особи, на нашу думку, слід відносити персональні дані, які виступають базовими для її ідентифікації (прізвище, ім'я, по батькові, адреса особи, паспортні дані, сімейний стан тощо); дані про освіту; інформацію про місце роботи; інформація про майновий стан та ін. Загальні персональні дані особи можна знайти в загальному доступі у відкритих державних реєстрах, засобах масової інформації, мережі інтернет, довідковій документації. Інформація, яка є загальнодоступною, може бути використана будь-якою зацікавленою особою. Необхідно наголосити, що у відповідності до чинного законодавства загальнодоступними є дані про доходи, витрати, спосіб життя політичних осіб, представників влади, чиновників, які займають керівні посади.

Взяті окремо базові персональні дані громадян загального характеру дозволяють ідентифікувати особу та можуть бути віднесені до інформації про людину, яка може вважатися ідентифікованою. Інформація про людину, яка є загальною, зазначена в паспорті, у військовому квитку, у документі про освіту, та ін. Отримати доступ до подібних персональних даних громадян досить просто, а це часто призводить і до відповідних проблем, зокрема, отримання «маркетингових» рекламних пропозицій та ін.

Біометричні персональні дані громадян характеризують носія за біологічним та фізіологічним (антропологічним) принципом. До них відносять дані, які стосуються фізичного та фізіологічного стану особи: дані про зріст, вагу, колір очей; інформацію про групу крові; дані аналізу ДНК та ін.

Так, наприклад, обробка дактилоскопічної інформації в системі біометричної ідентифікації здійснюється шляхом перетворення зображення папілярних візерунків на проміжній поверхні в цифрову форму та розміщення даних у базі даних у вигляді біометричного інформаційного шаблону. У зв'язку з тим, що дактилоскопічна інформація використовується для встановлення особистості конкретної особи і характеризує фізіологічні та біологічні

особливості людини. До біометричних персональних даних зараховують інформацію, що отримується в результаті відео- та фотозапису за участю людини.

Біометричні дані про особу, з нашої точки зору — це персональні дані, отримані в результаті спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових рис фізичної особи, а також дозволяють зробити або підтверджують однозначну ідентифікацію конкретної фізичної особи за сукупністю таких фізіологічних даних.

До біометричних персональних даних громадян можемо віднести фізіологічні та генетичні дані про особу та дані, що становлять собою медичні персональні дані особи. Генетичні дані про особу, на нашу думку, це персональні дані, що відносяться до набутих або спадкових ознак фізичної особи, які містять інформацію про фізіологію та стан здоров'я людини. Генетичні дані особи розуміються як персональні дані щодо генетичних характеристик фізичної особи, отриманих в результаті аналізу біологічного зразка такої фізичної особи, зокрема, аналіз хромосом, дезоксирибонуклеїнової кислоти (ДНК) або рибонуклеїнової кислоти (РНК), або в результаті аналізу інших генетичних елементів.

Персональні дані, що стосуються здоров'я, з нашої точки зору, це також персональні дані про фізичний та/або психічний стан фізичної особи, в тому числі про користування медичними послугами, що розкривають інформацію про стан її здоров'я.

Дані про стан здоров’я можуть бути надані з різних джерел: дані, зібрані з використанням картки пацієнта (наприклад, історія хвороби та результати обстежень і надання медичної допомоги); відомості отримані шляхом перехресного посилання на інші джерела (наприклад, ризики викликані високим кров’яним тиском, виміряного протягом певного періоду часу); відомості «самоперевірки» (наприклад, зазначення симптомів); контекстна інформація, яка стає даними про стан здоров’я (наприклад, відомості щодо нещодавньої поїздки або перебування в регіоні, охопленому інфекційними

захворюваннями, оброблена медичним працівником для встановлення діагнозу) [75].

До спеціальних персональних даних громадян ми пропонуємо відносити інформацію щодо участі у політичних партіях та громадських організаціях, а також віросповідання та форму релігійної приналежності, переконання світоглядного характеру, відомості про наявність або відсутність судимості, звички та переваги в особистому житті, гендерна орієнтація та переваги, інформація з реєстрів нерухомого майна.

Аналіз сучасних теоретичних підходів до поняття персональних даних дозволяє зробити нам власне визначення. Персональні дані громадян – це будь-які відомості або дані, в об’єктивізованій формі, що стосуються суб’єкта даних (фізичної особи), який підлягає ідентифікації.

При цьому фізична особа, що піддається ідентифікації, — це реальна фізична особа, яку можна визначити у прямий чи опосередкований спосіб, зокрема, за допомогою певних відомостей ідентифікуючого характеру, таких як ім'я, прізвище, по-батькові, ідентифікаційний номер, дані про народження, місцезнаходження, онлайновий ідентифікатор, або на один або кілька факторів (їх поєднання), які є специфічними та винятково властивими для соціальної, генетичної, фізичної, фізіологічної, інтелектуальної, майнової, культурної ідентичності цієї особи.

Персональним даним громадян притаманні наступні ознаки: інформаційний зміст персональних даних – вони є відомостями або даними про конкретну фізичну особу; ідентифікуючі властивості – вони дозволяють визначити (ідентифікувати ) конкретну фізичну особу; визначена форма фіксації у певному джерелі (носії) персональних даних; не вичерпність; правова форма персональних даних, яка розпочинається із початком сукупності дій пов’язаних із їх обробкою та забезпеченням захисту.

Враховуючи визначення персональних даних з позиції адміністративно-правовго регулювання та міжнародно-правового регламентування ми можемо запропонувати наступний підхід щодо виділення їх видів. Так пропонуємо

розділити персональні дані громадян на такі групи, використовуючи критерії їх змісту та рівня визначеної можливості доступу до них: на загальні дані про особу, спеціальні дані про особу, а також біометричні дані про особу. При цьому видами біометричних персональних даних громадян виступають генетичні дані про них та відомості, що стосуються їх здоров'я або отриманої медичної допомоги.

### 1.3 Суб’єкти персональних даних: поняття та класифікація

Важливе значення для дослідження адміністративно-правового забезпечення захисту персональних даних громадян суб’єктами публічної адміністрації є визначене коло учасників адміністративних правовідносин у зазначеній сфері. До суб’єктів адміністративно-правових відносин, поряд з фізичними та юридичними особами приватного права, належать органи публічної влади, як юридичні особи публічного права. Особливо необхідно розглянути правовий статус фізичних осіб, які виступають суб’єктами персональних даних.

Особливу роль у розумінні місця та значення суб’єктів здійснення адміністративно-правового забезпечення захисту персональних даних відіграє чітке законодавче визначення компетенції суб’єктів, яке включає повноваження, права, обов’язки та відповідальність за результати своєї діяльності.

При цьому важливо враховувати такі особливості. По-перше, здійснюючи правове регулювання повноважень та діяльності таких суб’єктів, необхідно враховувати специфіку суспільних відносин, пов’язаних із захистом персональних даних, які виступають невід’ємною складовою особистих немайнових прав, зокрема, права на приватність. По-друге, важливим є чітке визначення повноважень органів публічної влади щодо забезпечення захисту персональних даних з тією метою, щоб здійснення їх функцій не «блокувалися» повноваженнями інших суб’єктів публічної влади, або суб’єктів приватного

права. По-третє, це необхідність узгодження повноважень окремих суб’єктів та організація взаємодії між різними суб’єктами адміністративно-правового забезпечення захисту персональних даних.

Розглянемо загально-теоретичні підходи до розуміння суб’єктів правовідносин. Зокрема, О. Ф. Скакун до структури правовідносин відносить: юридичний факт, суб’єкти, юридичний зміст і його структуру та об’єкт [77, с. 525].

Таким чином, суб’єктом правовідносин є носій суб’єктивних прав та обов’язків. Суб’єкти наділені правосуб’єктністю, яка є сукупністю правоздатності та дієздатності [78, с. 127].

В адміністративному праві, суб’єкт – це учасник правовідносин, який наділений правами та обов’язками у сфері адміністративної діяльності. Адміністративна діяльність – це спрямована на досягнення певних цілей практична робота уповноважених учасників управлінських процесів, спрямована на організацію та координацію соціальних систем і процесів з використанням інструментів, методів та підходів, характерних для владної діяльності [79, с. 43], зокрема в процесі забезпечення захисту персональних даних.

На думку В.Б. Авер’янова, з погляду адміністративного права, суб'єкт часто визначається як учасник суспільних відносин, який має особисті права та зобов'язання, встановлені нормами адміністративного права [80, с. 214–215].

У цьому контексті Т. О. Коломоєць наголошує, що суб'єкт адміністративного права – це юридична або фізична особа, яка виступає в якості носія прав та обов'язків у сфері державного управління, які передбачені адміністративно-правовими нормами, та має здатність реалізувати надані права та виконувати покладені обов'язки [81, с. 78], в тому числі щодо збору, обробки, зберігання, захисту персональних даних як важливих елементів суспільних відносин, врегульованих нормами адміністративного права.

Варто зазначити, що суб’єкти адміністративно-правових відносин поділяються на приватних та публічних суб’єктів. До публічних суб’єктів

відносяться суб’єкти публічної влади, суб’єкти публічного управління (адміністрування).

В цьому аспекті варто зазначити, що суб’єкт публічної адміністрації – це суб’єкт владних повноважень, наділений законом повноваженнями здійснювати публічне адміністрування – надавати адміністративні послуги чи здійснювати виконавчо-розпорядчу діяльність [82]. Відтак, держава виступає учасником взаємодії через органи публічного управління (адміністрування) та їх посадових осіб, які наділені правами та обов’язками у конкретній сфері та провадять адміністративну діяльність [83].

В. Б. Авер’янов зазначав, що у контексті правовідносин, суб'єкт адміністративного права має лише потенційну можливість вступати у такі відносини. Він вважав, що суб'єкт адміністративних правовідносин – це фактичний учасник правових зв'язків, тобто він обов'язково бере у них активну участь, тоді як суб'єкт адміністративного права виступає як претендент на таку участь [80, с. 95].

Відтак, суб’єкт публічної адміністрації або суб’єкт публічного адміністрування – це суб’єкт, який у межах власних або делегованих повноважень здійснює практичну реалізацію функцій виконавчої влади, а саме бере участь у формуванні державної політики та її реалізації шляхом виконання Конституції та законів України. Відповідно публічна адміністрація в широкому розумінні є системою суб’єктів публічного адміністрування [84, с. 87], які здійснюють публічне управління у всіх сферах суспільного життя, зокрема щодо захисту персональних даних громадян.

Ю. А. Ведєрніков визначає суб'єкта адміністративного права як особу (юридичну чи фізичну), яка має права та обов'язки у сфері державного/публічного управління, передбачені відповідними адміністративно-правовими нормами, та здатну реалізовувати надані їй права і виконувати покладені обов'язки [85]. Суб’єкти адміністративно-правових відносин можуть здійснювати свої повноваження при наявності правосуб’єктності. Правосуб’єктність мають як суб'єкти права, так і учасники

правовідносин. Тобто, їх певні спільні риси можуть призвести до їхнього ототожнення. Однак, краще розрізняти зазначені поняття. По-перше, суб'єкти права можуть бути лише потенційними учасниками правовідносин. По-друге, володіння правами та їх реалізація можуть мати місце не лише у межах конкретних правовідносин. Наприклад, це може бути втіленням загальних норм, які визначають правовий статус і компетенцію суб'єкта права, що означає безперешкодне користування суб'єктом юридичними правами та виконання суб'єктивних юридичних обов'язків поза конкретними відносинами між суб'єктами права [86, с. 201]. Тому, важливо провести чітке розмежовування між суб'єктом адміністративного права та суб'єктом адміністративних відносин, звертаючи увагу на певні умови, за яких суб'єкт адміністративного права стає учасником адміністративних правовідносин. Ці умови включають наявність адміністративно-правових норм, що визначають права та обов'язки суб'єкта, а також адміністративну здатність та дієздатність суб'єкта. Також важливими є підстави для виникнення, зміни та припинення правовідносин [85].

При цьому, Т. О. Мацелик звертає увагу на те, що у всіх визначеннях суб'єктів адміністративно-правових відносин основний акцент робиться на адміністративно-правових нормах, які передбачають, встановлюють та формулюють права та обов'язки суб'єктів адміністративного права [87].

До суб’єктів адміністративно-правових відносин належать суб’єкти публічного адміністрування, які у межах власних або делегованих повноважень здійснюють практичну реалізацію функцій влади та складають відповідну систему, наділену вертикальною та горизонтальною компетенцією (повноваженнями), а також приватних суб’єктів (фізичних осіб, юридичних осіб, їх об’єднань, організацій та інших представників громадянського суспільства), у взаємодії з якими публічні органи влади беруть участь у здійсненні управління певними соціальними процесами.

Виходячи з такого теоретичного розуміння суб’єктів адміністративно-правових відносин у сфері захисту персональних даних, розглянемо таку групу

суб’єктів як безпосередньо суб’єкти персональних даних. Варто зазначити, що правовий статус суб’єктів адміністративно-правових відносин щодо збирання, зберігання, обігу та обробки персональних даних не однаковий, оскільки кожен з них виступає у своїй особливій ролі. Крім того, в кожному конкретному випадку такі суб’єкти будуть користуватися конкретними правами та нестимуть конкретні обов’язки як суб’єкти інформаційних відносин, пов’язаних із забезпеченням захисту персональних даних. Правові відносини, пов'язані з обігом та обробкою персональних даних, так само, як і інші відносини у цій сфері, мають стандартний склад, що включає учасників, їхні права та обов'язки, а також обставини, що призвели до виникнення цих відносин та конкретні юридичні факти [23].

Серед суб’єктів таких правовідносин можна виділити дві групи. Зокрема, на суб’єктів публічного управління (адміністрування), як суб’єктів адміністративно-правових відносин у сфері забезпечення захисту персональних даних покладається обов’язок безпосередньо забезпечення захисту персональних даних громадян, яких ми розуміємо як суб’єктів персональних даних. Фізичні особи-громадяни, в свою чергу, як суб’єкти адміністративних правовідносин мають право на захист персональних даних. Закон України «Про захист персональних даних» не визначає чітких критеріїв, а лише зазначає, що суб’єктом персональних даних є фізична особа, відносно якої відповідно до нормативно-правових вимог здійснюється обробка її персональних даних [88, с. 16].

Поняття «суб’єкт персональних даних» є вужчим за змістом ніж категорія «суб’єкти правових відносин, пов'язаних із персональними даними». Суб’єкти персональних даних є елементом системи суб’єктів правових відносин, пов'язаних із персональними даними у розумінні ст. 4 Закону України «Про захист персональних даних» [23], а саме виступають носієм тих суб’єктивних прав, пов’язаних з персональними даними, які підлягають захисту.

Аналіз наведеної законодавчої дефініції дає підстави наголосити, що суб’єктом персональних може бути лише фізична особа, тобто, людина як

учасник адміністративно-правових відносин щодо персональних даних. При цьому поняття «фізична особа» охоплює: громадян України, іноземців, осіб без громадянства, що перебувають в Україні на законних підставах. Наприклад, це зазначено у Законі України «Про правовий статус іноземців та осіб без громадянства» від 22 вересня 2011 року № 3773-VI [89] та у ст. 10 Закону України «Про біженців та осіб, які потребують додаткового або тимчасового захисту» від 8 липня 2011 року. № 3671-VI [90].

Відповідно ми можемо наголосити, що суб'єкт персональних даних – це конкретна фізична особа, персональні дані якої обробляються, а саме: підлягають збиранню, зміні, зберіганню та захисту з метою ідентифікації цієї особи, у тому числі з використанням інформаційних технологій та штучного інтелекту.

Законодавством визначені права суб'єктів правовідносин щодо обробки персональних даних. При цьому варто зазначити, що в окремих випадках така обробка здійснюється виключно за згодою суб'єкта персональних даних-фізичної особи.

Чинне законодавство виділяє певні окремі категорії громадян, які є окремими підгрупами суб'єктів персональних даних у залежності від їх правового становища, яке визначається сферою суспільних відносин публічного управління (адміністрування), де здійснюється обробка персональних даних. Важливим при цьому є характер змісту інформації, яка становить їх персональні дані та сфера їх застосування, пов'язана із публічним управлінням (адмініструванням), забезпеченням прав (виборчих прав, права на освіту) громадян, наданням публічних послуг тощо. Так, сьогодні на законодавчому рівні визначено такі підгрупи суб'єктів персональних даних:

- «здобувачі освіти, як суб'єкти персональних даних», персональні дані яких вносяться до ЄДЕБО [91];

- «пацієнти», персональні дані яких підлягають внесенню до електронної системи охорони здоров'я (Закон України «Про державні фінансові гарантії медичного обслуговування населення» [25];

- «працівники та службовці» (ч. 2 ст. 24 Кодексу законів про працю України [32] та Закон України «Про забезпечення хімічної безпеки та управління хімічною продукцією» від 1 грудня 2022 року № 2804-IX) [92];

- «фізична особа-підприємець», відомості про яку вносяться до Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань [93];

- «фізична особа-платник податків», відомості про яку вносяться до Державного реєстру фізичних осіб-платників податків, який формує та веде Міністерство фінансів України [94];

- «публічна особа, як суб'єкта персональних даних (ч. 6 ст. 6 Закону України «Про доступ до публічної інформації») [95];

- «фізична особа-суб'єкт кредитної історії» [61] (Закон України «Про організацію формування та обігу кредитних історій», а також Закону України «Про захист персональних даних») [23].

- «суб'єкт звернення за отриманням адміністративних послуг» [27], де збір і обробка персональних даних про таку особу підпадає під захист відповідно до Закону України «Про адміністративні послуги» [27].

- «громадяни України, які мають право голосу відповідно до ст. 70 Конституції України (виборці)» відомості про яку вносяться до Державного реєстру виборців відповідно до Закону Україні про «Державний реєстр виборців» [96].

Виходячи з такого підходу законодавця щодо нормативного визначення видів/підгруп суб'єктів персональних даних, можна запропонувати критерії для класифікації суб'єктів персональних даних.

На нашу думку, суб'єктів персональних даних можна класифікувати за рівнем законодавчого регулювання. Зокрема, суб'єкти, що підпадають під дію загального законодавства в сфері персональних даних, тобто безпосередньо Закону Україні «Про захист персональних даних». До цієї групи ми можемо віднести всіх суб'єктів персональних даних, тобто всіх фізичних осіб. Регулювання на рівні спеціального законодавства, яке на основі загального

закону у сфері захисту персональних даних забезпечує захист персональних даних підгруп суб'єктів. Ключовою ознакою для виокремлення зазначених підгруп суб'єктів персональних даних є збір та обробка додаткової інформації про таку особу. Зокрема, як приклад, збір даних про особу в медичній сфері, що передбачає отримання персональних даних про стан здоров'я суб'єкта, що передбачається окремим Законом України «Про державні фінансові гарантії медичного обслуговування населення».

Також, суб'єктів персональних даних можна класифікувати за критерієм сфери суспільних відносин: медична сфера (фізичні особи: пацієнти, медичний персонал); фінансова сфера (фізичні особи: клієнти банків та інших фінансових установ); освітня сфера (фізичні особи: кандидати на вступ, здобувачі освіти, викладачі, адміністративні працівники освітніх установ); сфера надання публічних послуг (фізичні особи: громадяни, що звертаються за отриманням публічних послуг, державні службовці); сфера реалізації виборчих прав (фізичні особи- виборці) та інші. Питання збору, обробки та захисту персональних даних зазначених підгруп суб'єктів персональних даних здійснюється на основі загального закону про захист персональних даних, а також законодавчими актами, які регулюють суспільні відносини у зазначених сферах, в тому числі і питання захисту персональних даних громадян.

Також, поділ суб'єктів персональних даних варто здійснювати, виходячи з загальної класифікації фізичних осіб, тобто поділ на громадян та не громадян (іноземці, особи без громадянства та інші). Виходячи з аналізу нормативного регулювання захисту прав персональних даних можна зробити висновок, що в більшості випадків зазначене регулювання стосується такого суб'єкта правовідносин у сфері захисту персональних даних, як громадянин. В той же час, суб'єктами персональних даних також виступають і особи, які не є громадянами України, щодо яких у визначених законом випадках також може здійснюватись збір та обробка додаткових персональних даних.

Перелік спеціальних категорій, підгруп суб'єктів персональних даних відповідно до діючого національного законодавства не є вичерпним та з часом

може бути розширений та конкретизований. Наразі можна припустити появу з часом нових категорій суб'єктів персональних даних, що безпосередньо пов'язано з розвитком суспільних відносин у різних сферах та необхідністю забезпечення прав громадян, зокрема у сфері захисту персональних даних. Також, на розширення підгруп суб'єктів персональних даних безпосередньо впливає розвиток інформаційних технологій, особливо швидкий та фактично неконтрольований розвиток останнім часом штучного інтелекту.

Проведений аналіз різних видів/підгруп суб'єктів персональних даних дозволяє прийти до таких висновків. По-перше, правовий режим персональних даних (їх відкритість, або віднесення до інформації з обмеженим доступом, до конференційної інформації), а також порядок здійснення може відрізнятися в залежності від сфери суспільних відносин та статусу суб'єктів персональних даних у випадках, передбачених законом. По-друге, який би статус не набув суб'єкт персональних даних, правовий режим його даних, зміст його прав та здійснення їх захисту в частині, яка не врегульована спеціальним законодавством, повинні відповідати загальним положенням Закону України «Про захист персональних даних». При цьому, якщо загальні гарантії щодо персональних даних сформульовано у Законі України «Про захист персональних даних», то зміст інформації, яка має бути віднесена до особистих даних відповідних суб'єктів та характер її збирання, обігу та захисту має міститися у відповідному спеціальному законі, який регулюватиме питання захисту персональних даних видів/підгруп суб'єктів персональних даних у різних сферах суспільних відносин.

**Висновки до розділу 1.**

1. Проведений аналіз генези теоретико-правових аспектів права на захист персональних даних дозволяє нам виділити чотири етапи розвитку та становлення нормативно-правового забезпечення захисту персональних даних в Європі та Україні:

Перший етап пов'язаний з теоретичним розвитком та закріпленням на нормативному рівні правової концепції «privacy» (або «право на приватність»), починаючи з кінця XIX століття і до середини XX в нормативних актах окремих європейських країн. Встановлено, що в період на території сучасної України відбувається виключно теоретичне формування забезпечення особистих прав людини, які на той час не були відображені в правових нормах.

Другий етап, припадає на період з другої половини і до кінця XX століття, коли з концепції «privacy» (або «право на приватність») окремо виділяється на теоретичному рівні сфера правового захисту персональних даних та здійснюється їх нормативно-правове закріплення. В цей час на території України на рівні радянської конституції було визначено особисті права громадянина, хоча це носило виключно декларативний характер і на законодавчому рівні не було правових механізмів їх реалізації.

Третій етап розпочинається з початку XXI століття і триває до 2023 року. Цей етап характеризується створенням загальних стандартів ЄС у сфері захисту персональних даних та закріплення їх на законодавчому рівні ЄС, імплементацією цих стандартів у національне законодавство країн-членів ЄС. В свою чергу, після відновлення незалежності в Україні розпочався розвиток законодавства у сфері захисту персональних даних у відповідності до європейських стандартів, що безпосередньо пов'язано з євроінтеграційним курсом України.

Четвертий, новітній етап, розпочинається з 2024 року і безпосередньо пов'язаний з розвитком інформаційних технологій штучного інтелекту, що вимагає створення нормативно-правової бази його використання та захисту персональних даних. Він характеризується прийняттям перших законодавчих

актів на національному рівні та на рівні ЄС щодо використання штучного інтелекту при обробці персональних даних.

2. Розгляд теоретичних підходів щодо розуміння поняття персональних даних дозволяє зробити наступне визначення: «персональні дані громадян – це будь-які відомості або дані, в об’єктивізованій формі, що стосуються суб’єкта даних (фізичної особи), який підлягає ідентифікації.

При цьому фізична особа, що піддається ідентифікації, — це реальна фізична особа, яку можна визначити у прямий чи опосередкований спосіб, зокрема, за допомогою певних відомостей ідентифікуючого характеру, таких як ім'я, прізвище, по-батькові, ідентифікаційний номер, дані про народження, місцезнаходження, онлайновий ідентифікатор, або на один або кілька факторів (їх поєднання), які є специфічними та виняткова властивими для соціальної, генетичної, фізичної, фізіологічної, інтелектуальної, майнової, культурної ідентичності цієї особи.

Персональним даним громадян притаманні наступні ознаки: інформаційний зміст персональних даних, які визначаються нами як відомості або дані про конкретну фізичну особу; ідентифікуючі властивості – вони дозволяють визначити (ідентифікувати) конкретну фізичну особу; визначена форма фіксації у певному джерелі (носії) персональних даних; не вичерпність; правова форма персональних даних, яка розпочинається із початком сукупності дій пов’язаних із їх обробкою та забезпеченням захисту.

Враховуючи визначення персональних даних з позиції адміністративно-правового регулювання та міжнародно-правового регламентування, ми можемо запропонувати наступний підхід щодо виділення їх видів. Так, пропонуємо розділити персональні дані громадян на такі групи, використовуючи критерії їх змісту та рівня визначеної можливості доступу до них: на загальні дані про особу, спеціальні дані про особу, а також біометричні дані про особу. При цьому видами біометричних персональних даних громадян виступають генетичні дані про них та відомості, що стосуються їх здоров'я або отриманої медичної допомоги.

3. Встановлено, що суб'єкт персональних даних – це конкретна фізична особа, персональні дані якої обробляються, а саме підлягають збиранню, зміні, зберіганню та захисту з метою ідентифікації цієї особи, у тому числі з використанням інформаційних технологій та штучного інтелекту.

Суб'єктів персональних даних можна класифікувати за наступними критеріями: за рівнем законодавчого регулювання, як такі, що підпадають під дію загального законодавства в сфері персональних даних, тобто безпосередньо Закону Україні «Про захист персональних даних». До цієї групи ми можемо віднести всіх суб'єктів персональних даних, тобто, всіх фізичних осіб. Регулювання зазначених відносин відбувається на рівні спеціального законодавства, яке на основі загального закону у сфері захисту персональних даних забезпечує захист персональних даних підгруп суб'єктів. Ключовою ознакою для виокремлення зазначених підгруп суб'єктів персональних даних є збір та обробка додаткової інформації про таку особу. Зокрема, як приклад, збір даних про особу в медичній сфері, що передбачає отримання персональних даних про стан здоров'я суб'єкта, що передбачається окремим Законом України «Про державні фінансові гарантії медичного обслуговування населення».

Також суб'єктів персональних даних можна класифікувати за критерієм сфери суспільних відносин: медична сфера (фізичні особи: пацієнти, медичний персонал), фінансова сфера (фізичні особи: клієнти банків та інших фінансових установ), освітня сфера ( фізичні особи: кандидати на вступ, здобувачі освіти, викладачі, адміністративні працівники освітніх установ), сфера надання публічних послуг (фізичні особи: громадяни, що звертаються за отриманням публічних послуг, державні службовці), сфера реалізації виборчих прав (фізичні особи-виборці) та інші. Питання збору, обробки та захисту персональних даних зазначених підгруп суб'єктів персональних даних здійснюється на основі загального закону про захист персональних даних, а також законодавчими актами, які регулюють суспільні відносини у зазначених сферах, в тому числі і питання захисту персональних даних громадян.

Поділ суб’єктів персональних даних варто здійснювати, виходячи з загальної класифікації фізичних осіб, тобто, поділ на громадян, не громадяни (іноземці, особи без громадянства та інші). Виходячи з аналізу нормативного регулювання захисту прав персональних даних можна зробити висновок, що в більшості випадків воно стосується такого суб’єкта правовідносин у сфері захисту персональних даних, як громадянин. В той же час, суб’єктами персональних даних також виступають і особи, які не є громадянами України, щодо яких у визначених законом випадках також може здійснюватись збір та обробка додаткових персональних даних.

Перелік спеціальних категорій, підгруп суб’єктів персональних даних відповідно до діючого національного законодавства не є вичерпним та з часом може бути розширений та конкретизований. Наразі можна припустити появу з часом нових категорій суб’єктів персональних даних, що безпосередньо пов’язано з розвитком суспільних відносин у різних сферах та необхідністю забезпечення прав громадян, зокрема у сфері захисту персональних даних. На подальше розширення підгруп суб’єктів персональних даних безпосередньо впливає розвиток інформаційних технологій, особливо швидкий та фактично неконтрольований розвиток останнім часом штучного інтелекту.

# РОЗДІЛ 2. МЕХАНІЗМ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН

## 2.1 Поняття та зміст адміністративно-правового забезпечення захисту персональних даних громадян

Дослідження поняття та сутності адміністративно-правового забезпечення персональних даних громадян вимагає розгляду таких правових категорій як «правове забезпечення» та «правове регулювання», які займають важливе місце у сучасній юридичній науці. Нині в юридичній науці існують різні підходи до розуміння та розмежування зазначених категорій.

Так, К.В. Барсуков розглядає правове забезпечення, як діяльність уповноважених державою органів щодо здійснення своїх функцій та одночасно, як результат цієї діяльності, що виражається у фактичній реалізації правових приписів, прав і свобод громадян [97, с. 12].

На думку М. В. Плескач між правовим забезпеченням та правовим регулюванням є відмінності, які виражаються у змісті, обсязі та структурних елементах [98], пов’язаних із впливом на суспільні відносини, а саме із їх правовим регулюванням, а також реалізацією норм права, які регулюють ці відносини практичній діяльності суб’єктів публічної влади.

Як зазначає, О. П. Сидоренко правове регулювання впливає на суспільні відносини за допомогою права та інших юридичних засобів. Водночас, правове забезпечення складається з різноманітних компонентів (таких як суб'єкти, цілі, результати, дії, операції, засоби і способи), які взаємодіють та взаємопов'язані через різноманітні відносини, що мають структурний, вертикальний, горизонтальний, координаційний, субординаційний, просторовий, часовий та інший характер [99, с. 43]. На його думку, у широкому розумінні, правове забезпечення відображає одну з основних функцій правової держави – збереження правопорядку. Воно також включає в себе систему заходів, таких

як юридичні, організаційні, ідеологічні тощо, спрямованих на вплив на суспільні відносини з метою їх регулювання [99, с. 41].

Відповідно, за обсягом та за змістом, «правове регулювання» та «правове забезпечення» істотно відрізняються. На наш погляд, правове регулювання є елементом правового забезпечення і повинно передувати правовому забезпеченню у певній сфері суспільних відносин, певного суспільного явища або функції держави. За своєю суспільною природою саме правове забезпечення створює нормативну базу, тобто, систему законодавства, яке регулює відповідну сферу суспільних відносин та формує для органів влади визначення законом їх функцій і завдання – компетенцію.

Правове забезпечення, в свою чергу, є втіленням публічно-правої управлінської діяльності органів влади, пов’язаної з процесом реалізації нормативно-правових приписів у конкретні дії суб'єктів публічної влади для задоволення публічних та приватних інтересів учасників адміністративних правовідносин.

Суб’єктами правового забезпечення виступають учасники правовідносин, а саме органи влади та їх посадові особи, що діють у відповідності з встановленою законодавством та локальними нормативними актами компетенцією, з метою реалізації свої повноважень.

Цілями правового забезпечення виступає задоволення прав, свобод та правових інтересів фізичних та юридичних осіб, територіальних громад та інших учасників правовідносин. Результатом правового забезпечення у кінцевому рахунку є такий стан правовідносин, за якого суб’єкти досягають бажаних для них цілей у правовий спосіб та, за необхідності, можуть отримати підтримку органів влади та їх посадових осіб для забезпечення свої прав. Це безпосередньо стосується суб’єктів публічної влади, основним завданням яких є адміністративно-правове забезпечення публічного інтересу за допомогою адміністративно-правових приписів.

Наразі поняття «адміністративно-правове забезпечення» є однією з важливих категорій науки адміністративного права. Зазначена тематика досить

часто привертає до себе увагу науковців та стає предметом ряду наукових досліджень, присвячених проблематиці адміністративно-правового забезпечення різних правових явищ, суспільних процесів, публічного управління у різних сферах. Варто відзначити, що за період 2007–2022 років лише у галузі адміністративного права було розміщено у репозиторії НБУ імені В. Вернадського більше 420 дисертаційних робіт та інших наукових публікацій, присвячених різноманітним питанням адміністративно-правового забезпечення діяльності органів влади, реалізації прав та свобод, окремих адміністративно-правових режимів.

Аналіз зазначених наукових досліджень свідчить про те, що існують різні наукові підходи та погляди щодо розуміння категорії адміністративно-правове забезпечення, її структури, сутності та змісту. Тому з'ясування сутності «адміністративно-правового забезпечення захисту персональних даних» та його елементів залишається актуальним для нашої наукової роботи.

Серед останніх досліджень присвячених проблематиці адміністративно-правового забезпечення різних сфер суспільної діяльності можна виділити праці О.М. Гуміна [100] , О.О. Терзі [101], Г. Ю. Лук'янової [102], А. В. Замриги [103], А. В. Кудіна [104], С. П. Гвоздика [105], В. Й. Пашинського [106] та інших науковців.

Підкреслимо, що досліджуючи адміністративно-правове забезпечення відносин у різних сферах суспільства, науковці по-різному розуміють цю категорію, її сутність та ознаки. Так, О.М. Дручек, аналізуючи поняття адміністративно-правового забезпечення прав, свобод та інтересів дитини органами Національної поліції України зазначає, що під таким забезпеченням розуміється діяльність держави, що включає в себе спеціальний механізм для упорядкування суспільних відносин, їх правове закріплення, захист, втілення та розвиток [107, с. 126–127].

На думку Д.О. Гомон, адміністративно-правове забезпечення охорони здоров'я – це вплив органів державної влади та місцевого самоврядування, їх посадових осіб, що здійснюється у межах визначеної законом компетенції, за

допомогою спеціального механізму, на відносини у сфері охорони здоров'я з метою забезпечення захисту та охорони прав, свобод та інтересів населення, необхідних для реалізації прав, пов'язаних із збереженням та підтриманням здоров'я, а також збільшенням тривалості життя населення [108, с.48–49].

Г.С. Римарчук визначає, що адміністративно-правове забезпечення права інтелектуальної власності – це здійснення державою за допомогою правових норм, приписів та різноманітних інструментів для упорядкування суспільних відносин, їх юридичного закріплення, захисту, втілення та розвитку [109, с. 8].

Так, Г.П. Циверенко розглядає адміністративно-правове забезпечення вираження народної волі як систему застосування різноманітних форм і методів, спрямованих на регулювання відносин у сфері вираження народної волі, які контролюються за допомогою адміністративного права [110, с. 4].

В свою чергу, В.І. Марчук під адміністративно-правовим забезпеченням встановленого порядку управління розуміється створення та підтримка необхідних умов для дотримання вимог установленого порядку управління за допомогою адміністративно-правових інструментів у сфері права [111], тобто шляхом реалізації суб’єктами публічного управління свої повноважень, визначених нормами адміністративного права.

В цьому контексті, Л. Чистоклетов та О. Хитра наголошують, адміністративно-правове забезпечення представляє собою основу впливу суб'єктів державно-владних повноважень на суспільні відносини у сфері публічного управління та їх діяльність. Ця діяльність спрямована на створення, використання та удосконалення відповідної основи з метою реалізації завдань адміністративного права. У свою чергу, варто зазначити, що механізм адміністративно-правового забезпечення є системою, утвореною через дії юридичних та фізичних осіб, які сприяють формуванню, функціонуванню та вдосконаленню цього забезпечення. Крім того, до цієї системи входять принципи, форми, методи адміністративно-правового регулювання та управлінські технології [112].

На думку М. В. Плескач, зважаючи на те, що предметом адміністративного права України є відносини, що виникають між органами публічної адміністрації та приватними особами, зміст предмету адміністративного права включає надання адміністративних послуг та здійснення виконавчо-розпорядчої діяльності, яка відноситься до публічного управління, здійснюваного адміністрацією [113, с. 20], з метою задоволення публічного інтересу.

Під адміністративно-правовим забезпеченням у найбільш широкому тлумаченні можна вважати систему заходів, які здійснюються з певною метою органами публічної адміністрації у процесі владної діяльності [114, с. 84].

Враховуючи зазначене, М. В. Плескач наголошує, що під адміністративно-правовим забезпеченням кібербезпеки людини можна вважати здійснювану органами публічної адміністрації та/або суб’єктами делегованих повноважень у процесі владної діяльності сукупність практичних заходів щодо забезпечення охорони та захисту життєво важливих прав, свобод та інтересів людини під час використання кіберпростору від ризиків та загроз, що охоплює юридичні, технічні, організаційні та освітні аспекти [98].

В той же час, Р.В. Ігонін, досліджуючи різні аспекти доктринального визначення поняття адміністративно-правового забезпечення, наголошує наступне. Якщо включити до поняття «адміністративно-правового забезпечення» діяльність суб'єктів державно-владних повноважень з реалізації норм адміністративного права, можна вважати, що це не є складовою адміністративно-правового регулювання, оскільки останнє є більш абстрактним поняттям порівняно з реалізаційною діяльністю відповідних суб'єктів. Правове регулювання цілком виправдано розглядати як спрямований вплив права на суспільні відносини з метою їх упорядкування. Однак реальний рівень упорядкування суспільних відносин, досягнутий через вплив норм права, може значно відрізнятися залежно від об'єктивних та суб'єктивних обставин. Основним показником такого стану є практика реалізації правових норм суб'єктами державно-владних повноважень. Для здійснення цієї

діяльності необхідно мати саме право, яке має бути реалізоване – в даному випадку, адміністративне право. Тому, в системі адміністративно-правового забезпечення, слід виділити два базові елементи – адміністративно-правові норми та правореалізаційну діяльність суб'єктів державновладних повноважень, які утворюють поняття адміністративно-правового забезпечення [115, с. 41].

На думку О. М. Гуміна, адміністративно-правове забезпечення можна розглядати у широкому і вузькому аспектах. У широкому розумінні, це означає упорядкування суспільних відносин, проведене уповноваженими державними органами, їх юридичне закріплення за допомогою правових норм, а також їх охорона, реалізація та розвиток. У вузькому розумінні, визначення адміністративно-правового забезпечення залежатиме від контексту конкретних суспільних відносин, про які йдеться [116], в тому числі, це може бути і питання адміністративно-правового забезпечення захисту персональних даних.

Поняття адміністративно-правового забезпечення включає кілька аспектів. По-перше, це аспект нормотворчої діяльності, який включає в себе розробку та прийняття правових норм, що регулюють різні аспекти життя суспільства і встановлюють права, обов'язки та відповідальність учасників правовідносин. По-друге, це правозастосовна діяльність, яка полягає в забезпеченні дотримання законності та правопорядку шляхом виконання приписів норм права і застосування санкцій у разі порушення встановлених вимог. По-третє, це аспект забезпечення стабільності правової системи та правопорядку, який здійснюється за допомогою механізмів забезпечення дотримання органами влади сформульованих гарантій прав, свобод та законних інтересів громадян [116].

Таким чином, адміністративно-правове забезпечення захисту персональних даних – це системна організаційно-розпорядча діяльність суб'єктів публічного управління, яка регламентується адміністративно-правовими нормами та спрямована на забезпечення захисту персональних

даних. Зазначена діяльність охоплює адміністративно-правове регулювання, реалізацію, охорону та захист суспільних відносин у сфері персональних даних.

Відтак, адміністративно-правове забезпечення передбачає утворення системи правових норм, які визначають обов'язки та повноваження державних установ та посадових осіб, процедури ухвалення адміністративних рішень, процедури оскарження таких рішень, а також встановлення відповідальності за порушення адміністративного права. Це все робиться з метою задоволення публічних інтересів та захисту прав особи.

Завдання адміністративно-правового забезпечення включають дотримання законності, підвищення ефективності функціонування державних органів (що передбачає встановлення правил і процедур для регулювання їх діяльності), захист прав, свобод та законних інтересів громадян. Забезпечення також включає забезпечення права на справедливий судовий захист, можливість оскарження рішень державних органів та захист від неправомірних дій або зловживань посадових осіб.

В цілому, адміністративно-правове забезпечення має за мету забезпечення рівних умов для всіх учасників адміністративних відносин, забезпечення прозорості, законності та відповідальності у діяльності державних органів, а також гарантування захисту прав громадян.

Наразі можем також говорити про існування різних наукових підходів до розуміння змісту та структури адміністративно-правового забезпечення як правової категорії. Так, на думку О.М. Гуміна, до основних елементів адміністративно-правового забезпечення необхідно віднести: 1) об’єкт; 2) суб’єкт; 3) норми права (норми адміністративного права); 4) адміністративно-правові відносини та їх зміст; 5) гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення [116].

В свою чергу, В. Й. Пашинський пропонує визначення адміністративно-правового забезпечення в контексті оборони держави як системної діяльності суб’єктів забезпечення оборони, заснованої на відповідних адміністративно-правових нормах. Основними учасниками цього процесу є суб’єкти публічного

управління, які ведуть адміністративно-правове регулювання, реалізують, охороняють та захищають суспільні відносини у сфері оборони. Ця діяльність спрямована на гарантування прав і законних інтересів усіх учасників правовідносин та створення необхідних умов для оборони держави у разі збройної агресії [106, с. 254].

У даному випадку об'єктом забезпечення будуть ті суспільні відносини або діяльність, які потребують державного втручання. Суб'єктом буде той державний орган або органи, які мають повноваження щодо регулювання, захисту або розвитку таких відносин. Перш за все, такий суб'єкт буде характеризуватися своєю структурою та адміністративно-правовим статусом. Норми адміністративного права контролюють суспільні відносини в сфері державного управління. Адміністративно-правові відносини – це правові зв'язки, які виникають, розвиваються та припиняються між суб'єктом та об'єктом під час застосування адміністративно-правових норм. Гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення будуть виступати як елементи, що фактично реалізовують політику держави стосовно різних суспільних відносин [116].

Подібних підходів щодо структури елементів адміністративно-правового забезпечення різних правових явищ та сфер публічного управління дотримуються більшість вчених, які досліджували зазначену проблематику. На їх думку структура адміністративно-правового забезпечення складається з таких елементів: 1) об'єкт; 2) суб'єкт; 3) норми права (норми адміністративного права); 4) адміністративно-правові відносини та їх зміст; 5) гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення [117]; [116, с.49]; [111, с. 9]; [118, с. 96–97]; [119, с.126]; [120].

Зазначене дає нам можливість запропонувати власне бачення змісту (структури) адміністративно-правового забезпечення як правової системи, яка включає об'єктно-суб'єктні елементи, зміст правовідносин адміністративно-правового забезпечення, норми адміністративного права як форми реалізації забезпечення захисту.

Розкриття загального поняття адміністративно-правового забезпечення та опис його структури дозволяють перейти до визначення поняття й змісту адміністративно-правового забезпечення у сфері захисту персональних даних громадян (це так зване «вузьке» або «предметне» визначення адміністративно-правового забезпечення), що залежить від характеру суспільних відносин, пов’язаних із захистом персональних даних громадян).

Захист персональних даних визначається як дії вповноваженого суб'єкта, а також діяльність юрисдикційних органів та осіб, які законом зобов'язані вжити належних заходів для відновлення порушеного або оспорюваного права. Цей захист є правовим інститутом, який включає систему заходів, спрямованих на забезпечення недоторканості права, його реалізацію та усунення наслідків порушення. Також захист персональних даних включає державний примус, спрямований на відновлення порушених прав та забезпечення виконання порушених обов'язків. Під формою захисту розуміється комплекс організаційних заходів, які взаємодіють між собою для захисту суб'єктивних прав та інтересів, які захищені законом [121, с. 350] громадян, які стосуються їх прав пов’язаних із персональними даними.

Поняття захисту персональних даних громадян органами публічної влади включає в себе прийняття відповідних правових та організаційних заходів для забезпечення безпеки та конфіденційності цих даних. Захист персональних даних органами публічної влади влади включає в себе наступні аспекти: збір та обробка даних лише з метою, передбаченою законом або в межах повноважень органу влади; використання відповідних заходів для запобігання несанкціонованому доступу до даних; забезпечення їх цілісності та точності; знищення даних після закінчення строку їх зберігання.

Захист персональних даних органами публічної влади ґрунтується на законодавстві та підзаконних нормативно-правових актах, які визначають права та обов'язки цих органів у відношенні до обробки особистих даних. Ці норми можуть включати вимоги щодо реєстрації даних, забезпечення конфіденційності, сповіщення особи про збір та використання її персональних

даних, а також встановлення відповідальності за порушення правил збереження персональних даних.

Подібних поглядів щодо адміністративно-правового забезпечення захисту персональних даних громадян дотримуються науковці, які досліджували зазначену проблематику. На думку, А. М. Мартинової адміністративно-правове забезпечення обігу та захисту біометричних персональних даних – це здійснення державою за допомогою правових норм, встановлених приписів і різноманітних засобів регулювання суспільних відносин, їх правове закріплення, захист, реалізація та просування [122, с.95].

Водночас, І. Б. Малаховська, досліджуючи питання адміністративно-правового забезпечення захисту персональних даних в діяльності Національної поліції, зазначає, що таке забезпечення включає законодавство, що регулює збір, зберігання, використання та захист персональних даних та систему заходів, які здійснюються уповноваженими суб’єктами для забезпечення конфіденційності та безпеки персональних даних, а також встановлення відповідальності за їх незаконне використання [123].

На думку П. С. Лютікова, основні засади забезпечення захисту персональних даних суб’єктами публічного управління включають проведення перевірок спеціально уповноваженим органом у сфері захисту персональних даних щодо дотримання власниками та обробниками персональних даних вимог законодавства щодо їх захисту, надання ним обов'язкових вимог (приписів) щодо запобігання або усунення порушень законодавства про захист персональних даних, а також встановлення адміністративної відповідальності для власників та обробників персональних даних за порушення законодавства щодо їх захисту [124].

Беручи до уваги наукові підходи щодо сучасного теоретичного розуміння загальної категорії «адміністративно-правове забезпечення», пропонуємо визначення поняття адміністративно-правового забезпечення захисту персональних даних громадян. З нашої точки зору, адміністративно-правове забезпечення захисту персональних даних громадян – це регламентована

адміністративно-правовими нормами системна діяльність суб’єктів забезпечення захисту персональних даних, насамперед діяльність суб’єктів публічного управління, щодо адміністративно-правового регулювання, реалізації, охорони та захисту суспільних відносин у сфері персональних даних, гарантування прав і законних інтересів всіх суб’єктів правовідносин, спрямованих на створення необхідних умов для додержання законодавства про захист персональних даних.

Відтак, структура адміністративно-правового забезпечення охоплює: 1) адміністративно-правові норми, які регламентують захист персональних даних громадян з боку органів публічної влади; 2) адміністративно-правові відносини у сфері персональних даних; 3) принципи дії механізму забезпечення захисту персональних даних громадян; 4) гарантії здійснення захисту персональних даних громадян; 5) акти застосування норм права у сфері захисту прав персональних даних [125, 687–688].

Характеризуючи структуру адміністративно-правового забезпечення захисту персональних даних, як окремої групи суспільних відносин, враховуючи її специфіку, розглянемо її елементи: 1) об’єкт адміністративно-правового забезпечення персональних даних – суспільні відносини в сфері обробки та захисту персональних даних; 2) суб’єкт адміністративно-правового забезпечення персональних даних – органи публічної влади, установи, підприємства, організації, в тому числі й приватні, які відповідають за розробку, впровадження та контроль дотримання нормативно-правових актів щодо захисту персональних даних громадян. Вони здійснюють регулюючу діяльність, спрямовану на забезпечення прав та свобод осіб у сфері обробки їхніх персональних даних, а також на забезпечення відповідності цих процесів вимогам законодавства та міжнародних стандартів; 3) норми адміністративного права щодо забезпечення захисту персональних даних – нормативно закріплені правила, процедури та відповідальність за обробку та захист персональних даних громадян. Ці норми регулюють діяльність органів пулічної влади та інших суб'єктів, що здійснюють обробку таких даних, зокрема встановлюють

умови збору, зберігання, використання та передачі персональних даних, а також встановлюють заходи захисту від несанкціонованого доступу, втрати, викривлення чи незаконного використання таких даних; 4) адміністративно-правові відносини в сфері забезпечення захисту персональних даних та їх зміст – це комплекс взаємодій між суб'єктами персональних даних та суб'єктами адміністративно-правового забезпечення захисту персональних даних, що здійснюють обробку персональних даних, та державними органами, які відповідають за забезпечення дотримання відповідних нормативно-правових актів. Зміст таких відносин полягає у реалізації заходів забезпечення прав та свобод громадян у сфері обробки їх персональних даних і включають такі аспекти: регулювання збору, зберігання, використання та передачі персональних даних відповідно до законодавства; встановлення процедур та вимог щодо захисту персональних даних від несанкціонованого доступу, втрати, викривлення чи незаконного використання; визначення відповідальності за порушення правил обробки персональних даних та невиконання вимог законодавства; забезпечення доступу до персональних даних у випадках, передбачених законом, та захисту конфіденційності таких даних; здійснення контролю та нагляду за дотриманням вимог щодо захисту персональних даних; 5) гарантії адміністративно-правового забезпечення захисту персональних даних включають: законодавчі гарантії, які встановлюють правові норми та стандарти, що регулюють збір, обробку, зберігання та передачу персональних даних, а також встановлення відповідальності за їх порушення; організаційні, які визначають систему організаційних та технічних заходів захисту персональних даних від несанкціонованого доступу, втрати, викривлення чи незаконного використання; контроль за забезпеченням захисту, який включає контроль за дотриманням вимог щодо захисту персональних даних включаючи оцінку ризиків та вдосконалення систем безпеки, а також можливість звернення за відновленням порушених прав.

Адміністративно-правове забезпечення захисту персональних даних громадян має місце у діяльності органів влади як елемент їх сервісної функції.

Адміністративно-правове забезпечення захисту персональних даних громадян – це врегульована адміністративними нормами системна діяльність суб'єктів публічної адміністрації щодо адміністративно-правового регулювання, реалізації, охорони та захисту суспільних відносин у сфері персональних даних.

Структуру адміністративно-правового забезпечення охоплюють адміністративно-правові норми, які регламентують захист персональних даних громадян з боку органів публічної влади; адміністративно-правові відносини у сфері персональних даних; принципи дії механізму забезпечення захисту персональних даних громадян; гарантії здійснення захисту персональних даних громадян; акти застосування норм права.

У підсумку підкреслимо, що сучасні теоретичні підходи до розуміння поняття та структури адміністративно-правового забезпечення захисту персональних даних безпосередньо впливають на розвиток законодавства, діяльність органів публічної влади в сфері забезпечення захисту персональних даних та потребують подальших наукових досліджень у зв'язку з швидким розвитком штучного інтелекту.

## 2.2 Система та повноваження суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян

Дослідження проблем адміністративно-правового забезпечення захисту персональних даних вимагає розгляду системи та повноважень суб'єктів публічної адміністрації, які безпосередньо здійснюють, у відповідності до національного законодавства, захист персональних даних.

Варто зазначити, що суб'єктами адміністративно-правового забезпечення захисту персональних даних будуть суб'єкти публічного управління (адміністрування), які є учасниками адміністративно-правових відносин. Як

зазначає Ю. П. Битяк, суб’єктом адміністративно-правових відносин є учасник, наділений певними правами та обов’язками, до яких входять: органи виконавчої влади, органи місцевого самоврядування, громадяни тощо [126, с. 57].

Ключовим суб’єктом адміністративно-правових відносин у сфері захисту персональних даних громадян є органи публічної адміністрації, які є частиною публічної влади. При цьому такі суб’єкти (публічна адміністрація) мають певну організаційну структуру, що включає органи виконавчої влади, органи місцевого самоврядування, їх посадових осіб та службовців, а також установи, організації та окремі недержавні структури, які, відповідно до законодавства, здійснюють управлінські функції для задоволення публічного інтересу, в тому числі щодо забезпечення захисту персональних даних. До основних суб’єктів органів публічного управління (публічної адміністрації) належать: органи виконавчої влади; суб’єкти місцевого самоврядування; суб’єкти делегованих повноважень [127].

Під суб’єктами публічної адміністрації розуміють суб’єкта владних повноважень, який здійснює публічне адміністрування: надає адміністративні послуги та з цією метою здійснює виконавчо-розпорядчу адміністративну діяльність. Ключовою ознакою суб’єкта публічного адміністрування є діяльнісний підхід – здійснення публічного адміністрування. Основою системи суб’єктів публічного управління (адміністрування) є – органи виконавчої влади та органи місцевого самоврядування [128, с. 74-75].

До найбільш суттєвих ознак суб’єктів публічної адміністрації можемо віднести такі: кожен з учасників є окремим елементом єдиної функціональної системи суб’єктів публічного адміністрування; їхні правові статуси визначаються відповідно до законів або підзаконних нормативно-правових актів; для виконання своїх обов'язків суб’єкти мають повноваження ухвалювати публічні владні рішення; їхні дії зорієнтовані на виконання законів та задоволення публічних інтересів, і всі суб’єкти публічного управління, в

першу чергу, спрямовані на це [128, с. 62], зокрема забезпечують публічний інтерес в сфері захисту персональних даних.

Для того щоб суб'єкти публічного управління (адміністрування) мали змогу здійснювати адміністративно-правове забезпечення захисту персональних даних, вони повинні бути наділені відповідними повноваженнями, під якими розуміють адміністративні обов'язки та права суб'єкта публічного адміністрування, надані їм законодавством [128, с. 85].

Таким чином, якщо розглядати поняття суб'єкт адміністративно-правового забезпечення через загальне визначення адміністративних відносин, то очевидним є те, що такий суб'єкт відноситься до сфери публічного адміністрування. Тобто, мають відповідний правовий статус, який визначається законодавством (посідає місце у державному механізмі, виконуючи окремі завдання) та надає адміністративні послуги чи виконавчо-розпорядчу адміністративну діяльність у сфері, окресленій його компетенцією.

На нашу думку, серед суб'єктів адміністративно-правового забезпечення захисту персональних даних ключову роль відіграють органи виконавчої влади. Система органів виконавчої влади функціонує на трьох рівнях: вищому, центральному та місцевому [128, с. 91]. Система органів виконавчої влади складається з Кабінету Міністрів України, який є вищим органом [129], а також з центральних органів виконавчої влади, до яких належать міністерства, державні служби, державні агентства, державі інспекції, центральні органи виконавчої влади зі спеціальним статусом [128, с. 94].

Такі центральні органи виконавчої влади як міністерства, відповідають за розробку та втілення державної політики у певних сферах, тоді як інші центральні органи виконавчої влади здійснюють конкретні функції, пов'язані з виконанням цієї політики [130], в тому числі в сфері забезпечення захисту персональних даних.

Як наголошує В.В. Галунько, інші центральні органи виконавчої влади забезпечують впровадження державної політики у конкретній галузі, крім того, вони надають адміністративні послуги, здійснюють державний нагляд

(контроль), керують об’єктами державної власності, узагальнюють практику застосування законодавства у своїй сфері відповідно до їх повноважень, передбачених законодавством [128, с. 96-97].

Також, до центральних органів виконавчої влади зі спеціальним статусом належать: Антимонопольний комітет України, Державний комітет телебачення й радіомовлення України, Фонд державного майна України, Національне агентство України з питань запобігання корупції, Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, Адміністрація Державної служби спеціального зв’язку та захисту інформації, Державне бюро розслідувань та інші [128, с. 97], які також здійснюють захист персональних даних при здійснені своїх повноважень.

Наголосимо, що до системи органів державної виконавчої влади на регіональному належать місцеві державні адміністрації, які здійснюють виконавчу владу в областях, районах, районах Автономної Республіки Крим, у містах Києві та Севастополі [131]. В умовах воєнного стану повноваження зазначених органів виконавчої влади, в тому числі, щодо забезпечення захисту персональних даних, можуть покладатись на військові адміністрації [132].

Акцентуємо увагу на тому, що суб’єктами є органи публічної влади, в тому числі органи виконавчої влади, публічного адміністрування, що виступають учасниками адміністративно-правових відносин в сфері захисту персональних даних та є суб’єктами забезпечення такого захисту [23].

Органу публічної адміністрації, як суб’єкту адміністративно-правового забезпечення захисту персональних даних громадян притаманні такі ознаки.

По-перше, кожен орган публічної адміністрації, наділений певним правовим статусом, виступає носієм відповідних державновладних повноважень, які мають обов’язково включати сферу забезпечення захисту персональних даних громадян.

По-друге, основним змістом діяльності органів публічної адміністрації є надання визначених адміністративних послуг і здійснення державного

управління, а відповідно такі органи виступають в ролі володільців, а іноді розпорядників персональних даних або третіх осіб.

По-третє, компетенція публічної адміністрації визначаються Конституцією та законами України, актами КМУ, іншими законодавчими актами та має включати регламентування використання та обробки персональних даних.

По-четверте, діяльність органів виконавчої влади має підзаконний, адміністративно-сервісний та виконавчо-розпорядчий характер, пов'язаний у тому числі, з здійсненням розробкою нових та застосуванням існуючих норм права у сфері захисту персональних даних, забезпечення дотримання законності та правопорядку учасниками правовідносин та застосування санкцій в разі порушення вимог законодавства; забезпечення гарантій прав, свобод та законних інтересів суб'єктів персональних даних та застосування комплексу юрисдикційних на неюрисдикційних заходів захисту визначених законодавством України, нормативно-правовими актами ЄС, міжнародними договорами, звичаями та судовою практикою у випадках порушення прав, свобод та законних інтересів суб'єктів персональних даних.

Важливо зауважити, що у процесі захисту прав, свобод і законних інтересів приватних осіб, а також забезпечення публічного інтересу держави та суспільства в цілому, вони мають право діяти у межах права, застосовуючи різноманітні юридичні та владні засоби, які можуть бути нормотворчого, виконавчого або правоохоронного характеру.

Отже, на основі поєднання широкого (вся система органів публічної влади, публічної адміністрації яка представлена у структурі публічного механізму) та спеціалізованого інституційного підходу (як ці органи публічної влади наділені повноваженнями щодо захисту персональних даних), визначимо систему та повноваження суб'єктів публічної адміністрації щодо адміністративно-правового забезпечення захисту персональних даних громадян.

Якщо розглядати систему суб'єктів публічної адміністрації як суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян, то стає очевидним, що ця система на даний час на законодавчому рівні потребує вдосконалення.

Мова йде про те, що єдиного органу у сфері захисту персональних даних громадян наразі не існує, хоча дискусія щодо його створення є активною [133]. Багато науковців висловлюють думку про потребу у створенні окремого незалежного органу, який би здійснював контроль за дотриманням прав на захист персональних даних та права на доступ до публічної інформації [134] з урахуванням європеських стандартів та досвіду у сфері забезпечення захисту персональних даних.

Діючу наразі систему суб'єктів публічної адміністрації щодо адміністративно-правового забезпечення захисту персональних даних представляють (крім згаданого у попередніх підрозділах досліджень Уповноваженого Верховної Ради України з прав людини) центральні та місцеві органи державної виконавчої влади, органи місцевого самоврядування та їх посадові особи.

Органи публічної адміністрації виступають в якості володільців, розпорядників персональних даних, третіх осіб. Володільцем чи/або операторами персональних даних (розпорядником) можуть бути також підприємства, установи та організації будь-якої форми власності, органи державної або місцевої влади, фізичні особи-підприємці, які обробляють персональні дані відповідно до законодавства. Однак, лише підприємства державної або комунальної форми власності можуть виступати як оператори персональних даних, якщо володільцем цих даних є державний або місцевий орган, окрім зазначених органів [23].

Таким чином, під суб'єктом адміністративно-правового забезпечення захисту персональних даних громадян необхідно розуміти орган публічної адміністрації, який здійснює публічне управління у сфері захисту персональних даних в процесі реалізації прав громадян та надання адміністративних послуг,

компетенція якого включає правове регулювання, збір, обробку, зберігання та забезпечення захисту персональних даних. Суб’єкт адміністративно-правового забезпечення захисту персональних даних громадян виступає в ролі володільців, а іноді – розпорядників персональних даних або третіх осіб.

Таким чином, основною ознакою суб’єкта адміністративно правового забезпечення захисту персональних даних, як учасника адміністративно-правових відносин, є наявність публічних владних повноважень. У цьому ж контексті М. В. Різак підкреслює, що для виникнення таких відносин обов'язковою умовою є участь однієї зі сторін, яка має юридичні та управлінські повноваження (обов'язкового суб'єкта), і яка діє в інтересах держави, спрямованих на захист основних прав та свобод особи і громадянина, зокрема права на приватне життя у зв'язку з обробкою персональних даних.

Отже, адміністративно-правові відносини у сфері обігу та обробки персональних даних розглядаються як наслідок впливу адміністративно-правових норм на поведінку суб'єктів обігу та обробки персональних даних, що призводить до виникнення між ними правових зв'язків [88].

З позицій публічного управління (як управлінської так і правоохоронної діяльності) інтереси та права суб’єктів персональних даних виступають об’єктом адміністративно-правового регулювання та забезпечення і знаходять своє відображення у компетенції уповноважених органів публічної влади у сфері забезпечення захисту персональних даних.

Відповідно до Закону України «Про захист персональних даних» можна визначити наступних суб’єктів персональних даних: володільця, розпорядника та третю особу у сфері цих правовідносин.

Водночас, варто зазначити, що органи публічної влади визначені виключно опосередковано через повноваження визначені в законі щодо обігу персональних даних громадян. Таким чином, крім категорії «суб’єкт персональних даних», Закон України «Про захист персональних даних» використовує категорію «суб'єкти відносин, пов'язаних із персональними даними» (ст. 4) [23]. Виходячи з цього, робимо висновок про те, що володільці,

розпорядники та треті особи можуть виступати у якості суб’єктів адміністративно-правових відносин і вони відносяться до групи суб’єктів – органи публічної влади.

Отже, до числа таких суб'єктів відносин, пов'язаних із персональними даними віднесено самого суб’єкта персональних даних – фізичну особу. Також, до суб’єктів відносин, пов'язаних із персональними даними, відносяться органи публічної влади, що виступають в якості володільця персональних даних (в міжнародних актах – контролер), розпорядника персональних даних, третя особа та Уповноваженого Верховної Ради України з прав людини [23], в межах своїх повноважень. Необхідно наголосити, що ці суб’єкти (володільці, розпорядники, треті особи, Уповноважений Верховної Ради України з прав людини) при обробці персональних даних безпосередньо несуть відповідальність за їх захист.

Зазначені норми національного законодавства в цілому відповідають європейським нормам щодо визначення суб’єктів захисту персональних даних. З позицій європейського законодавства органи публічної влади можуть виступати у ролі володільця (контролера), розпорядника (процесора), а в окремих випадках отримувача або третьої особи [20]. Процесор – це особа або організація, що обробляє персональні дані від імені та за дорученням контролера. Контролер – це особа або організація, яка самостійно або спільно з іншими визначає цілі та методи обробки персональних даних, відповідно до законодавства ЄС або національного законодавства держави-члена.

Згідно з регламентами ЄС, володільником персональних даних можуть бути різні суб'єкти, такі як підприємства, установи, організації усіх форм власності, органи державної влади, місцевого самоврядування, а також фізичні особи-підприємці, які законно обробляють такі дані. Якщо дані про одну особу обробляються різними суб'єктами на законних підставах, кожен з них є самостійним володільником цих даних. У випадку, коли кілька суб'єктів мають право на обробку однієї бази даних, вони вважаються співволодільцями. Проте, якщо кожен співволоділець може самостійно приймати рішення про обробку

окремої частини цієї бази даних, він вважається її володільцем у повному обсязі. Володілець має право обробляти персональні дані лише на законних підставах і тільки у межах, які відповідають законній меті обробки.

Третя особа (third party) – це фізична чи юридична особа, державний орган, установа чи орган, відмінний від суб'єкта даних, контролера та процесора, які уповноважені контролером або процесором під їх прямим керівництвом обробляти персональні дані, а «отримувач» – це фізична чи юридична особа, державний орган, установа чи інший орган, якому розкриваються персональні дані, незалежно від того, чи він є третьою особою чи ні. Однак органи державної влади, які можуть одержувати персональні дані в рамках окремого запиту відповідно до законодавства ЄС або держави-члена, не повинні розглядатися як одержувачі; обробка даних зазначеними державними органами повинна відповідати нормам, що застосовуються, про захист даних відповідно до цілей обробки [20].

Ознаками публічних органів влади, як суб'єктів відносин, пов'язаних із персональними даними, є здатність мати або реалізовувати повноваження у сфері державного управління, пов’язаного з обігом та захистом персональних даних громадян. До функціональних обов’язків органів публічної влади, як суб'єктів відносин, пов'язаних із персональними даними входить практичне забезпечення реалізації в життя наданих громадянам прав і свобод та покладених на них обов’язків щодо захисту персональних даних.

Варто зазначити, що у період з 6 квітня 2011 року до 10 вересня 2014 року у системі органів публічної влади існувала Державна служба України з питань захисту персональних даних, як центральний орган виконавчої влади з питань захисту персональних даних, діяльність якого спрямовувалася і координувалася КМУ через Міністра юстиції України. Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [135], який набув чинності 1 січня 2014 року, з метою забезпечення незалежного контролю з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у

зв'язку з автоматизованою обробкою персональних даних, повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини та суди [23].

Законодавство вимагає, аби володільці, розпорядники персональних даних та треті сторони забезпечували захист цих даних від можливих втрат, знищення чи незаконної обробки, включаючи незаконний доступ до них. Важливо відзначити, що у випадках, коли обробка персональних даних здійснюється державними або місцевими органами влади, які мають чітко визначені повноваження згідно з законом, обсяг і мета обробки вже уточнені в відповідних правових актах, що регулюють їхню діяльність. Крім того, зазвичай створюється відповідний структурний підрозділ або призначається відповідальна особа, яка організовує заходи з захисту персональних даних під час їх обробки.

Варто зазначити, що володільцями персональних даних можуть виступати, як публічні, до яких відносяться органи державної влади та органи місцевого самоврядування, та приватні володільці персональних даних, до яких відносяться підприємства, установи і організації усіх форм власності, фізичні особи-підприємці, які обробляють персональні дані на законних підставах. Тобто, роботодавці виступають такими щодо працівників та кандидатів на роботу; телекомунікаційні компанії – щодо контрактних абонентів; магазини та підприємства побутового обслуговування – виключно щодо клієнтів/власників дисконтних карток; заклади охорони здоров’я, виробники ліків – щодо пацієнтів, осіб які приймають участь у медико-клінічних випробовуваних; політичні партії, профспілки, релігійні, спортивні організації – щодо їх членів; банківські та страхові установи – щодо індивідуальних клієнтів, власних працівників та корпоративних клієнтів; органи влади – щодо відповідних категорій осіб, які звернулися щодо отримання публічних послуг, були внесені у певні бази даних, поступили на службу, вчинили протиправні дії.

Чинне законодавство визначає обов'язки органів публічної влади, їх посадових осіб щодо забезпечення захисту персональних даних громадян.

Так, наприклад, відповідно до Закону України «Про державну службу» кожен державний службовець зобов'язаний зберігати державну таємницю та персональні дані осіб, що стали йому відомі у зв'язку з виконанням посадових обов'язків, а також іншу інформацію, яка відповідно до закону не підлягає розголошенню (п. 12, ч. 1, ст. 8) [136].

Іншим прикладом регулювання досліджуваних відносин є Закон України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів», який передбачає обіг відомостей, необхідні для забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів. Володільцем Реєстру є Міністерство оборони України (далі – МОУ), розпорядниками Реєстру є Генеральний штаб Збройних Сил України, Служба безпеки України (далі – СБУ) та Служба зовнішньої розвідки України. Володілець Реєстру за погодженням з Державною службою спеціального зв'язку та захисту інформації України здійснює комплекс заходів для забезпечення технічного захисту персональних та інших даних Реєстру в процесі їх зберігання, обробки та передачі каналами телекомунікацій відповідно до законодавства України [137].

Закон України «Про поштовий зв'язок» прямо зазначає, що оператори поштового зв'язку виступають як розпорядники персональних даних [138]. Відомості, що містяться в єдиному державному реєстрі операторів поштового зв'язку, є відкритими та загальнодоступними і підлягають розкриттю з урахуванням Закону України «Про захист персональних даних» (ст. 14) [23].

Відповідно до Закону України «Про офіційну статистику», захист первинних даних, отриманих від респондентів під час проведення статистичних спостережень, у процесі їх оброблення з використанням телекомунікаційних мереж забезпечується відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закону України «Про захист персональних даних». Суб'єктами такого захисту виступають державні органи,

які проводять статистичні спостереження, та розпорядники адміністративних даних, у тому числі Національна рада з питань статистики [139].

Згідно з Законом України «Про державну реєстрацію геномної інформації людини», реєстрація геномної інформації здійснюється відповідно до вимог забезпечення охорони прав і свобод людини і громадянина, керуючись основними принципами, такими як верховенство права, гуманізм та конфіденційність, зокрема, захист персональних даних. Обробка геномної інформації включає різноманітні дії, такі як збирання, реєстрація, зберігання, використання та передача знеособлених персональних даних про особу, що стосуються генетичних характеристик. Державна реєстрація геномної інформації передбачає внесення в Електронний реєстр відомостей про генетичні ознаки людини та відповідних знеособлених персональних даних згідно з вимогами законодавства [140].

В контексті аналізу повноважень органів публічної влади, необхідно зазначити, що Закону України «Про хмарні послуги» відносить до числа суб’єктів правових відносин, пов'язаних із персональними даними (система державного управління і регулювання при наданні хмарних послуг) наступні органи влади: КМУ; регулятор комунікаційних послуг; центральний орган виконавчої влади, що формує та реалізує державну політику при наданні хмарних послуг; орган, уповноважений здійснювати контроль за додержанням законодавства про захист персональних даних; МОУ; Національний банк України; ЦВК. Захист персональних даних при використанні для їх обробки технології хмарних обчислень та наданні хмарних послуг та/або послуг центру обробки даних здійснюється відповідно до вимог Закону України «Про захист персональних даних» [141].

Розглянемо повноваження органів публічної влади, які є суб’єктами правових відносин, пов'язаних із персональними даними і відповідно до чинного законодавства виступають суб’єктами адміністративно-правового забезпечення захисту персональних даних. До основних суб’єктів

адміністративно-правового забезпечення захисту персональних даних громадян, в умовах російської збройної агресії, необхідно віднести МОУ.

МОУ є головним органом у системі центральних органів виконавчої влади, який забезпечує формування та реалізує державну політику з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва у мирний час та особливий період [142].

В контексті захисту персональних даних до повноважень МОУ належать повноваження щодо забезпечення захисту персональних даних особливих груп громадян, таких як: військовослужбовці, військовозобов'язані, резервісти, військовослужбовці, які перебувають в полоні, військовослужбовці, які пропали безвісти.

МОУ обробляються такі персональні дані: анкетні дані особи; інформацію щодо її народження; інформацію пов'язану з паспортом та обліком платника податків; інформацію про освіту, інформацію щодо стану здоров'я (в обсязі, необхідному для визначення придатності до військової служби та/або для реалізації трудових відносин), про фактичне місце проживання; номери телефонів. При цьому, МОУ, виступає володільцем персональних даних, а розпорядниками персональних даних є військові частини [143].

В цьому аспекті, як наголошує П.В. Діхтієвський, адміністративно-правове забезпечення захисту персональних даних під час воєнного стану повинно враховувати швидкі зміни суспільних відносин у цій сфері, а також потенційні та реальні загрози для системи захисту персональних даних громадян. Це забезпечення має ґрунтуватися на законодавстві України та служити конкретним і законним цілям, таким як захист прав і свобод людини, а також забезпечення національної безпеки і оборони країни [22].

Відтак, для забезпечення національної безпеки та оборони України в умовах російської військової агресії особливої актуальності набуває Закон України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів» [137] в контексті комплектування Збройних Сил України, проведення мобілізації для відбиття російської збройної агресії. Зазначимо, що

Єдиний державний реєстр призовників, військовозобов'язаних та резервістів – автоматизована інформаційно-телекомунікаційна система, призначена для збирання, зберігання, обробки та використання даних про призовників, військовозобов'язаних та резервістів, створена для забезпечення військового обліку громадян України [137].

До Реєстру заносяться та зберігаються персональні дані та службові дані про призовників, військовозобов'язаних та резервістів. При цьому згода призовників, військовозобов'язаних та резервістів на обробку зазначених даних не потрібна. У разі відсутності окремих відомостей до Реєстру вноситься відмітка про їх відсутність. Органам ведення Реєстру забороняється збирати, вносити до Реєстру та зберігати в базі даних Реєстру відомості, не передбачені у законодавстві. До персональних даних призовника, військовозобов'язаного та резервіста серед іншого відносяться реєстраційний номер облікової картки платника податків, унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності) та відцифрований образ обличчя особи (за наявності). Необхідно зазначити, що для формування Реєстру (ст. 13) використовуються дані реєстру виборців. Центральна виборча комісія одноразово подає володільцю Реєстру відомості, стосовно усіх громадян України віком від 18 до 60 років. Відомості про громадян України, які не є призовниками, військовозобов'язаними та резервістами, підлягають обов'язковому знищенню [137].

Також вважаємо, що для забезпечення захисту персональних даних військовослужбовців важливо розробити окремі інформаційні реєстри для цих категорій осіб з різним рівнем доступу. Нормування можливостей отримання інформації про суб'єктів, що внесені до цих баз даних, або, навпаки, відсутність інформації про певні особи, має бути також враховано. Це допоможе уникнути неконтрольованого розміщення в соціальних мережах численних сторінок із фотографіями та відео українських військових і військовополонених разом із їхніми персональними даними. Такий підхід дозволить уникнути порушень

прав військовослужбовців через несанкціонований доступ до їхніх особистих даних [144, с.52].

Серед суб'єктів адміністративно-правового забезпечення захисту персональних даних щодо громадян, які є ветеранами російсько-української війни, необхідно виділити Міністерство у справах ветеранів. Серед завдань Міністерства у справах ветеранів є створення та забезпечення формування і ведення Єдиного державного реєстру ветеранів війни, безпеки особистих даних, що зібрані відповідно до закону, включає захист інформації з обмеженим доступом, а також впровадження технічних заходів для захисту цієї інформації. Крім того, воно організовує та керує обміном даних між наявними державними реєстрами, інформаційно-аналітичними системами, а також між постачальниками пільг і послугами [145].

Міністерства у справах ветеранів України як володілець персональних даних, здійснює:

- ведення обліку осіб, які брали безпосередню участь в антитерористичній операції, забезпеченні її проведення чи у здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування російської збройної агресії;

- ведення обліку ветеранів війни, осіб, які мають особливі заслуги перед Батьківщиною, постраждалих учасників Революції Гідності, членів сімей таких осіб та членів сімей загиблих (померлих) ветеранів війни, членів сімей загиблих (померлих) Захисників і Захисниць України, реалізації ними пільг та інших соціальних гарантій, передбачених законодавчими актами, координації діяльності центральних та місцевих органів виконавчої влади та у випадках, передбачених законом, органів місцевого самоврядування з питань їх соціального захисту [146].

З метою забезпечення безпеки обробки особистих даних вживаються спеціальні технічні заходи захисту, включаючи заходи щодо унеможливлення несанкціонованого доступу до цих даних під час роботи технічного та програмного комплексу, через який здійснюється обробка. Операції, пов'язані

з обробкою особистих даних та доступом до них, реєструються Міністерством у справах ветеранів України відповідно до чинного законодавства. Під час обробки особистих даних необхідно гарантувати їхній захист від несанкціонованого та неконтрольованого доступу, модифікації, знищення, копіювання та поширення. Всі випадки порушень процесу обробки та захисту особистих даних документально фіксуються відповідальною особою [146].

Суб'єктом адміністративно-правового забезпечення захисту персональних даних громадян є Міністерство внутрішніх справ України (далі-МВС України), яке з метою обробки, зберігання, захисту персональних даних забезпечує належне функціонування єдиної інформаційної системи МВС України, формує та підтримує в актуальному стані інформаційні ресурси, що входять до єдиної інформаційної системи МВС України, здійснює обробку персональних даних у межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні та кваліфіковані електронні довірчі послуги, забезпечує здійснення повноважень з питань цифрового розвитку [147].

Водночас, сам текст Положення про Міністерство внутрішніх справ України не містить завдань, пов'язаних з обробкою та захистом персональних даних громадян. Також у системі МВС України діє Сервіс центральної підсистеми єдиної інформаційної системи МВС України «Єдине вікно для громадян» [148], який розроблено Державним підприємством «ІНФОТЕХ», реалізуючи свої повноваження адміністратора ЄІС МВС, відповідно до «Положення про єдину інформаційну систему Міністерства внутрішніх справ» [149]. Виходячи із зазначеного, Державним підприємством «ІНФОТЕХ» буде виступати розпорядником персональних даних, володільцем яких є саме МВС України, які забезпечують захист персональних даних.

Наголосимо, що розглядаючи МВС України, як суб'єкта адміністративно-правового забезпечення захисту персональних даних громадян ми говоримо про центральні органи виконавчої влади, діяльність яких спрямовується і координується КМУ через МВС України та забезпечує

реалізацію державної політики у різних сферах, а саме: Державна прикордонна служба України, яка є центральним органом виконавчої влади, і який реалізує державну політику у сфері захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні [150]; Національна гвардія України, яка є військовим формуванням з правоохоронними функціями, що забезпечує реалізацію правоохоронної функції держави, а також у випадку збройної агресії приймає участь у обороні держави [151]; Державну міграційну службу України, яка є центральним органом виконавчої влади, що забезпечує реалізацію державної міграційної політики [152] та інші. Для реалізації державної політики у відповідних сферах зазначені органи публічної влади володіють базами даних та забезпечують захист персональних даних.

Національна поліція України – це центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [153]. Службова діяльність Національної поліції безпосередньо пов'язана з використанням певних відомостей та обробкою персональних даних про осіб, що є невід'ємною складовою процесу накопичення та зберігання інформації в базах персональних даних, що належать до єдиної інформаційної системи МВС України [154].

У межах інформаційно-аналітичної діяльності поліція: формує бази (банки) даних, що належать до єдиної інформаційної системи МВС України; користується базами (банками) даних МВС України й інших органів державної влади; здійснює інформаційно-пошукову та інформаційноаналітичну роботу; забезпечує інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав і міжнародними організаціями [153].

Під час виконання своїх повноважень Національна поліція України здійснює збір та обробку особистих даних громадян, включаючи також дані, що відносяться до «чутливих» категорій. Це може включати надання необмеженого доступу до таких даних, їх розкриття широкому загалу, а також

збір інформації без належної законної підстави та обґрунтованої мети, або розкриття даних громадськості. Також може мати місце збір надмірного обсягу даних, які в подальшому обробляються для цілей, що потребують подальшого вивчення, про що свідчать дослідження багатьох українських авторів [123], [155], [156], [157].

Необхідно зазначити, що істотною проблемою залишається питання правового регулювання обробки відеозаписів з нагрудних камер поліцейських, які містять персональні дані, а також систем відеоспостереження (збір, доступ, формування баз, порядок та термін зберігання такої інформації), що також можуть містити персональні дані. Зокрема, поширення відеозаписів з камер, що з‘являються в мережі Інтернет, без дотримання вимог законодавства про захист персональних даних [158], що є порушенням права на приватність.

На думку О.А. Заярного для забезпечення правомірної обробки біометричних даних по всім напрямам і рівням діяльності Національної поліції, на нашу думку, необхідно затвердити окремими наказами міністра внутрішніх справ України «Порядок обробки біометричних даних в базах даних, володільцем яких виступає Національна поліція» та «Положення про базу (бази) біометричних даних, володільцем яких виступає Національна поліція» [159].

На наш погляд, такий підхід щодо забезпечення обробки персональних даних повинен бути застосований всіма суб’єктами щодо забезпечення обробки персональних даних та в діяльності інших уповноважених суб’єктів, шляхом видання відомчих актів.

В умовах воєнного стану особливої актуальності набуває питання збору та обробки МВС України інформації відносно осіб, що зникли безвісти. Такі особи становлять вразливу категорію громадян, що потребують додаткового захисту. Так, станом на кінець листопада 2022 року безвісти зниклими вважається понад 15 тисяч осіб [160], на травень 2023 року 23 тисячі осіб [161], а станом на квітень 2024 року у реєстрі зниклих безвісти 37 тисяч [162]

В реєстрі будуть зібрані та централізовані дані щодо осіб, які зникли безвісти, включаючи прізвище, ім'я, по батькові, місце та дату народження, сімейний стан, адресу проживання, місце та обставини зникнення, а також прикмети. Також реєстр буде містити інформацію про те, чи було прийняте рішення суду щодо визнання таких осіб безвісно відсутніми або оголошення їх померлими, а також інші дані, які сприятимуть їх пошуку. За допомогою витягу з реєстру люди матимуть змогу звернутися до Пенсійного фонду України для отримання пенсії для непрацездатних членів сім'ї, якщо основного годувальника втрачено [161]. Витяги з Єдиного реєстру надаватимуть представники Департаменту інформатизації МВС України.

Серед суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян необхідно виділити Міністерство охорони здоров'я України (далі – МОЗ України), яке здійснює ведення та визначення порядку функціонування інформаційно-аналітичних систем, інформаційних ресурсів, електронних реєстрів та баз даних, які створюються, впроваджуються та ведуться у сферах охорони здоров'я [163].

До зазначених вище електронних ресурсів доцільно віднести: створення та ведення загальнодержавного реєстру хворих, які потребують імплантації електрокардіостимуляторів; ведення реєстрів донорів крові та її компонентів, обміну даними між ними і порядок виключення донорів із зазначених реєстрів; реєстрації живонароджених і мертвонароджених; ведення реєстру хворих на туберкульоз; здійснення координацію Національної Служби Здоров'я України (далі – НСЗУ) та інших установ, підприємств, організацій, що здійснюють впровадження електронної системи охорони здоров'я та пов'язаних інформаційних систем, електронних реєстрів і баз даних у сфері охорони здоров'я [163].

Натомість, нормативно-правововое регулювання щодо захисту персональних даних громадян безпосередньо пов'язана з тим як побудована система публічного управління у сфері охорони здоров'я і на підзаконному

рівні регулюється постановою КМУ, яка визначає порядок функціонування електронної системи охорони здоров’я [164].

Електронна система охорони здоров'я (далі - ЕСОЗ) є системою, яка обробляє персональні дані пацієнтів з метою забезпечення їх прав і гарантій, в сфері охорони здоров’я, зокрема, на вибір лікаря, отримання безоплатних медичних послуг і лікарських засобів за програмою медичних гарантій тощо. Варто зазначити, що електронна система охорони здоров’я eHealth складається з двох елементів: державного центрального компоненту та зовнішнього приватного компонента.

Центральна база даних (далі – ЦБД) — це інформаційно-телекомунікаційна система, яка містить передбачені законодавством реєстри, програмні модулі, інформаційну систему НСЗУ, в частині, необхідній для реалізації державних фінансових гарантій та ін. Забезпечує можливість створення, перегляду, обміну інформацією та документами між реєстрами, державними електронними інформаційними ресурсами, електронними медичними інформаційними системами [165], з дотриманням вимог законодавства щодо захисту персональних даних.

Електронна медична інформаційна система (далі – МІС) – це інформаційно-телекомунікаційна система, яка дає змогу автоматизувати роботу суб’єктів господарювання у сфері охорони здоров’я, створювати, переглядати, обмінюватися інформацією в електронній формі, зокрема з центральною базою даних (у разі підключення) [165].

Згідно з твердженнями МОЗ України, медичні дані, що зберігаються в електронній системі охорони здоров’я, є більш захищеними у порівнянні з картками пацієнтів на паперових носіях у закладах охорони здоров’я. eHealth – одна з небагатьох систем в Україні, в якій реалізовані найсучасніші засоби захисту: використання користувачами кваліфікованих електронних підписів (КЕР), відокремлене зберігання медичних та персональних даних, алгоритми, що забезпечують цілісність даних [134].

В зазначені системі зберігаються записи про пацієнтів у реєстрі пацієнтів та усі медичні записи складають електронну медичну карту пацієнта, що містить такі персональні дані про особу: 1) унікальний номер запису в Єдиному державному демографічному реєстрі (у разі наявності); 2) реєстраційний номер облікової картки платника податків (за умови присвоєння такого номера); 3) прізвище, ім'я, по батькові; 4) дата та місце народження; 5) адреса фактичного місця проживання або перебування; 7) реквізити документа, що посвідчує особу; 8) номер телефону, адреса електронної пошти; 10) інформацію про довірену особу для повідомлення в разі настання екстреного випадку тощо. А також безпосередньо медичну інформацію: групу крові пацієнта, інформацію про візити до лікаря, госпіталізації, інформацію про електронні направлення та рецепти, огляди, процедури тощо [166].

Володільцем ЕСОЗ є держава у особі НСЗУ. Доступ до даних про пацієнта, що містяться в ЕСОЗ, має лікар, якого обрав пацієнт, а також інші лікарі за його направленням у межах, необхідних для надання медичних послуг такими лікарями. Персональні дані обробляються у формі, що допускає ідентифікацію пацієнта, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.

Необхідно наголосити, що персональні дані пацієнтів в ЕСОЗ захищені від несанкціонованого доступу, використання, розголошення і знищення. Для захисту персональних даних застосовуються такі заходи: фізичний захист серверів, на яких зберігаються персональні дані; використання криптографічних технологій; наявність системи контролю доступу; навчання співробітників ЕСОЗ правилам захисту персональних даних.

Пацієнти мають право доступу до своїх персональних даних, які обробляються в ЕСОЗ. Вони також мають право на внесення змін до своїх персональних даних, а також на їх видалення. Для отримання додаткової інформації про ЕСОЗ, а також для захисту своїх персональних даних, пацієнти можуть звернутися до Національної служби здоров'я України. Даний реєстр пацієнтів на кінець 2023 року налічує понад 35 млн записів, реєстр медичних

спеціалістів і працівників становить понад 310 тис. користувачів, які щоденно генерують понад 3 млн електронних медзаписів про пацієнтів. Загальна кількість цих записів — понад 2 млрд [167].

В той же час, на думку науковців, аналіз ситуації доводить відсутність цілісної системи нормативно-правового регулювання та необхідність нормативно-правового регулювання обробки, зберігання та захисту персональних даних у сфері охорони здоров'я на рівні єдиного законодавчого акту [168].

Зокрема, пропонується прийняття Закону України «Про функціонування електронної системи охорони здоров'я в Україні». Завданням цього документа має бути визначення суб'єктів здійснення інформаційної політики у цій сфері, повноваження окремих органів і недержавних організацій або суб'єктів господарської комерційної діяльності, які залучені до розроблення та функціонування електронної системи охорони здоров'я [168].

На нашу думку, функціонування електронної системи охорони здоров'я безпосередньо пов'язане з реалізацією права на охорону здоров'я, така система містить велику кількість персональних даних, в тому числі, що являються конфіденційною та особливо чутливою інформацією, саме тому розробка такого закону безпосередньо впливатимиме на забезпечення належного захисту таких персональних даних громадян, відповідно до чинного законодавства про захист персональних даних.

Важливим суб'єктом адміністративно-правового забезпечення захисту персональних даних громадян також є Міністерство юстиції України (далі-Мін'юст) [169], яке формує і займається веденням реєстрів і баз даних, забезпечує доступ арбітражних керуючих до державних баз даних і реєстрів, держателем яких є Мін'юст, зокрема електронних, що містять інформацію про боржників, їх майно та кошти; формування та ведення Єдиного державного реєстру осіб, щодо яких застосовано положення Закону України «Про очищення влади», надання інформації із зазначеного Реєстру та оприлюднення на власному веб-сайті відомостей з нього; забезпечує створення, ведення та

функціонування Державного реєстру актів цивільного стану громадян; Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань; забезпечує доступ державних та приватних виконавців до баз даних і реєстрів, зокрема електронних, що містять інформацію про боржників, їх майно та кошти; організовує облік та реєстрацію засуджених та осіб, узятих під варту [169].

Також суб'єктом адміністративно-правового забезпечення захисту персональних даних громадян є Міністерство фінансів України [170], яке здійснює на основі результатів аналізу персональних даних та інформації, що містить банківську таємницю, проводиться перевірка та моніторинг достовірності даних, наданих фізичними особами. Крім того, забезпечується обробка та захист цих даних під час верифікації та моніторингу державних виплат, а також під час перевірки достовірності інформації та документів, введених до електронної системи охорони здоров'я. Ця перевірка не включає в себе інформацію про стан здоров'я людини. Ці дані використовуються для оплати медичних послуг та лікарських засобів в рамках програми медичних гарантій [170].

Особливо важливим в сфері забезпечення захисту персональних даних є обробки персональних даних у базі персональних даних – Державному реєстрі фізичних осіб-платників податків (далі – ДРФО) [94], яка здійснюється Міністерством фінансів України. Під обробкою персональних даних фізичної особи-платника податків розуміється будь-яка дія або сукупність дій, здійснюваних в Інформаційній комунікаційній системі Державного реєстру фізичних осіб-платників податків (далі – ІКС ДРФО ), які пов'язані із збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, відновленням, використанням та поширенням, знеособленням, знищенням відомостей про фізичну особу [94].

Захист персональних даних в ІКС ДРФО здійснюється шляхом створення та забезпечення функціонування комплексної системи захисту інформації з підтвердженою відповідністю [94].

Суб'єктом адміністративно-правового забезпечення захисту персональних у сфері освіти є Міністерство освіти і науки України (далі – МОН України), яке забезпечує ведення та функціонування Єдиної державної електронної бази з питань освіти, інших державних електронних баз та реєстрів, інших інформаційних систем у сфері, що належить до його компетенції [171].

Наказом МОН України від 16.02.2021 № 204 «Про затвердження положень про реєстри Єдиної державної електронної бази з питань освіти» та з метою визначення порядку ведення реєстрів Єдиної державної електронної бази з питань освіти було затверджено: Положення про Реєстр документів про освіту Єдиної державної електронної бази з питань освіти; Положення про Реєстр суб'єктів освітньої діяльності Єдиної державної електронної бази з питань освіти; Положення про Реєстр сертифікатів зовнішнього незалежного оцінювання Єдиної державної електронної бази з питань освіти; Положення про Реєстр студентських (учнівських) квитків Єдиної державної електронної бази з питань освіти; Положення про Реєстр сертифікатів педагогічних працівників Єдиної державної електронної бази з питань освіти [172]. Слід підкреслити, що обмін інформацією між Реєстром та державними електронними інформаційними ресурсами здійснюється через систему електронної взаємодії, яка включає комплексну систему захисту інформації з підтвердженою відповідністю [172].

Інші органи центральної влади в межах свої компетенцій також здійснюють збір, зберігання, обробку та захист персональних даних громадян у відповідності до законодавства про захист персональних даних та спеціального законодавства, яке регулює діяльність того чи іншого органу.

В той же час, в системі суб'єктів адміністративно-правового забезпечення захисту персональних даних особливе місце буде займати Міністерство цифрової трансформації України (далі- Мінцифри) [173], яке безпосередньо координує діяльність всіх органів публічної влади щодо створення, ведення реєстрів та забезпечення захисту персональних даних громадян. Зокрема

міністерство здійснює заходи щодо створення та забезпечення функціонування: системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта»; системи електронної взаємодії органів виконавчої влади; інтегрованої системи електронної ідентифікації; єдиного державного веб-порталу відкритих даних; національного реєстру електронних інформаційних ресурсів; Єдиного державного вебпорталу електронних послуг; Національної веб-платформи центрів надання адміністративних послуг; онлайн-платформи взаємодії органів виконавчої влади з громадянами та інститутами громадянського суспільства; державної платформи стану розвитку широкосмугового доступу до Інтернету (broadband.gov.ua); державного веб-порталу правового режиму Дія Сіті (city.diia.gov.ua), реєстру Дія Сіті; єдиного державного веб-порталу цифрової освіти; Єдиного державного вебпорталу для збору пожертв на підтримку України «United24»; веб-порталу «Дія. Цифрова громада»; Єдиної інформаційної системи обліку Національної програми інформатизації.

Поряд з веденням зазначених вище реєстрів, Мінцифри наділено повноваженнями щодо розробки пропозицій, внесення змін до нормативно-правових актів з питань захисту персональних даних, охорони інтелектуальної власності та формуванні державної політики у сферах криптографічного та технічного захисту інформації, в тому числі, що є особливо важливим і кіберзахисту [173]. Тобто, забезпечення захисту та запобіганню зовнішніх кібератак (зовнішніх втручань).

На Мінцифри покладається обов’язок захисту персональних даних у відповідних інформаційних та інформаційно-телекомунікаційних системах [174]. Під час обробки персональних даних використовуються заходи, що гарантують їхню безпеку та недоступність для сторонніх осіб.

Інформаційні системи обладнані антивірусним захистом та механізмами безперебійного живлення, щоб запобігти непередбаченим ситуаціям. Під час обробки персональних даних важливо забезпечити захист від несанкціонованого доступу, зміни, втрати, копіювання та розповсюдження.

Будь-які порушення процесу обробки та захисту персональних даних фіксуються документально відповідальною особою [174].

До суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян належать також органи місцевого самоврядування, які здійснюють забезпечення захисту персональних даних громадян під час надання адміністративних послуг на місцевому рівні, з метою підвищення якості життя населення на території територіального утворення.

Як наголошує А. Малинка, організація роботи по захисту персональних даних в органах місцевого самоврядування ще до початку російського вторгнення в Україну мала низку проблем, організаційного, технічного та фінансового характеру. Виконавчим органам сільських, селищних та міських рад доводиться обробляти колосальні обсяги інформації, а це – бази персональних даних [175], які потребують захисту особливо в умовах воєнного стану. Сучасні проблеми, з якими стикаються органи місцевого самоврядування у сфері захисту персональних даних у воєнний час, пов'язані з:

- відсутністю чітких та дієвих механізмів всередині органів місцевого самоврядування, які б забезпечували належне зберігання та обробку персональних даних. До початку війни досить невелика кількість громад мали розроблені та запроваджені внутрішні розпорядчі документи (наприклад, політика приватності, положення про захист персональних даних тощо), які б забезпечували якісні та дієві процедури накопичення, зберігання та обробки персональних даних. Це, зі свого боку, призводило до безсистемності та низької ефективності зусиль органів місцевого самоврядування у захисті права на захист персональних даних;

- відсутністю або недостатньою підготовкою посадових осіб, відповідальних за зберігання персональних даних. Незважаючи на вказівку закону (частина 2 статті 24 Закону України «Про захист персональних даних») у переважної більшості органів місцевого самоврядування не призначена/не визначена посадова особа, відповідальна за захист персональних даних;

- відсутністю нормативного регламентування питання зберігання баз персональних даних;

- відсутність роботи з оцінки ризиків у сфері обробки персональних даних [175];

- неналежне матеріальне, технічне та фінансове забезпечення.

Важливим аспектом аналізу системи та повноваження суб'єктів публічної адміністрації щодо адміністративно-правового забезпечення захисту персональних даних громадян є визначення у цій системі підприємств, організацій, громадських об'єднань, творчих спілок чи саморегулівних організацій, їх об'єднань та асоціацій, які фактично виконують делеговані повноваження щодо захисту персональних даних.

Термін «делеговані публічно-владні повноваження» передбачає, що державні органи передають виконання певних функцій або завдань, які традиційно вважаються державними, іншим недержавним суб'єктам (наприклад, приватним компаніям, громадським організаціям або іншим неурядовим організаціям) [176].

У контексті системи суб'єктів адміністраивно-правового забезпечення захисту персональних даних громадян необхідно згадати суб'єктів, на яких покладено повноваження щодо здійснення контролю за забезпеченням захисту персональних даних. Так, Закон України «Про захист персональних даних», передбачає, що контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснює такі органи як Уповноважений Верховної Ради України з прав людини, який включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних) та суди.

Підкреслимо, що Уповноваженим Верховної Ради України з прав людини з метою виконання контрольних функцій щодо захисту персональних даних видано ряд підзаконних нормативних актів. Наказом «Про затвердження документів у сфері захисту персональних даних» затверджено: Типовий

порядок обробки персональних даних [177]; Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [178]; Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації [179].

Варто зазначити, що суди є особливими суб'єктами адміністративно-правового забезпечення захисту прав персональних даних, розглядаючи спори стосовно порушення прав персональних даних. Таким чином, у випадку порушення прав персональних даних відповідно до законодавства про захист персональних суб'єкт персональних даних може звернутись до Уповноваженого Верховної Ради з прав людини або до суду.

Отже, система суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян представлена центральними (міністерства, державні служби, державні центральні органи виконавчої влади зі спеціальним статусом) та місцевими державними органами виконавчої влади, органами місцевого самоврядування, їх посадовими особами, державними підприємствами, установами, громадськими організаціями та їх об'єднаннями (у випадку здійснення делегованих повноважень), складовою частиною правового статусу яких виступає сфера забезпечення захисту персональних даних громадян в процесі надання адміністративних послуг і здійснення публічного управління, що включає реалізацію повноважень щодо використання та обробки персональних даних громадян. Зазначені суб'єкти, з позицій захисту персональних даних, виступають у правовідносинах в ролі володільців, в окремих випадках – розпорядників персональних даних чи третіх осіб.

Наголосимо, що суб’єктів адміністративно-правового забезпечення захисту персональних даних за функціями щодо обробки персональних даних можна згрупувати наступним чином:

по-перше, володільці персональних даних – це фізичні або юридичні особи, які визначають мету обробки персональних даних, встановлюють склад цих даних та процедури їх обробки, до числа яких ч. 2 ст. 4 Закону України «Про захист персональних даних» відносить підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичних осіб-підприємців;

по-друге, розпорядники персональних даних – це фізичні або юридичні особи, яким володільцем персональних даних або законом надано право обробляти ці дані від його імені, до числа яких ч. 3 ст. 4 Закону України «Про захист персональних даних» відносить лише підприємство державної або комунальної форми власності, якщо володільцем яких є орган державної влади чи орган місцевого самоврядування;

по-третє, третя особа – будь-яка особа, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних, за винятком суб’єкта цих персональних даних та Уповноваженого Верховної Ради України з прав людини (у випадках виконання ним функцій з контролю захисту персональних даних), яка здійснює подальший обіг та обробку персональних даних у межах визначених договором передачі та згодою суб’єкта персональних даних або законом;

по-четверте, це Уповноважений Верховної Ради України з прав людини, як уповноважений державний орган з питань захисту персональних даних та органи правосуддя.

Таким чином, органи влади як суб’єкти у сфері адміністративно-правових відносин, пов'язаних із персональними даними виступають як володільці, розпорядники та треті особи. Водночас, у частині згаданих третіх осіб Закон України «Про захист персональних даних» не містить окремого положення про

те, що ними можуть виступати органи державної влади чи органи місцевого самоврядування, що необхідно вважати істотним упущенням.

Відповідно необхідно запропонувати доповнити положення ч. 2 ст. 4 Закон України «Про захист персональних даних» другим реченням наступного змісту. «…Третьою особою можуть бути органи державної влади чи органи місцевого самоврядування, державні підприємства, установи і організації та інші публічні юридичні особи». Підкреслимо, що до числа таких «інших публічних юридичних осіб необхідно відносити і військові частини, як суб'єкти публічно-правових відносин.

Узагальнимо, що з позицій адміністративно-правових відносин на даний момент загальною компетенцією щодо питання володіння, обробки та захисту персональними даними наділені всі без виключення органи публічної влади. В розрізі нормативно-правового регулювання у окремих законодавчих актах, які визначають компетенцію та повноваження цих органів присутні, як правило, бланкетні норми, які відсилають до визначених Законом України «Про захист персональних даних» загальних засад захисту та обробки персональних даних. Водночас, окремі з них, наділені спеціальною компетенцією (наприклад, розпорядники) щодо здійснення захисту персональних даних, що знаходить своє відображення у змісті відповідних повноважень цих органів.

Беручи до уваги позиції науковців та аналіз норм чинного законодавства усю сукупність суб'єктів адміністративно-правового забезпечення можна класифікувати за наступними критеріями.

По-перше, що є вкрай важливим в умовах збройної російської агресії, необхідно класифікувати суб'єктів забезпечення захисту персональних даних за сферою їх діяльності: на цивільні (Міністерство охорони здоров'я України, Міністерство освіти і науки України тощо) та мілітаризовані (МОУ щодо ведення реєстру військовозобов'язаних, призовників, резервістів тощо; МВС України щодо ведення реєстру у справах пропавших безвісти в особливих обставинах).

По-друге, суб'єктів забезпечення захисту персональних даних також можливо класифікувати за сферою повноважень на публічні (органи публічної влади: органи виконавчої влади, органи місцевого самоврядування) та приватні ( приватні юридичні особи та фізичні особи підприємці) суб'єкти забезпечення захисту персональних даних.

По-третє, суб'єкти забезпечення захисту персональних даних також можна класифікувати відповідно до виду персональних даних, яки вони забезпечують, тобто на суб'єкти забезпечення захисту загальних персональних даних (МОН України, Міністерство юстиції) та суб'єкти забезпечення захисту особливо чутливих та конфіденційних персональних даних (МОЗ України, МВС України, в частині реєстру пропавших безвісти, МОУ).

Варто наголосити, що проведений аналіз нормативно-правового регулювання повноважень суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян дозволяє стверджувати про наявність прогалин у чинному законодавстві та необхідності удосконалення як порядку їх здійснення у сфері забезпечення захисту персональних даних так і розширення змісту таких повноважень.

Окремі органи влади не мають власних положень про порядок обробки персональних даних у базі персональних даних, або такі положення носять загальний та неактуальний характер. Функція забезпечення захисту персональних даних описана у їх змісті досить загально. Не чітко виділено межі та можливості здійснення відомчого контролю та нагляду. Загальним є відсутність посилання на можливості органами публічної адміністрації здійснювати розгляд відповідно до закону звернень громадян, а також скарг на рішення, на дії або бездіяльність підконтрольних у межах визначених повноважень учасників відносин у сфері обробки персональних даних та порядку прийняття обов'язкових до виконання рішення.

Важливим залишається питання врегулювання проблеми обробки персональних даних після смерті суб'єкта персональних даних, використання технологій відстеження дій суб'єктів персональних даних у електронних

комунікаціях та сервісах, регламентування порядку розгляду вимог суб'єкта персональних даних, у тому числі щодо виправлення персональних даних громадянина, необхідності дотримання вимог право на забуття персональних даних, тобто на повне знищення володільцем його персональних даних без надмірної затримки**,** реалізації принципу мобільність персональних даних та захисту від автоматизованого прийняття рішення.

На нашу думку, потребують подальших наукових досліджень питання щодо виділення в системі суб'єктів публічної адміністрації адміністративно-правового забезпечення захисту персональних даних громадян спеціалізованого органу центральної виконавчої влади на який може бути покладено здійснення функцій загального контролю за дотриманням законодавства у сфері захисту персональних даних громадян.

## 2.3 Інструменти адміністративно-правового забезпечення захисту персональних даних громадян

Діяльність органів публічної адміністрації щодо адміністративно-правового забезпечення у тій чи іншій сфері суспільних відносин пов'язана з використанням певного правового інструментарію – інструментів публічного управління (публічного адміністрування). У цьому контексті С. Г. Стеценко та В. Ю. Стеценко підкреслюють, що останніми роками поняття «інструменти публічного адміністрування» прийшло на заміну традиційним відомим в адміністративному праві поняттям «форми та методи публічного управління», причому інструменти публічного управління більшою мірою асоціюються саме з формами публічного управління [180, с. 312].

Як зазначає К. Примаков у теорії адміністративного права, та в практичній правозастосовній діяльності, важливою є категорія «інструменти діяльності публічної адміністрації». Інструменти діяльності публічної адміністрації представляють собою конкретні адміністративно-правові дії, які виражають специфіку та характер роботи цих структур. Зазначені дії

реалізуються у визначених формах та відповідно до повноважень суб'єктів згідно з встановленою процедурою з метою вирішення завдань та функцій публічної адміністрації та забезпечення прав, свобод і інтересів осіб у сфері публічно-правових відносин [181]. В свою чергу, В.О. Резніченко, визначаючи інструменти публічного адміністрування, називає їх зовнішньою формою дій суб'єктів публічної адміністрації [182, с. 119].

Підкреслимо, що поняття «інструментів публічного управління (адміністрування)» широко використовується як категорія не тільки в адміністративному праві, а також у теорії державного управління. Так, на думку О.В. Михайловської, інструментарій у науці про державне управління та адміністрування є категорією, що охоплює сукупності методів, технік, засобів та механізмів, які використовуються для реалізації завдань та функцій у сфері державного управління. Публічне управління неодмінно має бути спрямоване на забезпечення прав та інтересів громадянського суспільства [183], суб'єктивних прав громадян у різних сферах суспільного життя.

Інструментарій як сукупність інструментів публічного управління мають ключове значення та включають в себе як традиційні форми управлінської діяльності, так і новітні технології та підходи, адаптовані до сучасних умов. Особливо це має значення для захисту персональних даних громадян в умовах швидкого розвитку інформаційних технологій і їх застосування органами публічної влади з метою задоволення прав громадян, надання публічних послуг не можливе без використання персональних даних.

До інструментів публічного управління, в першу чергу, можемо віднести різноманітні нормативно-правові акти, методики аналізу та прогнозування, системи моніторингу та контролю, методи прийняття рішень, інформаційно-комунікаційні технології та інші інструменти, що застосовуються у сфері публічного управління. Важливість інструментів публічного управління у сфері захисту персональних даних громадян полягає у тому, що саме вони дозволяють органам публічного управління ефективно здійснювати свої

повноваження із дотриманням вимог щодо захисту персональних даних та адаптуватися до швидко змінюваних суспільних відносин у зазначеній сфері.

На думку М.В. Жуков, до інструментів діяльності публічної адміністрації, зокрема, належать: прийняття нормативно-правових актів, видання адміністративних актів, укладання адміністративних договорів; адміністративні акти-дії; акти-плани [184].

Прибічники нинішньої концепції інструментів публічної адміністрації та концепції форм адміністративно-правового регулювання до інструментів (форм) відносять нормативні акти, адміністративні акти, адміністративні договори [128, с. 144]. Так, О. Правоторова вважає, що однією з ключових характеристик державної влади є методи та форми діяльності публічної адміністрації, які виступають інструментами у виконанні конкретних завдань у межах адміністративно-правового механізму. Первинним серед адміністративних інструментів є форми адміністративної діяльності публічної адміністрації [185, с. 124], групи адміністративних дій суб'єктів публічної адміністрації [128, с. 144].

Водночас, ті науковці, що продовжують надавати перевагу визначенню поняття «форма адміністративно-правового регулювання», вказують, що це може бути вираженням волевиявлення суб'єктів публічної адміністрації або зовнішньо вираженою дією. Таким чином, вчені-адміністративісти використовують різні терміни, але надають їм схоже значення [184].

Окрім цього, О. Сукманова визначає «форми публічного адміністрування» як засоби, методи та прийоми, які виражено зовні та такі, які використовуються суб'єктами публічної адміністрації для регулювання правовідносин у конкретній сфері. Вони є складовою частиною механізму публічного адміністрування та використовуються відповідно до повноважень, наданих суб'єктам публічної адміністрації [186, с. 331].

С. Г. Стеценко та В. Ю. Стеценко пропонують розуміти під інструментами публічного управління зовнішні прояви конкретних дій суб'єктів публічного адміністрування, в рамках яких реалізуються їх

повноваження і за допомогою яких здійснюється регулюючий вплив на об’єкти публічного адміністрування [180, с. 312].

На думку інших вчених, інструмент публічного адміністрування виявляється у зовнішньому прояві однорідних за характером та правовою природою груп адміністративних дій, які здійснюються суб'єктами публічної адміністрації в межах чітко визначеної законом компетенції з метою досягнення певного результату в адмініструванні [128, с. 144] у сфері забезпечення захисту персональних даних громадян.

Інструментам адміністративно-правового забезпечення персональних даних властиві такі ознаки: вони є зовнішнім виразом форми адміністративної діяльності публічної адміністрації наділених повноваженнями у сфері захисту персональних даних; відображають правову динаміку публічного адміністрування у сфері захисту персональних даних; залежать від змісту компетенцій у сфері захисту персональних даних суб’єктів публічної адміністрації; зумовлені реалізацією адміністративних обов’язків суб’єктів публічної адміністрації у сфері забезпечення захисту персональних даних; їх вибір зумовлюється специфікою поставленої мети щодо певного об’єкта (відносини у сфері забезпечення захисту персональних даних) публічного впливу, що встановлює найбільш ефективний варіант діяльності [128, с. 143–144].

За визначенням К. Примакова інструменти діяльності публічної адміністрації виявляються як зовнішні вирази однорідних за своїм характером та змістом груп адміністративно-правових дій публічного управління, що здійснюються у визначених у законодавстві формах, в межах повноважень відповідних суб’єктів, за встановленою процедурою з метою виконання завдань та функцій публічної адміністрації, а також забезпечення прав, свобод та інтересів осіб у сфері публічно-правових відносин [181]. Інструменти діяльності публічної адміністрації у сфері захисту персональних даних громадян за їх юридичною природою зумовлюються повноваженнями суб’єктів публічної адміністрації, а їх реалізація відбувається за встановленими

адміністративними процедурами, зокрема, пов'язаними із застосуванням сучасних інформаційних технологій, технічних засобів та вимог щодо їх використання.

Таким чином, під інструментами публічного управління необхідно розуміти врегульовані нормами адміністративного права зовнішні прояви застосування правових засобів управлінської діяльності у діях суб'єктів публічного адміністрування, за допомогою яких відбувається регулюючий вплив на об'єкти публічного управління, що призводить до настання правових наслідків.

В той же час, основними інструментами діяльності публічної адміністрації, в тому числі в сфері захисту персональних даних, є нормативні акти публічної адміністрації, адміністративні акти, адміністративні договори [187, с. 253–296]; нормативно-правові акти, адміністративні акти, адміністративний договір, план та фактичні дії [180, с. 313-314]; підзаконні нормативні акти, адміністративні акти, адміністративні договори, адміністративні акти дії та акти-плани [188, с. 175].

В. В. Толкованов виділяє дві підгрупи інструментів публічного управління: загальні (універсальні) і локальні. Загальні інструменти управління – це стандартні правила та норми управлінської діяльності, які закріплені у правових документах, таких як закони, статути, інструкції тощо. Локальні інструменти управління, у свою чергу, доповнюють та конкретизують загальні норми, сприяючи виконанню більш загальних управлінських рішень. Вони можуть приймати форму постанов, наказів, розпоряджень, угод, контрактів, проведення нарад тощо [189].

Частина науковців до інструментів публічного адміністрування відносяться різноманітні форми і методи діяльності публічної адміністрації. Ці форми включають видання адміністративних актів, яке поділяється на видання підзаконних нормативно-правових актів та видання індивідуальних адміністративних актів. Також до них відноситься укладення адміністративних угод, учинення інших юридично значущих адміністративних дій та здійснення

матеріально-технічних операцій, то основними методами публічного адміністрування є заохочення, переконання і примус [128, с. 144].

Втім перелік інструментів публічного управління може бути розширений, оскільки в діяльності публічної адміністрації можуть використовуватися також регуляторно-планувальні, організаційно-технічні, інформативні, технічні прийоми, засоби та способи [190] у сфері захисту персональних даних.

Найбільш розповсюдженими інструментами діяльності публічної адміністрації (публічного адміністрування) у сфері захисту персональних даних можуть бути нормативні й індивідуальні (адміністративні) акти. Нормативні акти представляють собою правові документи, які ухвалюються у рамках підзаконної розпорядчої діяльності органів публічної адміністрації. Вони мають загальний характер і стосуються компетенції всіх органів, посадових осіб та установ. Нормативні акти деталізують та конкретизують закони з метою їх подальшого правозастосування [128, с. 147].

Для забезпечення захисту персональних даних використовується система нормативно-правових актів, які поділяються на законні і підзаконні акти. Одним із ключових законів, який є загальним у сфері захисту персональних даних, Закон України «Про захист персональних даних» та формує основу для захисту приватності та конфіденційності персональних даних громадян. Цей закон визначає права та обов'язки сторін, порядок обробки персональних даних, а також механізми захисту цих даних від незаконного доступу, використання та поширення.

Крім зазначеного вище загального закону, існують і спеціальні закони, які регулюють компетенції суб'єктів публічної влади в сфері захисту персональних даних та визначають їх повноваження. Такі спеціальні закони можуть включати в себе норми, що стосуються захисту персональних даних у певних сферах, наприклад, у медицині, освіті, фінансовій сфері тощо. Вони доповнюють загальний закон і надають додаткові вимоги та механізми обробки, зберігання, контролю за обробкою та захисту персональних даних у конкретних галузях.

Зокрема, варто наголосити, що такі спеціальні закони регулюють питання обробки, зберігання та захисту додаткових персональних даних. Наприклад, у сфері охорони здоров'я це стосується обробки додаткових персональних даних, що стосується стану здоров'я пацієнта, яка одночасно є конфіденційною інформацією і потребує додаткового захисту. Також, додаткові персональні дані щодо особи будуть оброблятись у сфері освіти, здійснення господарської діяльності, податковій сфері тощо. Так, з початку 2024 року в Україні зареєстровано 3,43 млн суб'єктів підприємницької діяльності, а кількість платників податків зросла на 60 тисяч [191].

Необхідно також наголосити, що застосування різних інструментів публічного адміністрування в сфері надання адміністративних послуг здійснюється з дотриманням принципу захищеності персональних даних [27].

Закон України «Про адміністративні процедури» передбачає, що при наданні адміністративних послуг ознайомлення з матеріалами справи, одержання копій документів та відомостей здійснюється виключно із законодавством про захист інформації [192].

При наданні публічних (електронних публічних) послуг обробка персональних даних суб'єктів звернення здійснюється володільцем та держателем Єдиного державного веб-порталу електронних послуг здійснюється згідно вимог законодавства про захист персональних даних [28].

Також, слід зазначити важливу роль підзаконних нормативно-правових актів, які приймають на виконання законів та деталізують, в тому чилі, порядок здійснення обробки, зберігання та захисту персональних даних органами публічної влади. До таких підзаконних нормативно-правових актів можемо віднести положення про відповідні центральні органи виконавчої влади, накази, порядки, інструкції в яких уточнюються повноваження органів публічної влади, їх структурних підрозділів щодо збирання, обробки, зберігання персональних даних, визначаються процедури щодо забезпечення їх захисту.

Так, Наказом Міністерства цифрової трансформації України від 20 травня 2020 року № 72 затверджено Порядок обробки та захисту персональних даних, володільцем яких є Мінцифри. Цей Порядок визначає загальні вимоги до організаційних і технічних заходів для обробки та захисту персональних даних. Ці заходи спрямовані на забезпечення таких цілей обробки персональних даних: забезпечення права особи на доступ до електронних послуг та інформації щодо адміністративних та інших публічних послуг; можливість звернення до органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій та отримання необхідної інформації з національних електронних інформаційних ресурсів для надання послуг; надання фізичним та юридичним особам інформації, необхідної для звернення до центрів надання адміністративних послуг; організація можливості попереднього запису суб'єктів звернення на прийом до працівників центрів надання адміністративних послуг шляхом електронної реєстрації; забезпечення доступу фізичних і юридичних осіб до навчальних ресурсів, пов'язаних з наданням адміністративних та інших публічних послуг; проведення моніторингу та оцінки якості послуг та інших дій [174].

Серед інструментів забепечення персональних даних важливу роль відіграє адміністративний акт – це вирішення, прийняте суб'єктом публічної адміністрації для вирішення конкретного адміністративного питання, що має юридичні наслідки для відповідних суб'єктів адміністративного права. Після одноразового застосування (виконання умов, передбачених у ньому) дія адміністративного акта завершується [128, с. 160].

Відтак, адміністративний акт може мати зв'язок з персональними даними у випадках, коли він містить інформацію про конкретні особи, яка є об'єктом обробки персональних даних. Наприклад, в адміністративному акті може бути зазначена інформація про ім'я, прізвище, адресу, контактні дані чи інші персональні характеристики осіб, на яких спрямований цей акт.

Згідно з принципами захисту персональних даних, обробка такої інформації є підпорядкованою закону та повинна відбуватися відповідно до

вимог правових норм, зокрема, до Закону України «Про захист персональних даних». Це означає, що перед збиранням, зберіганням, використанням чи передачею персональних даних у складі адміністративного акта, необхідно отримати згоду від осіб, чиї дані будуть використовуватися.

Таким чином, в контексті адміністративних актів, обробка персональних даних повинна здійснюватися відповідно до законодавства та з урахуванням прав та свобод громадян, включаючи право на конфіденційність і захист персональних даних.

У більшості випадків прийняття адміністративних, індивідуальних актів суб'єктами владних повноважень, пов'язаних із використанням персональних даних, здійснюється за згодою суб'єкта персональних даних. Прийняття індивідуальних адміністративних актів супроводжується вчинення суб'єктами публічної влади фактичних дій, пов'язаних із обробкою персональних даних у випадках отримання дозволу суб'єкту персональних даних або передбачених законом.

Фактичні дії як інструменти публічного адміністрування у сфері захисту персональних даних – це допоміжні форми публічного адміністрування суспільних відносин з метою задоволення публічного інтересу, прав і свобод людини, що пов'язано із обробкою персональних даних. Ці дії не призводять безпосередньо до формування нового юридичного становища або зміни існуючих правовідносин, проте стають значущими умовами для виникнення визначених юридичних наслідків незалежно від того, чи були вони спрямовані на досягнення цих наслідків чи ні [180, с. 181–182] для конкретного суб'єкта правовідносин, в тому числі для суб'єктів персональних даних. В процесі роботи з персональними даними суб'єкти публічної влади вчиняють фактичні дії щодо збирання, зберігання, обробки персональних даних, такі дії можуть бути врегульовані відомчими нормативно-правовими актами, що врегульовують питання захисту персональних даних.

Важливість інструментарію полягає у тому, що він допомагає органам державного управління адаптуватися до змінюваних умов зовнішнього та

внутрішнього середовища, відповідати сучасним викликам та загрозам, а також ефективно взаємодіяти з різними учасниками управлінського процесу. Слід зазначити, що у суто правовому та управлінському розумінні інструментарій управління має певні відмінності, але вони стосуються більшою мірою не розуміння змісту, а бачення «палітри» можливих варіантів інструментарію для публічного управління.

Інструментарій публічного управління у сфері захисту персональних даних включає в себе як традиційні форми управлінської діяльності, так і новітні технології та підходи, засновані на сучасних інформаційно-комунікаційних технологіях методики аналізу та прогнозування, а також системи моніторингу та контролю, методи прийняття рішень та інші інструменти, що забезпечують ефективне планування, організацію, мотивацію та контроль у сфері публічного управління, в тому числі пов'язані з обробкою персональних даних та забезпеченням персональних даних.

Наразі в Україні, публічне управління нерозривно пов'язане з використанням інформаційно-комунікаційних технологій, які виступають невід'ємною складовою забезпечення сталості та розвитку держави, а також забезпечення нею реалізації основної функції прав і свобод людини. Крім того, необхідною умовою входження нашої країни в глобальний інформаційний технічний простір та адаптації до стандартів ЄС є становлення та розвиток комунікаційної стратегії органів публічної влади. Нині актуальною залишається проблема збереження генеральної спрямованості розвитку країни на широке запровадження інформаційно-комунікаційних технологій у всі сфері соціального та економічного життя, забезпечення взаємозв'язку державних рішень щодо реалізації окремих концепцій: інформаційного суспільства, відкритого уряду, електронного урядування та електронної демократії, інформаційної та кібербезпеки тощо [193].

У контексті розвитку сучасного публічного управління, де інформаційні-телекомунікаційні системи набувають все більш широкого використання та значення, забезпечення захисту персональних даних набуває ключового

значення. Відтак, варто наголосити, що реалізація комунікаційної стратегії органів публічної влади, в тому числі запровадження системи електронного урядування в різних сферах публічного управління, не можлива без забезпечення і впровадження стандартів щодо обробки та захисту персональних даних.

Тому важливе місце у системі захисту персональних даних займають цифрові інструменти здійснення публічного управління. Цифрові інструменти публічного управління – це комп'ютерні програми, платформи та технології, які дозволяють органам державної влади ефективно взаємодіяти з громадянами, опрацьовувати великі обсяги даних та автоматизувати рутинні процеси. Ці інструменти використовують потужність цифрових технологій для підвищення ефективності, прозорості та доступності публічного управління. В цьому аспекті постає проблема законодавчого регулювання цифрових інструменти публічного управління.

Як наголошує М. Міхровська, електронне урядування визначається як публічно-управлінська діяльність із застосуванням інформаційно-комунікаційних технологій для надання державних послуг, обміну інформаційними комунікаційними трансакціями, інтеграції різних автономних систем і послуг між урядом і громадянами [180, с. 446–447], що нерозривно пов’язано із захистом персональних даних. Прикладами використання цифрових інструментів публічного управління виступають електронні системи, пов’язані із забезпеченням надання електронних публічних послуг, медичних послуг, освітніх послуг, системи електронного документообігу тощо. Вони можуть служити як засоби для надання громадянам доступу до інформації, так і як інструменти для збору та аналізу даних для прийняття обґрунтованих рішень щодо реалізації прав громадян.

Однак, використання цифрових технологій інструментів органами публічної влади вимагає великої уваги до питань безпеки, зокрема захисту персональних даних, приватності та етики.

Аналіз науково-теоретичних підходів доводить, що нині відсутні істотні відмінності і у багатьох сенсах за своїм змістом вони співпадають. Центральним у розумінні інструментів публічного управління є те, що вони виступають засобами, за допомогою яких державні органи реалізують свої функції, щоб досягти цілей у сфері публічної політики.

Водночас, на нашу думку, інструменти діяльності суб'єктів публічної адміністрації – це засоби реалізації функцій (повноважень) таких органів, а не лише засіб практичної реалізації певного управлінського рішення.

До основних підходів щодо класифікації інструментів діяльності суб'єктів публічної адміністрації можна віднести їх поділ на: загальні (універсальні) і локальні (за сферою дії); нормативно-правові, адміністративно-управлінські, економічно-фінансові, інституціональні (за змістом діяльності); нормативні й індивідуальні (адміністративні) акти, фактичні адміністративно значущі дії, укладення адміністративних договорів (за характером діяльності); регуляторно-планувальні, організаційно-технічні (за характеристикою діяльності). Окреме місце відведено також цифровим інструментам здійснення публічного управління.

Беручи до уваги зазначене вище теоретичного розуміння інструментів публічного управління, проаналізуємо окремі особливості інструментів адміністративно-правового забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації.

З позицій розуміння інструментального підходу системи публічної адміністрації, розглянемо положення важливого нормативно-правового акту у сфері обігу персональних даних – Типового порядку обробки персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 [177].

Якщо розглянути зазначений порядок з позицій правових функцій, то стає зрозумілим, що під інструментами захисту персональних даних (пункт 3) розуміються як регулятивні, організаційні, технічні, так і охоронні заходи публічно-управлінської діяльності у сфері персональних даних. Так, серед

іншого, йдеться про те, що володілець та розпорядник персональних даних зобов’язані вживати заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Водночас деталізація подібних організаційних та технічних заходів відсутня. Очевидно, йдеться про застосування організаційно-управлінських заходів та заходів технічного захисту інформації.

Водночас, у зв’язку з розвитком технологічних рішень в системі публічного управління, потрібно особливу увагу звернути на доповнення переліку цифрових організаційно-управлінських інструментів гарантіями захисту особи від прийняття автоматизованого рішення щодо обробки персональних даних, які мають бути закріплені на рівні нормативно-правового регулювання. Ми вважаємо, що особа має право не піддаватися рішенню, яке засноване виключно на автоматизованій обробці інформації. Це також стосується й інформації про її персональні дані, в тому числі профілюванні, що викликає для неї юридичні наслідки, або схожим чином суттєво впливає на її життя [156].

В цьому питанні, важливим є законодавче врегулювання процесу автоматичного аналізу персональних даних з метою оцінки певних особистих аспектів, таких як працевлаштування, економічний статус, здоров'я, особисті інтереси тощо, щодо конкретної особи. Цей процес використовується в різних сферах, включаючи маркетинг, банківську сферу, страхування тощо. Автоматизоване прийняття рішень відбувається без значущого людського втручання. За його допомогою системи можуть приймати рішення на основі алгоритмічного або предиктивного моделювання, використовуючи великі набори даних.

На нашу думку, обидва зазначені процеси можуть співпрацювати. Наприклад, профілювання може використовуватися для створення моделі поведінки користувача, яка потім використовується системою для автоматизованого прийняття рішень, таких як надання кредиту або персоналізація реклами. Важливо зазначити, що автоматизоване прийняття

рішень та профілювання можуть породжувати питання етики, прозорості та захисту персональних даних. Тому важливо забезпечувати правове регулювання та контроль, здійснювати перевірку таких систем на наявність системних збоїв або помилок, а також визначити технічні процедури для забезпечення захисту персональних даних.

Як наголошує У. Шадська, автоматизоване прийняття рішень у справах персональних даних означає використання персоналізованої інформації особи для оцінки різних аспектів, таких як робота, соціальний статус, стан здоров'я, особисті уподобання, місцезнаходження, подорожі та інше. Це відбувається за допомогою комп'ютерних систем без прямого втручання людини. Саме відсутність такого втручання є ризиком для захисту прав і інтересів суб'єктів персональних даних, оскільки програма не має здатності усвідомлювати всі можливі наслідки своїх рішень для особи, її прав та загального життя. Крім того, під час розробки алгоритму не завжди можна передбачити всі реальні ситуації, які можуть виникнути, що може призвести до прийняття помилкових рішень [156], в тому числі втручання в персональні дані.

Таким чином, на рівні нормативно-правового регулювання вимагає свого вирішення питання захисту персональних даних громадян при здійсненні автоматичної обробки, автоматизованого прийняття рішень, що досі на законодавчому не врегульовано належним чином.

Іншим важливим інструментом публічного адміністрування виступають фактичні дії суб’єктів публічного адміністрування. С. Г. Стеценко та В. Ю. Стеценко пропонують під фактичними діями розуміти практично орієнтовані дії суб’єктів публічного адміністрування, спрямовані на досягнення для приватних осіб конкретного результату, які проте не призводять до юридичних наслідків та зміни правового статусу учасників суспільних відносин [180, с. 378].

До таких фактичних дій у сфері адміністративно-правового забезпечення захисту персональних даних ми пропонуємо відносити організаційно-управлінські заходи, регуляторно-планувальні, організаційно-технічні заходи,

контрольно-наглядові та заходи з моніторингу. Характеристика організаційно-управлінських заходів, має бути розглянута через призму компетенції того чи іншого органу публічного управління та мети обробки персональних даних громадян. Наприклад, відмінності у меті використання персональних даних Єдиним державним демографічним реєстром (далі – ЄДДР) України [194] та Єдиним державним реєстром призовників, військовозобов'язаних та резервістів [137]. Так, перший, ЄДДР України створений з метою централізації, систематизації та уніфікації зберігання, обробки та використання демографічної інформації про громадян України, іноземців та осіб без громадянства, які перебувають на території держави. Основною метою ЄДДР є забезпечення державних органів, місцевого самоврядування, юридичних та фізичних осіб надійною, актуальною та оперативно доступною демографічною інформацією. Це сприяє покращенню якості надання адміністративних послуг, оптимізації управлінських процесів, підвищенню рівня захисту персональних даних та забезпеченню застосування єдиного підходу до ведення та використання демографічних даних у різних сферах діяльності. І зовсім іншою метою обумовлене ведення Єдиного державного реєстру призовників, військовозобов'язаних та резервістів, створеного для забезпечення військового обліку громадян України [137].

Безпосередньо у Положенні про технічний захист інформації в Україні [195] серед передбачених організаційних заходів, включають визначення процедури доступу працівників володільця/розпорядника до персональних даних; встановлення порядку обліку операцій, що пов'язані з обробкою персональних даних суб'єктів та їх доступом до них; розробку плану дій на випадок несанкціонованого доступу до персональних даних; пошкодження технічного обладнання чи виникнення надзвичайних ситуацій; проведення регулярних навчань співробітників, які мають стосунок до персональних даних [195].

Водночас, ефективна реалізація завдань публічного управління стає можливою і через використання інших інструментів адміністративно-

правового забезпечення захисту персональних даних, особливо коли йдеться про діяльність персоналу – уповноважених суб'єктів публічної влади, їх підрозділів та посадових осіб. До таких ми відносимо такі інструменти адміністративно-правового забезпечення як контроль (нагляд) та моніторинг.

В цілому, контроль у публічному управлінні є інструментом, спрямованим на перевірку діяльності органів влади, їх підрозділів, посадових осіб та інших суб'єктів з метою забезпечення їх відповідності законодавству, нормам, стандартам та іншим вимогам. Його основна мета – в першу чергу, забезпечення законності та визначення ефективності управлінської діяльності, в тому числі використання інструментів публічного управління, організаційних і технічних процедур у сфері захисту персональних даних, а також ефективності використання суб'єктами публічної влади ресурсів з метою виконання функції публічного управління у зазначеній сфері.

Необхідно зазначити, що контроль є невідємним елементом, стадією процесу публічного управління, її завершальним етапом, який вцілому визначає ефективність управління.

Підкреслимо, що на нашу думку, кожен з суб'єктів публічної адміністрації наділений повноваженнями щодо захисту персональних даних, в тому числі здійснення контролю в межах визначених законодавством. Зазначене дозволяє доповнити перелік необхідних управлінських рішень, а саме – актів дій, наступними елементами. По-перше, серед актів індивідуальної дії мають особливе місце займати відомчі приписи про усунення порушень у сфері захисту персональних даних фізичних осіб та притягнення до відповідальності посадових осіб, у дія яких було виявлено порушення. Такі дії носять неюрисдикційний характер. По-друге, це можливість винесення рішення про відшкодування завданої шкоди на підставі укладеної угоди з потерпілою стороною як форми альтернативного (досудового) врегулювання спору шляхом застосування процедури медіації.

Ще одним важливим інструментом адміністративно-правового забезпечення захисту персональних даних виступає моніторинг [128]. В цілому,

моніторинг як інструмент публічного управління представляє собою систематичний процес збору, аналізу та інтерпретації даних з метою відстеження та оцінки ефективності реалізації публічних політик, програм та проектів у різних сфер суспільних відносин, в тому числі у сфері обробки, зберігання та захисту персональних даних. Моніторинг також використовується для виявлення змін, прогресу або проблем публічного управління під час виконання завдань та досягнення поставлених цілей, коли мова йде про результати діяльності публічної адміністрації щодо захисту персональних даних.

Моніторинг дозволяє органам публічної адміністрації отримувати актуальну інформацію про стан реалізації різних ініціатив, виявляти недоліки та відхилення від запланованого, а також вносити корективи в управлінські рішення. Також моніторинг сприяє підвищенню прозорості та відкритості діяльності державних органів, оскільки результати моніторингу часто публікуються для широкої громадськості.

Існують різні методи та техніки моніторингу, зокрема опитування, аналіз документів, вивчення статистичних даних, проведення експертних досліджень, спостереження тощо. Вибір конкретного методу залежить від цілей моніторингу, доступності даних та ресурсів. Застосування моніторингу у сфері захисту персональних даних, як інструменту публічного управління, допомагає підвищити відповідальність, ефективність та результативність діяльності органів влади, а також зміцнює довіру громадян до державних інституцій щодо забезпечення їх прав.

Оцінюючи існуючи у науці підходи до вирішення проблематики дослідження, запропонуємо виділення інструментів адміністративно-правового забезпечення захисту персональних даних громадян: загальні (універсальні), тобто спільні інструменти для всіх суб’єктів публічної влади та локальні (відомчі), обумовлені специфікою компетенції окремого органу влади; нормативно-правові законодавчого та підзаконного характеру, а також нормативно визначені концепції та стратегії забезпечення захисту

персональних даних громадян; індивідуальні правозастосовні (адміністративні) акти та укладення адміністративних договорів; контрольно-наглядові, моніторингові, організаційно-управлінські та технічні інструменти забезпечення захисту персональних даних громадян.

Таким чином, інструменти адміністративно-правового забезпечення захисту персональних даних громадян – це врегульовані нормами адміністративного права зовнішні прояви конкретних дій уповноважених суб'єктів публічної адміністрації, в рамках яких реалізуються і за допомогою яких здійснюються регулюючий вплив на суспільні відносини у сфері обігу персональних даних для забезпечення прав та законних інтересів суб'єктів цих правовідносин.

Основними ознаками інструментів адміністративно-правового забезпечення захисту персональних даних громадян виступають наступні: інструменти адміністративно-правового забезпечення захисту персональних даних громадян, що відображають правову динаміку діяльності суб'єктів публічної адміністрації щодо виконання своїх повноважень у зазначеній сфері; реалізуються суб'єктами публічної адміністрації у межах повноважень визначених законодавством, яке регулює суспільні відносини у сфері забезпечення захисту персональних даних; реалізуються у відповідній процесуальній формі за встановленою процедурою з метою реалізації завдань та функції публічної адміністрації, щодо забезпечення прав, свобод та інтересів громадян у сфері забезпечення захисту персональних даних (нормативно-правового акту або акту індивідуальної правозастосовної дії); вибір інструментів адміністративно-правового забезпечення захисту персональних даних громадян зумовлюється специфікою поставленої мети щодо певного об'єкта публічного впливу, що встановлює найбільш ефективний варіант діяльності.

## 2.4 Європейський досвід адміністративно-правового забезпечення захисту персональних даних

Формування державної політики у сфері обігу та обробки та захисту персональних даних, на сучасному етапі євроінтеграційних процесів України вимагає аналізу зарубіжного досвіду адміністративно-правового забезпечення захисту персональних даних. В першу чергу йдеться про досвід ЄС, нормативно-правове регламентування та судову практику захисту персональних даних громадян у країнах-членах ЄС.

Державна політика у цій сфері та діяльність органів публічного адміністрування має базуватись на глибокому і всебічному теоретичному осмисленні правового, зокрема, й адміністративно-правового забезпечення відносин обігу, обробки та захисту персональних даних, сутності та механізму публічного управління у зазначеній сфері. Європейська правова система запропонувала та продовжує продукувати ефективні правові механізми забезпечення захисту персональних даних, серед яких вагоме місце відведене адміністративно-правовим засобам захисту персональних даних. Адміністративно-правове забезпечення захисту персональних даних пояснюється тенденцією до зростання масштабів використання персональних даних громадян у системі публічного управління та реалізації функції держави та її органів і посадових осіб, в тому числі в сфері захисту персональних даних.

Правове регулювання у сфері захисту персональних даних у ЄС ставить за мету захист прав, свобод і законних інтересів усіх фізичних осіб, що перебувають на його території, чиї персональні дані піддаються обробці. Діяльність органів публічної адміністрації при цьому базуються на концепції верховенства права людини, законної, прозорої та контрольованої обробки даних фізичних осіб, які надають свої персональні дані (суб'єктів персональних даних).

При цьому в ЄС, домінує підхід щодо забезпечення комплексу прав, до якого входить фундаментальне право фізичної особи на захист персональних

даних, з урахуванням існуючих ризиків для безпеки особистої інформації, у тому числі в мережі Інтернет, і включає наступні права: право на видалення даних (право бути забутим); право на доступ до інформації; право на виправлення; декларація про обмеження обробки даних; право на портативність даних; декларація про заперечення; декларація про захист персональних даних дітей.

У нормативно-правовій системі закріплено принцип, відповідно до якого реалізація особою своїх прав в сфері захисту персональних даних не повинна негативно впливати на права та свободи інших осіб. Для ефективного здійснення правового регулювання кожний суб'єкт правовідносин в сфері персональних даних наділений відповідними права і обов'язками, пов'язаними з обробкою (обов'язок особи дотримуватись нормативних актів ЄС та держав-членів, що стосуються захисту персональних даних), та факультативні, які передбачені для певних випадків (обов'язок надати додаткову інформацію, необхідну для підтвердження) особистості суб'єкта даних, або згода законного представника та ін.).

Наразі Україна вживає необхідних заходів щодо адаптації європейських стандартів щодо захисту персональних даних в національне законодавство, як держава-кандидат на вступ до ЄС. З цього приводу В. І. Теремецький та Д. В. Цвірюк наголошують про те, що незважаючи на успішне створення сучасної та адекватної нормативно-правової бази для розвитку системи захисту персональних даних в Україні за останні роки, на даний момент в країні напрацьовані лише основи законодавства у цій сфері. Це законодавство в цілому відповідає міжнародним стандартам, проте потребує подальшої роботи з систематизації, розробки виконавчих актів, національних стандартів та чіткого визначення термінів, понять і категорій [196, с.81].

Вирішення питання ефективного публічно-правового механізму забезпечення персональних даних громадян є також частиною вимог щодо майбутнього вступу України до ЄС та знаходить своє відображення у відповідних програмних документах.

Так, зокрема, у тексті Доповіді Європейської комісії «Ukraine 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels, 8.11.2023 SWD(2023) 699 final» («Звіт про Україну 2023, що супроводжує документ Повідомлення Комісії до Європейського парламенту, Ради, Європейського економічного та соціального комітету та Комітету регіонів Брюссель, 8.11.2023 SWD(2023) 699») йдеться поміж іншого про те, що Україна зобов'язана прийняти закон про захист персональних даних, узгоджений із acquis ЄС [197; 198, с. 6]. Також, у Доповіді Європейської комісії йдеться про те, що у сфері захисту персональних даних, Україна має продовжити роботу над приведенням у відповідність із acquis ЄС. Нинішнім ключовим законодавчим актом, який регулює захист даних, є Закон про захист персональних даних від 2010 року (Law on personal data protection of 2010). Він недостатньо деталізований і недостатньо виконується. Також, Україна ратифікувала Конвенцію 108 про захист осіб щодо автоматизованої обробки персональних даних (ILO Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data). Уповноважений Верховної Ради України з прав людини є органом, відповідальним за перевірку дотримання законодавства про захист персональних даних, але він не має відповідних ресурсів, щоб робити це ефективно. Законопроект про захист персональних даних було внесено до Верховної Ради 7 вересня 2022 року» [198, с.42].

Наголосимо, що базовим при цьому є приведення національного законодавства у сфері персональних даних до «acquis ЄС», яке походить від французького терміну «acquis communautaire», що в перекладі означає «спільне надбання». Acquis ЄС включає в себе різноманітні аспекти нормативно-правової уніфікації. Його ідея полягає в тому, щоб забезпечити єдність норм, стандартів і політик серед країн-членів ЄС, створюючи таким чином спільну базу для ефективної інтеграції та співпраці країн ЄС у різних сферах суспільного життя.

Ця сукупність включає різноманітні аспекти, які регулюють питання внутрішнього ринку, конкуренції, енергетики, транспорту, права людини, невід'ємною складовою яких є забезпечення права на приватність та захист персональних даних, споживачів тощо. Водночас, заходи осучаснення нормативно-правовго регулювання захисту персональних даних в Україні повинні відповідати умовам виконання Угоди про Асоціацію, між Україною та Європейським Союзом. Україна зобов'язується розробити та впровадити механізм, який забезпечить високий рівень захисту обігу персональних даних у відповідності до найвищих європейських та міжнародних стандартів, зокрема документів Ради Європи. Згідно зі статтею 14 Угоди про Асоціацію між Україною та Європейським Союзом, у систему захисту обігу персональних даних можуть бути включені такі складові, як обмін інформацією та експертами [199].

Система нормативного регулювання правових відносин персональних даних має достатньо довгу історію в Європі, які були розглянуті нами раніше, зокрема, при розгляді генези нормативно-правового регулювання забезпечення захисту персональних даних.

Новий етап у правовому регулюванні права на захист персональних даних почався з набрання чинності в 2018 році на території ЄС Загального Регламенту щодо захисту даних (Регламент (ЄС) 2016/679). Цей регламент замінив та скасував Директиву 95/46/ЄС, а також Директиву (ЄС) 2016/680, що встановлює правила захисту особистих даних щодо їх обробки компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування за кримінальні злочини або виконання кримінальних покарань. Кожна держава-член ЄС має імплементувати ці правила в своє законодавство і використовувати їх на своїй території з 6 травня 2018 року.

Розглянемо більш детально еволюцію правового регламентування як самого захисту персональних даних, так і ролі у ньому суб'єктів публічного управління. Положення цього Регламенту націлені на узгодження захисту основних прав та свобод фізичних осіб у контексті обробки персональних

даних та забезпечення вільного потоку цих даних між державами-членами ЄС. Головна мета Регламенту полягає у сприянні створенню простору свободи, безпеки, справедливості та економічного союзу, а також у підтримці економічного та соціального прогресу, закріпленні законності та зближенні економік у межах внутрішнього ринку, а також загальному добробуту громадян держав-членів ЄС.

Цілі та принципи Регламенту відповідають основним положенням Директиви 95/46/ЄС. Однак з розвитком інформаційних технологій та глобалізацією збільшилися транскордонні потоки персональних даних, що сформувало нові виклики у сфері їх захисту. Масштаб збору та використання цих даних значно зріс, а технології вплинули як на економіку, так і на соціальне життя. У зв'язку з цим виникла потреба у подальшій уніфікації та гармонізації законодавства про захист персональних даних у всіх країнах-членах ЄС [200, с. 89]. Регламент розширює вже існуючі права фізичних осіб як суб'єктів персональних даних та вводить нові, зокрема право на підвищений доступ до цих даних, право на перенесення персональних даних, право на забування, а також право на інформацію про випадки незаконного доступу до персональних даних.

Суб'єктами таких правовідносин виступають такі особи: фізичні особи, які надають свої персональні дані для обробки; фізичні чи юридичні особи, які проводять обробку таких даних; інститути, органи, агентства та установи Європейського Союзу (до них застосовується Регламент (ЄС) 2018/1725 та деякі інші правові акти Союзу); уповноважені незалежні органи, які здійснюють регулювання захисту персональних даних у Європейському Союзі та державах-членах; держави-члени ЄС (за винятком провадження ними діяльності, що підпадає під сферу дії Глави 2 Розділу V ДЕС) та їх органи (правила, що стосуються обробки персональних даних правоохоронними та судовими органами держав-членів, встановлює Директива (ЄС) 2016/680).

Під об'єктом права на захист персональних даних, у свою чергу, слід розуміти персональні дані, які означають будь-яку інформацію, що стосується

ідентифікованої або такої, що піддається ідентифікації фізичної особи. Така інформація має бути правдивою та повинна позначати унікальну характеристику даної особи (його ідентичність) у конкретний момент часу. До персональних даних може відноситися як загальнодоступна інформація, так і інформація конфіденційного характеру. Анонімна інформація може бути віднесена до персональних даних за дотримання певних умов.

Забезпечення захисту персональних даних також здійснюються Європейським судом з прав людини (далі – ЄСПЛ). Попри те, що право на персональні дані безпосередньо не згадується в Конвенції про захист прав людини і основоположних свобод, підпадає під її дію, що неодноразово підтверджувалось в практиці ЄСПЛ.

У 1987 році ЄСПЛ у справі Leander проти Швеції [201] визнав, що інформація з секретного поліцейського реєстру, що містила дані про особисте життя пана Леандера, а також відмова у наданні можливості йому спростувати ці дані, порушували його право на повагу до приватного життя, яке гарантується статтею 8 Конвенції про захист прав людини [202]. Суд надав визначення терміну «персональні дані» як будь-яку інформацію, яка стосується конкретно визначеної особи або особи, яка може бути конкретно визначеною. Це поняття охоплює не лише відомості про «приватне життя», що розуміється ширше, адже воно включає право на встановлення та розвиток відносин з іншими людьми, а також інформацію про професійну та ділову діяльність. [202**Error! Reference source not found.**]. Більше того, публічна інформація може вважатися «приватним життям», якщо вона систематично збирається та зберігається в базах даних, якими володіють органи публічної влади [203].

ЄСПЛ визначив різноманітні види персональних даних, що були предметом розгляду в справі. Серед них були такі дані: офіційний перепис, де збирається інформація про стать, сімейний стан, місце народження, етнічну приналежність та інші особисті дані; збір відбитків пальців, знімків, зразків клітин, профілів ДНК та іншої особистої або публічної інформації, навіть якщо

на неї поширюються умови таємності; збирання та зберігання медичних даних і інших записів; вимагання надати детальну інформацію про особисті витрати з фіскальною метою; прослуховування, запис і зберігання телефонних розмов; системи ідентифікації особи, розроблені для адміністративних і цивільних цілей, наприклад, бази даних в сфері охорони здоров'я, соціальної допомоги і податкових органів; знімки систем відеоспостереження, зроблені на вулицях; системи перехоплення розмов між ув'язненими і їх родичами у кімнатах для побачень у місцях ув'язнення.

Наразі практика Європейського суду з прав людини акцентує увагу на важливості захисту прав суб'єкта персональних даних. Особливу увагу приділяється праву на доступ до власних персональних даних. Це право передбачає, насамперед, обов'язок держави не втручатися у приватне життя шляхом обмеження можливості особи ознайомитись з інформацією про неї, яка збирається, зберігається, використовується та поширюється державними органами [201]. Крім цього, це право виникає із обов'язку держави забезпечувати повагу до приватного життя шляхом встановлення механізму доступу до персональних даних [204]. У цьому контексті, доступ до інформації має бути результативним, тобто, такий доступ не лише забезпечує можливість ознайомлення з персональними даними та складання витягів власноруч, але й дозволяє отримати копії документів із зазначеними персональними даними [205], а також бути здійсненим в межах розумних строків [206]. Право на доступ до персональних даних може бути звужено в інтересах держави, наприклад, для забезпечення національної безпеки [201], а також у приватних інтересах, наприклад, для захисту конфіденційної інформації третіх осіб [207].

Особливу увагу слід приділити забезпеченню безпеки персональних даних, що вимагає від держави позитивного зобов’язання забезпечувати повагу до приватного життя осіб, що передбачає впровадження системи правил та гарантій для захисту даних. Ця система має бути практичною та ефективною, перш за все, забезпечуючи виключення будь-якого несанкціонованого доступу до персональних даних. [**Error! Reference source not found.**]. Згідно з позицією

ЄСПЛ, право на корекцію або видалення своїх персональних даних означає, що відмова у можливості спростувати неточні персональні дані становить порушення права на повагу до приватного життя, яке гарантується статтею 8 Конвенції [203].

Крім того, позитивний обов’язок держави забезпечити повагу до приватного життя у цьому випадку передбачає наявність процедури, що дозволяє внесення змін у персональні дані, включаючи дані щодо етнічної належності суб’єкта персональних даних [208]. ЄСПЛ також визнає існування так званого права на забуття. Це означає, що тривале зберігання персональних даних без належних підстав вважається непропорційним втручанням у право на повагу до приватного життя [209].

Практика ЄСПЛ містить критерії правомірного обмеження прав на персональні дані, які відповідають загальним принципам законного втручання в приватне життя: втручання повинно бути здійснене відповідно до закону; воно має переслідувати законну мету; воно є необхідним у демократичному суспільстві. Поняття «відповідно до закону» не тільки передбачає, що відповідні заходи мають певну підставу в законі, але також ставить вимогу до якості цього закону, вимагаючи, щоб він був доступний особам, які стосуються, та передбачуваний в частині наслідків його застосування [202].

За практикою ЄСПЛ, вимога доступності закону передбачає, що нормативно-правові акти, які обмежують права на персональні дані, повинні бути оприлюднені та доступні громадськості. Це означає, що будь-які норми, які визначають обмеження прав особи на захист її персональних даних, повинні бути відомі та доступні для перегляду та зрозуміння. Такий принцип не лише забезпечує прозорість законодавства, а й дозволяє особам, які стосуються обмеження, бути інформованими про свої права та обов'язки. Важливо, щоб правила та умови обмеження були чіткими та однозначними, щоб уникнути непорозумінь та спростувати недоречні або несправедливі дії владних органів [203].

Передбачуваність у законі виявляється в тому, що норма має бути сформульована настільки чітко і зрозуміло, щоб будь-яка особа могла, в разі необхідності, отримати відповідну допомогу та розуміти, яким чином вона може регулювати своє поведінку відповідно до цих норм. Це передбачає, що правила повинні бути такими, щоб вони були доступними та зрозумілими для кожного, хто має з ними стикатися, і щоб особа могла передбачити наслідки своїх дій чи бездіяльності. Такий підхід забезпечує, що законність та справедливість застосування правових норм будуть зрозумілі і доступні для всіх громадян [203].

Переслідувана мета вважатиметься законною, якщо вона відповідає одному з визначених у другій частині статті 8 Конвенції суспільних інтересів або правам і свободам інших осіб. Це означає, що мета, яку переслідує держава, повинна бути відповідною інтересам суспільства або правам і свободам інших громадян. Наприклад, якщо держава переслідує мету забезпечення безпеки або громадського порядку, це може вважатися легітимним, оскільки ці цілі стосуються суспільних інтересів. Також, якщо держава переслідує мету захисту прав і свобод інших осіб, наприклад, захисту приватності або безпеки, це також може вважатися законним. Однак важливо, щоб переслідувана мета була обґрунтованою та не перевищувала необхідних меж для досягнення цієї мети [210, с. 71].

Втручання в особисті дані вважається обґрунтованим у демократичному суспільстві, якщо воно відповідає актуальним суспільним потребам і є пропорційним до законної мети, яку переслідує держава. Наприклад, захист національної безпеки може вважатися пріоритетним при здійсненні перевірок для прийняття на посаду, що має важливе значення з точки зору безпеки країни, і ці інтереси переважають приватні інтереси особи, яка здобувається персональні дані. Важливо, щоб втручання було обґрунтованим та не перевищувало межі, необхідні для досягнення цієї мети, забезпечуючи відповідність із загальними принципами права і правами людини [201].

Отже, відповідно до практики ЄСПЛ, право на захист персональних даних забезпечується в рамках права на особисте життя. Персональні дані включають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, яку можна конкретно ідентифікувати. Суб'єкт персональних даних має ряд прав, таких як право на доступ, право на зміну, право на знищення та право на захист своїх персональних даних. Проте, ці права можуть бути обмежені в інтересах досягнення легітимної мети, за умови, що таке обмеження відповідає закону і є необхідним у демократичному суспільстві.

Законодавство ЄС встановлює спеціальні уповноважені органи для забезпечення захисту персональних даних. Згідно з положеннями Конвенції № 108 Ради Європи від 1981 року та «Пакету захисту даних» Європейського Союзу від 2016 року, у всіх країнах ЄС і країнах, що мають економічні зв'язки з державами-членами ЄС, мають бути створені спеціальні державні органи для нагляду і контролю за дотриманням прав у сфері захисту персональних даних – уповноважені органи нагляду (Омбудсмен чи Уповноважений) з захисту персональних даних. Ці органи мають бути незалежними, підпорядкованими закону, підзвітними парламенту, а в організаційних питаннях можуть бути підконтрольними уряду. Національні уповноважені органи, в свою чергу, призначають контролерів, які визначають цілі і засоби обробки персональних даних, яка здійснюється фізичною або юридичною особою, державним органом, установою або іншим органом («процесором»), що обробляє персональні дані за його дорученням [211, с.55].

На рівні ЄС створено спеціальний орган – Європейську Раду із захисту даних, який є незалежним органом ЄС, що сприяє послідовному застосуванню правил захисту даних у всьому Європейському Союзі, а також сприяє співпраці між органами захисту даних ЄС. Зазначений орган складається з керівників одного наглядового органу від кожної держави-члена ЄС, а також Європейського інспектора захисту персональних даних, або з їх представників. У випадку, коли в державі-члені більше одного наглядового органу, які є відповідальними за моніторинг застосування положень щодо персональних

даних, призначається єдиний представник відповідно до права такої держави-члена. Водночас, Європейська Комісія має право брати участь у діяльності та засіданнях Європейської ради із захисту даних без права голосу. Для цього Європейська Комісія призначає свого представника. Голова Європейської ради із захисту даних інформує Європейську Комісію про діяльність Європейської ради із захисту даних [20].

Таким чином, Європейська рада із захисту даних складається з представників національних органів захисту даних та окремих представників інших органів Європейського Союзу. Європейська рада із захисту даних має власний секретаріат, що відповідає за організацію її діяльності.

Європейська Рада із захисту даних виконує контрольну, виконавчу, консультативну функцію, а також функцію з координації та взаємодії. На Європейського Уповноваженого із захисту даних покладено інформаційну, консультативну, організаційну, охоронну та контрольну функції. Національні наглядові органи наділені повноваженнями для здійснення інформаційної, охоронної, виконавчої, контрольної функції та функції з координації та взаємодії. Для цілей реалізації своїх функцій кожен уповноважений орган наділений владними повноваженнями стосовно суб'єктів, які перебувають у його юрисдикції.

Відповідно до підходів європейського консенсусу Європейська рада із захисту даних забезпечує уніфіковане застосування на рівні Регламенту 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. «Про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних». При цьому важливо відзначити, що європейський консенсус може бути визначений на двох рівнях. По-перше, це може бути реалізовано через встановлення конкретних правил і заходів, які застосовуються для втілення правових принципів у конкретних системах. По-друге, консенсус може бути відображений на рівні загальних принципів, які лежать в основі національних правових стандартів [212, с. 13].

Загальний регламент про захист даних також дає право Європейській раді із захисту даних приймати обов'язкові рішення, адресовані національним органам нагляду, для забезпечення послідовного виконання його положень серед яких: надавати загальні керівні роз’яснення щодо законодавства про захист персональних даних; консультувати Європейську Комісію з будь-яких питань, що стосуються захисту персональних даних, та щодо будь-якого нового запропонованого законодавства, на рівні Європейського Союзу; приймати висновки щодо механізму забезпечення узгодженості у транскордонних справах, пов'язаних із захистом персональних даних; сприяти співпраці та ефективному обміну інформацією та передовим досвідом між національними наглядовими органами [20].

Важливим елементом входження України у європейський правовий простір захисту персональних даних є отримання статусу спостерігача при Європейській раді із захисту даних. Прийняття України в якості члена зі статусом спостерігача до Європейської ради із захисту даних буде сприяти європейській інтеграції, поглибленню взаємовідносин між Україною та Європейським Союзом як в економічному, так і політичному плані, запровадженню європейських принципів і стандартів захисту персональних даних.

Наголосимо, що система публічного контролю дотримання прав суб’єктів персональних даних, з врахуванням європейської практики та доктрини має включати наступні складові: по-перше, на загальноєвропейському інституційному рівні – Європейську Комісія, по-друге, – це Європейську раду із захисту даних (входять голови всіх наглядових органів), по-третє, наглядові органи (свій для кожної країни ЄС) та керівний наглядовий орган – за місцем знаходження контролера/оператора (рис.2.1).

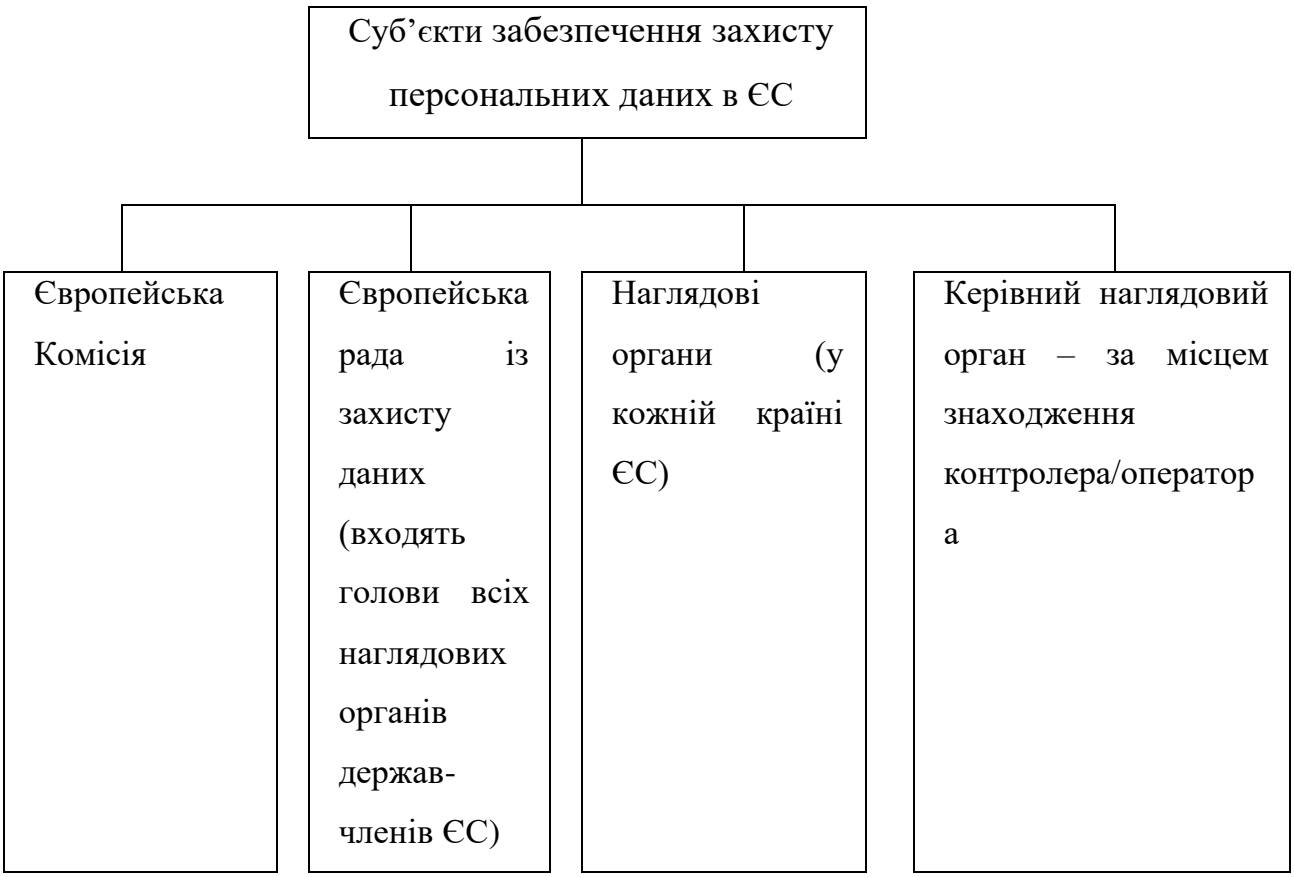



Рисунок – 2.1 Структура суб’єктів забезпечення захисту персональних даних в ЄС

Примітка. Розроблено автором.

Наголосимо, що кожен із уповноважених органів має специфічні функції, спрямовані на здійснення єдиної мети – захисту прав, свобод та законних інтересів фізичних осіб при проведенні операцій з обробки їх персональних даних різними суб'єктами.

Керівний наглядовий орган (supervisory authority concerned) – це наглядовий орган, у відомстві якого знаходиться обробка, оскільки: контролер або процесор має організаційну одиницю на території держави-члена цього наглядового органу; обробка істотно відбивається або очікувано позначиться

істотно на особах, які проживають у державі-члені наглядового органу; або до цього наглядового органу подано скаргу.

Основна організаційна одиниця контролера в Євросоюзі має бути місцем його центральної адміністрації в ЄС, крім тих випадків, коли рішення про цілі та засоби обробки персональних даних приймаються іншою організаційною одиницею контролера в ЄС – у такому разі ця інша організаційна одиниця має вважатися основною організаційною одиницею.

На думку вітчизняних вчених, які досліджували питання захисту персональних даних, сутність публічного контролю у царині захисту персональних даних полягає у встановленні відповідності процесу обробки персональних даних вимогам міжнародним директивам, договорам України у сфері захисту персональних даних, ратифікованих Верховною Радою України та національним нормативно-правовим актам [213].

Як слушно зазначає О.А. Заярний, для забезпечення здійснення публічного моніторингу та виконання міжнародних зобов'язань, що випливають з актів Ради Європи та GDPR, в Україні розглядається важливим створення інформаційного омбудсмена. Цей омбудсмен буде незалежним, колегіальним центральним органом виконавчої влади, який матиме спеціальний статус. Він буде нести відповідальність перед Президентом України та підконтрольний і підзвітний Верховній Раді України [159].

Відтак, наразі Україна вживає заходів щодо приведення національного законодавства до стандартів ЄС. Позиція українського законодавця полягає в тому, що контролюючим органом, за аналогією та стандартами ЄС, має стати, Національна комісія з питань захисту персональних даних та доступу до публічної інформації [134]. Зазначена пропозиція відповідає Оновленій Конвенції 108, що кожна держава має призначити щонайменше один контролюючий орган влади, який би був відповідальним за забезпечення дотримання вимог із захисту персональних даних [214].

Для досягнення цієї мети, національний контролюючий орган повинен мати широкі повноваження. Зокрема, він може проводити розслідування та

здійснювати втручання, виконувати функції, пов'язані з транскордонною передачею даних, приймати рішення щодо порушень і застосування адміністративних санкцій, а також брати участь у судових провадженнях. Крім того, згідно з Конвенцією, законодавчі та адміністративні заходи, що передбачають обробку персональних даних, повинні бути обов'язково погоджені з контролюючим органом [133].

В Україні наразі контроль за дотриманням зазначених прав здійснює Уповноважений Верховної Ради України з прав людини. Однак, виконання ефективного контролю в цій сфері відповідно до всіх міжнародних стандартів стає неможливим в межах повноважень Омбудсмена. Об'єднання функцій контролю за вказаними правами з мандатом Омбудсмена загрожує ефективності реалізації як першого, так і другого [133].

Також наголосимо, що Регламентом (ЄС) 2018/1807 про вільний рух неперсональних даних в Європейському Союзі [215] та Регламентом (ЄС) 2022/868 про управління даними [216] також створюються інституційні структури для контролю за обробкою даних, незалежно від того, чи має справу персональні чи неперсональні дані. Ці механізми мають використовуватися разом з Регламентом (ЄС) 2016/679 (GDPR) для забезпечення ефективного регулювання цього процесу і забезпечення відповідності вимогам щодо захисту даних [20].

Віще зазначені нормативно-правові акти визначають стандарти для обробки особистих та неперсональних даних, а також визначає права громадян у сфері захисту їх приватності. Відповідно до цих інституційних рамок, установлених зазначеними актами, організації та установи повинні адаптувати свою діяльність з огляду на перехід від попереднього підходу, спрямованого на захист даних, до цілісного підходу, заснованого на управлінні даними.

Відзначається, що управління даними включає в себе не тільки аспекти безпеки, але й аналіз, структурування, якість та зберігання даних, а також їхню відкритість для внутрішніх потреб та можливість взаємодії з іншими системами та організаціями.

Отже, підхід спрямований на цілісне управлінні даними висвітлює перехід від вузького підходу винятково захисту даних до більш широкого стратегічного управління даними, яке є ключовим для досягнення успіху в умовах сучасного інформаційного середовища.

Останні законодавчі акти ЄС (Регламент (ЄС) 2016/679 (GDPR), Регламент (ЄС) 2018/1807 Європейського парламенту та Ради від 14 листопада 2018 року щодо рамок вільного руху неперсональних даних в Європейському Союзі, Регламент (ЄС) 2022/868, Директива Європейського Парламенту і Ради 2002/58/ЄС), що визначає принципи та умови для ефективного обміну неперсональними даними в межах ЄС, зокрема: створює умови для вільного переміщення даних за територією ЄС без обмежень; забезпечує відсутність обмежень при зберіганні та обробці неперсональних даних в інших країнах-членах; розвиває прозорість та стандартизацію в області неперсональних даних, сприяючи їх ефективному використанню та обміну в різних секторах економіки; визначає правила для забезпечення безпеки та захисту цих даних, зокрема, стандарти щодо копіювання та реплікації даних в інших європейських країнах; встановлює механізми управління ризиками та вирішення конфліктів, пов'язаних із здійсненням вільного руху неперсональних даних; надає прозорий каркас для взаємодії між підприємствами та публічними органами щодо обміну неперсональними даними відповідно до встановлених стандартів; сприяє розвитку цифрового ринку та підтримує інновації шляхом створення дієвого механізму для використання неперсональних даних у різних галузях економіки та суспільства [215], [15], [216].

Крім того, Регламент (ЄС) 2022/868 передбачає створення Єдиного інформаційного пункту, який діятиме як інтерфейс для вторинних користувачів, що прагнуть повторно використовувати ці дані, а також створення/призначення окремого компетентного органу з реєстрації організацій з альтруїстичного обміну даними. Ініціатива щодо «створення/призначення окремого компетентного органу з реєстрації організацій з альтруїстичного обміну даними» вказує на потребу у визначенні

чіткої інституційної структури для регулювання та координації організацій, які здійснюють обмін даними у сфері альтруїзму чи добровільних ініціатив. Основною метою є створення спеціалізованого, компетентного органу, який відповідатиме за реєстрацію та нагляд за діяльністю організацій, які здійснюють обмін даними в рамках альтруїстичних проектів чи ініціатив, спрямованих на благодійність або громадське благо. Такий компетентний орган може виконувати функції реєстрації, моніторингу, оцінки та регулювання діяльності цих організацій, забезпечуючи додержання законів та етичних стандартів у сфері обміну даними та забезпечення їх захисту.

Міністерство цифрової трансформації України може мати повноваження щодо обробки міждержавних запитів на доступ до даних від постачальників, не нав'язуючи собі функції накладання санкцій. У той же час, сприяння розвитку системи державного контролю за обігом даних може передбачати створення нового контролюючого органу в інформаційній сфері, який об'єднає повноваження з питань доступу до інформації та захисту персональних даних [217, с.16]. На нашу думку, доцільним є підтримання проекту Закону, який передбачає створення окремого органу для забезпечення контролю за захистом персональних даних.

В останні роки важливість адміністративно-правового забезпечення захисту персональних даних стає особливо актуальною як у країнах ЄС, так і в Україні. Це відбувається на тлі широкої дискусії щодо впровадження в різні сфери життя суспільства інформаційних технологій та програмних комплексів, які об'єднуються терміном штучний інтелект [218]. У процесі їх застосування, як показує сучасна практика, виникають проблеми з надійним захистом персональних даних користувачів.

З метою правового врегулювання проблем використання штучного інтелекту при обробці персональних даних громадян та з метою їх забезпечення парламентом ЄС 13 березня 2024 року було прийнято перший нормативно-правовий акт «Artificial Intelligence Act» («Закон про штучний інтелект») [36], який врегулював питання використання штучного інтелекту та захисту

персональних даних при його використанні. Заявлена мета цього нормативно-правового акту полягає в захисті фундаментальних прав, демократії, принципу верховенства закону та екологічної стійкості від потенційно небезпечного використання штучного інтелекту. Також його метою є сприяння інноваціям та зміцнення позицій Європи як провідного гравця в цій галузі [219]. Зазначений нормативно-правовий акт знаменує собою ключовий момент у глобальному регулюванні використання штучного інтелекту, встановлюючи прецедент для відповідальної та етичної розробки і його практичного впровадження. Прийняття зазначеного акту знаменує собою початок нового етапу нормативно-правового регулювання, як питань використання штучного інтелекту, так і питань захисту персональних даних при його використані.

«Artificial Intelligence Act» передбачає: заходи для розробки і використання технології штучного інтелекту враховуючи пріоритет прав людини, безпеки та прозорості; вимоги щодо надійних гарантій захисту від алгоритмічних упереджень і дискримінації, суворі вимоги до конфіденційності та безпеки даних, а також механізми підзвітності та контролю.

Згідно з новими правилами особлива увага приділяється використанню штучного інтелекту у сферах, які вважаються високоризиковими, щодо забезпечення прав людини. Наприклад ті, що використовуються в охороні здоров’я, на транспорті та в правоохоронних органах, підлягатимуть суворій регулятивній перевірці та вимогам до тестування. Нові принципи містять заборони застосування штучного інтелекту, які можуть порушувати права громадян, включаючи системи біометричної ідентифікації на основі чутливих ознак, а також непризначене збирання зображень осіб з Інтернету або відеозаписів з камер відеоспостереження для створення баз даних для розпізнавання осіб [36].

Згідно з новим законом, використання систем біометричної ідентифікації правоохоронними органами «в принципі заборонено, за винятком конкретно визначених та обмежених випадків». Використання таких систем у реальному часі можливе лише за умови суворого дотримання заходів безпеки і «потребує

спеціального попереднього судового або адміністративного дозволу». Це може стосуватися наприклад ситуацій пошуку зниклої людини або запобігання терористичним загрозам [219].

Яскравим прикладом необхідності створення організаційних та правових рамок для захисту прав людини в сфері обігу персональних даних є швидке поширення штучного інтелекту, наприклад, чат-бота на основі штучного інтелекту ChatGPT, розробленим компанією OpenAI. Останніми роками штучний інтелект набув широкого використання, що в свою чергу породжує низку правових питань, в тому числі щодо обробки штучним інтелектом персональних даних, які містяться в вильному доступі в світовій мережі. Італія стала першою країною, яка ввела обмеження на використання штучного інтелекту через проблеми, пов'язані, в тому числі, з обробкою персональних даних користувачів [220].

Причиною цього рішення була втрата персональних даних та платіжної інформації користувачів чат-бота 20 березня 2023 року. За думкою Національного управління із захисту персональних даних Італії, масштабна діяльність зі збору персональних даних, проведена розробниками чат-бота на основі штучного інтелекту ChatGPT, не може бути виправдана режимом тестування алгоритмів, що лежать в його основі, через відсутність нормативно-правових засад. Національне управління із захисту персональних даних Італії вказує на те, що недостатність будь-якого фільтра для перевірки віку користувачів ставить неповнолітніх під ризик неприпустимої поведінки відносно їхнього розвитку і самосвідомості. OpenAI були зобов'язані повідомити про вжиті заходи з усунення виявлених технічних проблем [221].

У квітні 2023 року Міністри цифрових технологій країн «Великої сімки» (G7) зреагували на проблему правового регулювання використання штучного інтелекту. Вони узгодили необхідність прийняття відповідних законів для цього. Зазначено, що таке правове регулювання має зберігати відкрите та сприятливе середовище для розвитку технологій штучного інтелекту. Крім

того, воно повинно ґрунтуватися на демократичних цінностях, враховуючи занепокоєння щодо конфіденційності та ризиків для безпеки [222].

Наразі забезпечення захисту персональних даних фізичних осіб у контексті розвитку штучного інтелекту стає важливим завданням для органів публічного управління і повинно бути врегульоване законодавством. Потреба у створенні ефективних механізмів захисту особистих даних обумовлена також широким використанням інноваційних проектів, таких як «цифрове урядування» та «смарт-міста», що ґрунтуються на створенні обширних баз даних користувачів. Необхідно регулювати питання стосовно використання та обробки персональних даних у процесі «навчання» штучного інтелекту [223].

Враховуючи, що нині Україна є одним із лідерів щодо запровадження інформаційних технологій в діяльність органів публічного управління, а також створення системи електронного урядування, та здійснює широкий доступ до застосування, в тому числі програм штучного інтелекту. Проте, із зростанням використання інформаційно-телекомунікаційних технологій та технологій штучного інтелекту виникає потреба у відповідних нормативно-правових механізмах, які гарантуватимуть ефективне забезпечення захист прав та свобод громадян, включаючи захист персональних даних відповідно до стандартів ЄС.

Зазначені вище приклади з світової практики доводять необхідність вже зараз розпочати розробку комплексу правових та організаційно-управлінських заходів забезпечення захисту персональних даних громадян у контексті використання штучного інтелекту. Аналіз досвіду ЄС дає підстави зазначити, що основними завданнями щодо подальшого вдосконалення правового регулювання захисту персональних даних є здійснення заходів за такими напрямками: а) приведення національного законодавства щодо захисту персональних даних до стандартів ЄС, як невід’ємна складова європейської інтеграції України; б) визначення на законодавчому рівні системи органів публічного контролю за забезпеченням захисту персональних даних, яке відповідає законодавству ЄС.

Аналіз зарубіжного досвіду адміністративно-правового забезпечення захисту персональних даних дає можливість запропонувати такі зміни до національного законодавства в сфері забезпечення захисту персональних даних.

Зокрема, доповнити ст. 2 «Визначення термінів» Закон України «Про захист персональних даних» абзацом четвертим в такій редакції: «захист персональних даних – це застосування юрисдикційних та неюрисдикційних заходів визначених законодавством України, нормативно-правовими актами ЄС, міжнародними договорами, звичаями та судовою практикою у випадках порушення вимог захисту персональних даних». Також, доповнити ст. 2 «Визначення термінів» зазначеного закону абзацом одинадцятим та викласти його в такій редакції: «порушення захисту персональних даних - порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які було передано, збережено або іншим чином опрацьовано».

Зазначене розуміння категорій відповідає усталеній практиці прийнятій у європейській правовій системі. Так у Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) закріплено тезу, що порушення можна класифікувати відповідно до трьох відомих принципів інформаційної безпеки, пов’язаних з найбільш поширеними видами правопорушень: «порушення конфіденційності» (Confidentiality breach) – коли відбувається несанкціоноване або випадкове розкриття персональних даних або доступ до них; «порушення цілісності» (Integrity breach) – випадкова несанкціонована або випадкова зміна персональних даних; «Порушення доступності» (Availability breach) – випадкова чи несанкціонована втрата доступу до персональних даних або їх знищення [224].

Водночас, положення Закону України «Про захист персональних даних» необхідно доповнити новою статтею 22-1, пов’язаною з можливостями забезпечення захисту персональних даних органами державної влади та

органами місцевого самоврядування. Цю статтю пропонуємо викласти у такій редакції:

**«Стаття 22-1. Забезпечення захисту персональних даних органами державної влади та органами місцевого самоврядування**

1. У випадках, встановлених Конституцією України, законом, міжнародними договорами, згода на обов'язковість яких надана у встановленому законодавством порядку, особа має право звернутися за захистом персональних даних до органу державної влади або органу місцевого самоврядування.

2. Орган державної влади або орган місцевого самоврядування забезпечують здійснення захисту персональних даних у межах, на підставах та у спосіб, що встановлені Конституцією України, законом, міжнародними договорами, згода на обов'язковість яких надана у встановленому законодавством порядку .

Рішення, прийняте зазначеними органами щодо захисту персональних даних, не є перешкодою для звернення за їх захистом до суду».

Варто наголосити, що європейський досвід в сфері захисту персональних даних в контексті євроінтеграції України набуває особливої актуальності. Оскільки, це стосується забезпечення відповідності українського законодавства міжнародним стандартам щодо захисту персональних даних, зокрема, Загальному регламенту з захисту даних (GDPR) ЄС, що сприятиме підвищенню рівня захисту, конфіденційності і приватності персональних даних громадян у всіх сферах. Слід окремо наголосити, про необхідність нормативно-правового регулювання, відповідно до законодавства ЄС, питань функціонування штучного інтелекту та захисту при цьому персональних даних. Це допоможе уникнути недоліків та ризиків, пов'язаних з використанням безпосередньо штучного інтелекту та використання штучним інтелектом інформації, яка містить персональні дані, що знаходяться в мережі у вільному доступі. Таке регулювання забезпечить правовий фундамент для розвитку та використання новітніх технологій в Україні, дозволить зберегти баланс між

інноваціями та правами людини, забезпечуючи високий рівень захисту прав та свобод громадян. Зазначене вимагатиме також подальших наукових досліджень та змін на законодавчому рівні у сфері забезпечення захисту персональних даних.

**Висновки до розділу 2.**

1. Проведений аналіз теоретичних та практичних аспектів адміністративно-правового забезпечення захисту персональних даних громадян дозволяє зробити такі висновки. Адміністративно-правове забезпечення захисту персональних даних громадян – це врегульована адміністративними нормами системна діяльність суб’єктів публічної адміністрації щодо адміністративно-правового регулювання, реалізації, охорони та захисту суспільних відносин у сфері персональних даних.

Структура адміністративно-правового забезпечення захисту персональних даних, як окрема група суспільних відносин, враховуючи її специфіку, складається з таких елементів: 1) об’єкт адміністративно-правового забезпечення захисту персональних даних – суспільні відносини в сфері обробки та захисту персональних даних; 2) суб’єкти адміністративно-правового забезпечення захисту персональних даних – органи публічної влади, установи, підприємства, організації, в тому числі і приватні, які відповідають за розробку, впровадження та контроль дотримання нормативно-правових актів щодо захисту персональних даних громадян. Вони здійснюють регулюючу діяльність, спрямовану на забезпечення прав та свобод осіб у сфері обробки їхніх персональних даних, а також на забезпечення відповідності цих процесів вимогам законодавства та міжнародних стандартів; 3) норми адміністративного права щодо забезпечення захисту персональних даних – нормативно закріплені правила, процедури та відповідальність за обробку та захист персональних даних громадян. Ці норми регулюють діяльність органів публічної влади та інших суб'єктів, що здійснюють обробку таких даних, зокрема встановлюють умови збору, зберігання, використання та передачі персональних даних, а

також встановлюють заходи захисту від несанкціонованого доступу, втрати, викривлення чи незаконного використання таких даних; 4) адміністративно-правові відносини в сфері забезпечення захисту персональних даних та їх зміст – це комплекс взаємодій між суб'єктами персональних даних та суб’єктами адміністративно-правового забезпечення захисту персональних даних, що здійснюють обробку персональних даних, та державними органами, які відповідають за забезпечення дотримання відповідних нормативно-правових актів. Зміст таких відносин полягає у реалізації заходів забезпечення прав та свобод громадян у сфері обробки їх персональних даних і включають такі аспекти: регулювання збору, зберігання, використання та передачі персональних даних відповідно до законодавства; встановлення процедур та вимог щодо захисту персональних даних від несанкціонованого доступу, втрати, викривлення чи незаконного використання; визначення відповідальності за порушення правил обробки персональних даних та невиконання вимог законодавства; забезпечення доступу до персональних даних у випадках, передбачених законом, та захисту конфіденційності таких даних; здійснення контролю за дотриманням вимог законодавства щодо захисту персональних даних; 5) гарантії адміністративно-правового забезпечення захисту персональних даних включають: законодавчі гарантії, які встановлюють правові норми та стандарти, що регулюють збір, обробку, зберігання та передачу персональних даних, а також встановлення відповідальності за їх порушення; організаційні, які визначають систему організаційних та технічних заходів захисту персональних даних від несанкціонованого доступу, втрати, викривлення чи незаконного використання; контроль за забезпеченням захисту, який включає контроль за дотриманням вимог щодо захисту персональних даних включаючи оцінку ризиків та вдосконалення систем безпеки, а також можливість звернення за відновленням порушених прав.

2. Під суб’єктом адміністративно-правового забезпечення захисту персональних даних громадян необхідно розуміти орган публічної

адміністрації, який здійснює публічне управління у сфері захисту персональних даних в процесі реалізації прав громадян та надання адміністративних послуг компетенція якого включає правове регулювання, збір, обробку, зберігання та забезпечення захисту персональних даних. Суб'єкт адміністративно-правового забезпечення захисту персональних даних громадян може виступати в ролі володільців, а іноді розпорядників персональних даних або третіх осіб.

Суб'єктів адміністративно-правового забезпечення можна класифікувати за наступними критеріями. По-перше, що є вкрай важливим в умовах збройної російської агресії, класифікувати суб'єктів забезпечення захисту персональних даних за сферами діяльності: на цивільні (Міністерство охорони здоров'я України, Міністерство освіти і науки України тощо) та мілітаризовані (МОУ, в аспекті ведення реєстру військовозобов'язаних, призовників, резервістів тощо; МВС України в аспекті ведення реєстру у справах пропавших безвісти в особливих обставинах). По-друге, можна здійснити класифікацію за сферами повноважень, тобто на публічні (органи публічної влади: органи виконавчої влади, органи місцевого самоврядування) та приватні (приватні юридичні особи та фізичні особи підприємці) По-третє, суб'єкти забезпечення захисту персональних даних можна класифікувати за критерієм відносно виду персональних даних, тобто на суб'єкти забезпечення захисту загальних персональних даних (МОН України, Міністерство юстиції, підприємства) та суб'єкти забезпечення захисту особливо чутливих та конфіденційних персональних даних (МОЗ України, МВС України, в частині реєстру пропавших безвісти, МОУ)

Проведений аналіз нормативно-правового регулювання повноважень суб'єктів адміністративно-правового забезпечення захисту персональних даних громадян дозволяє стверджувати про наявність прогалин у чинному законодавстві та необхідність удосконалення як порядку їх здійснення у цій сфері так і розширення змісту та уточнення таких повноважень на рівні законодавчих та підзаконних нормативно-правових актів. Важливим залишається питання врегулювання проблеми обробки персональних даних

після смерті суб'єкта персональних даних, використання технологій штучного інтелекту для відстеження дій суб'єктів персональних даних у електронних комунікаціях та сервісах, регламентування порядку розгляду вимог суб'єкта персональних даних.

3. Захист персональних даних здійснюється за допомогою інструментів адміністративно-правового забезпечення. Інструменти адміністративно-правового забезпечення захисту персональних даних громадян – це врегульовані нормами адміністративного права зовнішні прояви конкретних дій уповноважених суб'єктів публічної адміністрації, в рамках яких реалізуються і за допомогою яких здійснюються регулюючий вплив на суспільні відносини у сфері обігу персональних даних для забезпечення прав та законних інтересів суб'єктів цих правовідносин.

Основними ознаками інструментів адміністративно-правового забезпечення захисту персональних даних громадян виступають наступні: відображають правову динаміку діяльності суб'єктів публічної адміністрації щодо виконання своїх повноважень у зазначеній сфері; реалізуються суб'єктами публічної адміністрації у межах повноважень визначених законодавством, яке регулює суспільні відносини у сфері забезпечення захисту персональних даних; реалізуються у відповідній процесуальній формі за встановленою адміністративною процедурою; реалізуються з метою виконання завдань та функції публічної адміністрації, щодо забезпечення прав, свобод та інтересів громадян у сфері забезпечення захисту персональних даних (нормативно-правового акту або акту індивідуальної правозастосовної дії); вибір інструментів адміністративно-правового забезпечення захисту персональних даних громадян зумовлюється специфікою поставленої мети щодо забезпечення захисту персональних даних.

Інструменти адміністративно-правового забезпечення захисту персональних даних громадян можна поділити на: загальні (універсальні), тобто спільні інструменти для всіх суб'єктів публічної влади та локальні (відомчі), обумовлені специфікою компетенції окремого органу влади;

нормативно-правові: законодавчого та підзаконного характеру, а також нормативно визначені концепції та стратегії забезпечення захисту персональних даних громадян; індивідуальні (адміністративні) акти; фактичні дії; контрольно-наглядові, моніторингові, організаційно-управлінські та технічні інструменти забезпечення захисту персональних даних громадян.

4. Досвід ЄС щодо адміністративно-правового забезпечення персональних даних дозоляє зробити висновок про те, що основними завданнями України в контексті євроінтеграції в зазначеній сфері є здійснення правових та організаційних заходів за такими напрямками: а) приведення національного законодавства щодо захисту персональних даних до стандартів ЄС з метою формування невідємної складової європейської інтеграції України; б) визначення на законодавчому рівні системи органів публічного контролю за забезпеченням захисту персональних даних та їх повноважень. Надзвичайно важливе значення має виконання стандартів ЄС щодо створення єдиного окремого органу державної влади, який буде визначати стандарти обробки та безпеки персональних даних, здійснювати контроль за суб'єктами публічної влади щодо забезпечення захисту персональних даних.

# ВИСНОВКИ

1. З аналізу генези теоретико-правових аспектів права на захист персональних даних можна виділити чотири етапи розвитку та становлення нормативно-правового забезпечення захисту персональних даних в Європі та Україні:

Перший етап пов'язаний з появою та нормативнним закріпленням в окремих європейських країнах правової концепції «privacy» (або «право на приватність») починаючи з кінця XIX століття і до середини XX. В цей період на теренах України відбувається виключно теоретичне формування забезпечення особистих прав людини та її приватності, які не були безпосередньо відображені в правових нормах.

Другий етап, припадає на період з другої половини і до кінця XX століття, коли окремо виділяється на теоретичному рівні сфера правового захисту персональних даних та здійснюється їх нормативно-правове регулювання на рівні національного законодавства та законодавства ЄС. В цей час на території України на рівні радянської конституції було визначено особисті права громадянина, хоча це носило виключно декларативний характер.

Третій етап розпочинається з початку XXI століття і до 2023 року характеризується створенням загальних стандартів ЄС у сфері захисту персональних даних та закріплення їх на законодавчому рівні ЄС, імплементацією цих стандартів у національне законодавство країн-членів ЄС. В Україні з отриманням незалежності почався розвиток законодавства у сфері захисту персональних даних у відповідності до європейських стандартів, що безпосередньо пов'язано з євроінтеграційним курсом України.

Четвертий, новітній етап безпосередньо пов'язаний з швидким розвитком технології штучного інтелекту і розпочинається з 20-х років XXI ст, прийняттям перших законодавчих актів на національному рівні та на рівні ЄС щодо використання штучного інтелекту при обробці персональних даних та необхідності їх забезепечення.

2. Персональні дані громадян - це будь-які відомості або дані, в об'єктивізованій формі, що стосуються суб'єкта даних (фізичної особи), який підлягає ідентифікації. Персональним даним громадян притаманні наступні ознаки: інформаційний зміст персональних даних – вони є відомостями або даними про конкретну фізичну особу; ідентифікуючі властивості- вони дозволяють визначити ( ідентифікувати ) конкретну фізичну особу; визначена форма фіксації у певному джерелі (носії) персональних даних; не вичерпність; правова форма персональних даних, яка розпочинається із початком сукупності дій пов'язаних із їх обробкою та забезпеченням захисту..

3. Суб'єкт персональних даних – це конкретна фізична особа , персональні дані якої обробляються, а саме підлягають збиранню, зміні, зберіганню та захисту з метою ідентифікації цієї особи, у тому числі з використанням інформаційних технологій та штучного інтелекту.

Суб'єктів персональних даних можна класифікувати за рівнем законодавчого регулювання, як такі, що підпадають під дію загального законодавства в сфері персональних даних, тобто безпосередньо Закону України «Про захист персональних даних», та регулювання на рівні спеціального законодавства, яке на основі загального закону у сфері захисту персональних даних забезпечує захист персональних даних підгруп суб'єктів.

Суб'єктів персональних даних можна класифікувати за критерієм сфери суспільних відносин: медична сфера; фінансова сфера; освітня сфера; сфера надання публічних послуг; сфера реалізації виборчих прав та інші.

4. Адміністративно-правововое забезпечення захисту персональних даних громадян - це врегульована адміністративними нормами системна діяльність суб'єктів публічної адміністрації щодо адміністративно-правового регулювання, реалізації, охорони та захисту суспільних відносин у сфері персональних даних.

Структура адміністративно-правового забезпечення захисту персональних даних, як окрема група суспільних відносин, враховуючи її специфіку, буде складатися з таких елементів: 1) об'єкт адміністративно-

правового забезпечення захисту персональних даних; 2) суб'єкт адміністративно-правового забезпечення захисту персональних даних; 3) норми адміністративного права щодо забезпечення захисту персональних даних; 4) адміністративно-правові відносини в сфері забезпечення захисту персональних даних; 5) гарантії адміністративно-правового забезпечення захисту персональних даних.

5. Під суб'єктом адміністративно-правового забезпечення захисту персональних даних громадян необхідно розуміти орган публічної адміністрації, який здійснює публічне управління у сфері захисту персональних даних в процесі реалізації прав громадян та надання адміністративних послуг компетенція якого включає правове регулювання, збір, обробку, зберігання та забезпечення захисту персональних даних.

Суб'єкти адміністративно-правового забезпечення можна класифікувати за наступними критеріями: 1) за сферами діяльності та повноваженнями на цивільні та мілітаризовані; 2) за сферами повноважень: публічні та приватні; 3) за видами персональних даних: суб'єкти забезпечення захисту загальних персональних даних та суб'єкти забезпечення захисту особливо чутливих та конфіденційних персональних даних.

6. Інструменти адміністративно-правового забезпечення захисту персональних даних громадян – це врегульовані нормами адміністративного права зовнішні прояви конкретних дій уповноважених суб'єктів публічної адміністрації, в рамках яких реалізуються і за допомогою яких здійснюються регулюючий вплив на суспільні відносини у сфері обігу персональних даних для забезпечення прав та законних інтересів суб'єктів цих правовідносин.

Основними ознаками інструменти адміністративно-правового забезпечення захисту персональних даних громадян виступають наступні : відображають правову динаміку діяльності суб'єктів публічної адміністрації щодо виконання своїх повноважень у зазначеній сфері; реалізуються суб'єктами публічної адміністрації у межах повноважень визначених законодавством, яке регулює суспільні відносини у сфері забезпечення захисту

персональних даних; реалізуються відповідній процесуальній формі за встановленою адміністративною процедурою; реалізуються з метою виконання завдань та функцій публічної адміністрації, щодо забезпечення прав, свобод та інтересів громадян у сфері забезпечення захисту персональних даних (нормативно-правового акту або акту індивідуальної правозастосовної дії); вибір інструментів адміністративно-правового забезпечення захисту персональних даних громадян зумовлюється специфікою поставленої мети щодозабезпечення захист персональних даних.

Інструментів адміністративно-правового забезпечення захисту персональних даних громадян можна поділити на: загальні (універсальні) та локальні (відомчі); нормативно-правові законодавчого та підзаконного характеру, а також нормативно визначені концепції та стратегії забезпечення захисту персональних даних громадян; індивідуальні (адміністративні) акти та фактичні дії; контрольно-наглядові, моніторингові, організаційно-управлінські та технічні інструменти забезпечення захисту персональних даних громадян.

7. Досвід ЄС щодо адміністративно-правового забезпечення персональних даних основними завданнями України в контексті євроінтеграції в зазначеній сфері є здійснення правових та організаційних заходів за такими напрямками: а) приведення національного законодавства щодо захисту персональних даних до стандартів ЄС, як невід'ємна складова європейської інтеграції України; б) визначення на законодавчому рівні системи органів публічного контролю за забезпеченням захисту персональних даних, яке відповідає законодавству ЄС, зокрема, щодо створення єдиного окремого органу державної влади, який буде визначати стандарти обробки та безпеки персональних даних, здійснювати контроль за суб'єктами публічної влади щодо забезпечення захисту персональних даних.

8. Запровадження стандартів ЄС вимагає внесення змін до національного законодавства в сфері забезпечення захисту персональних даних. Зокрема, доповнити ст. 2 «Визначення термінів» Закон України «Про захист персональних даних» абзацом четвертим в такій редакції : «захист

персональних даних - це застосування юрисдикційних та неюрисдикційних заходів визначених законодавством України, нормативно-правовими актами ЄС, міжнародними договорами, звичаями та судовою практикою у випадках порушення вимог захисту персональних даних». Також, доповнити ст. 2 «Визначення термінів» зазначеного закону абзацом одинадцятим та викласти його в такій редакції «порушення захисту персональних даних - порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які було передано, збережено або іншим чином опрацьовано».

Положення Закону України «Про захист персональних даних» необхідно доповнити новою статтею 22-1 щодо повноважень органів державної влади та органів місцевого самоврядування та викласти у такій редакції :

**«Стаття 22-1. Забезпечення захисту персональних даних органами державної влади та органами місцевого самоврядування**

1. У випадках, встановлених Конституцією України, законом, міжнародними договорами, згода на обов'язковість яких надана у встановленому законодавством порядку, особа має право звернутися за захистом персональних даних до органу державної влади або органу місцевого самоврядування.

2. Орган державної влади або орган місцевого самоврядування забезпечують здійснення захист персональних даних у межах, на підставах та у спосіб, що встановлені Конституцією України, законом, міжнародними договорами, згода на обов'язковість яких надана у встановленому законодавством порядку.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Софіюк Т. О. Прайвесі і концепція поколінь прав людини. *Часопис Київського університету права*. 2020. № 2. С. 255–258.

2. Judith DeCew Privacy. Stanford Encyclopedia of Philosophy. URL: https://plato.stanford.edu/entries/privacy/ (дата звернення: 11.12.2021).

3. Худояр Л. В. Принцип рівності у правовій ідеології українських православних братств XVI-XVIII ст. *Часопис Київського університету права*. 2011. № 1. С. 66-70. URL: http://nbuv.gov.ua/UJRN/Chkup_2011_1_19. (дата звернення: 11.12.2021).

4. Драгомановський збірник. «Вільна Спілка» та сучасний український конституціоналізм / за редакцією Т.Г. Андрусяка. Львів: Світ, 1996. 256 с.

5. Загальна декларація прав людини: Міжнародний документ від 10 грудня 1948 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 11.12.2021).

6. Конвенція про захист прав людини і основоположних свобод: Міжнародний документ від 04 листопада 1950 р. / Верховна Рада України. URL: http://zakon3.rada.gov.ua/ laws/show/995_004 (дата звернення: 11.12.2021).

7. The Privacy Act of 1974. Office of Privacy and Civil Liberties. U.S. Departament of Justice. URL: https://www.justice.gov/opcl/privacy-act-1974 (дата звернення: 11.12.2021).

8. Malte Kröger. *Datenschutz und Prüfungsrecht Was das Nowak-Urteil für das Prüfungswesen bedeutet. Junge Wissenschaft im Öffentlichen Recht.* URL: https://www.juwiss.de/8-2018/ (дата звернення: 11.12.2021).

9. Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/ 2021-01-27/ (дата звернення: 11.12.2021).

10. SAFARI ou la chasse aux Français. URL: http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg (дата звернення: 11.12.2021).

11. Конституції СРСР 1977 року. URL: https://zakononline.com.ua /documents/show/169373___601885 (дата звернення: 11.12.2021).

12. Конституція Української Радянської Соціалістичної Республіки. Прийнята на позачерговій сьомій сесії Верховної Ради Української РСР дев'ятого скликання 20 квітня 1978 р. / Верховна Рада України. URL: http://static.rada.gov.ua/site/const/istoriya /1978.html (дата звернення 11.12.2021 р.)

13. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Міжнародний документ від 28 січня 1981 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 11.12.2021).

14. Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» : Міжнародний документ від 24 жовтня 1995 р. / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 11.12.2021).

15. Директива Європейського Парламенту і Ради 2002/58/ЄС щодо обробки персональних даних та захисту конфіденційності в секторі електронних засобів зв'язку (Директива про електронну конфіденційність): Міжнародний документ від 12 липня 2002 р. URL: https://ips.ligazakon.net/document/view/mu02283 (дата звернення: 20.11.2023).

16. Regulation (EC) № 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)**.** *Eur-lex.* URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML (дата звернення: 11.12.2021).

17. Treaty establishing the European Economic Community (Rome, 25 March 1957). URL: https://www.cvce.eu/en/obj/treaty_establishing_the_european_economic_

community_rome_25_march_1957-en-cca6ba28-0bf3-4ce6-8a76-6b0b3252696e.html (дата звернення: 11.12.2021).

18. Договір про Європейський Союз (Маастріхт, 7 лютого) Міжнародний документ від 7 лютого 1992 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_029#Text (дата звернення: 11.12.2021).

19. Хартія Основних прав Європейського Союзу: Міжнародний документ від 7 грудня 2000 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text (дата звернення: 11.12.2021).

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм (дата звернення: 11.12.2021).

21. Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» (Директива PNR)». URL: http://ippi.org.ua/sites/default/files/8_1.pdf (дата звернення: 11.12.2021).

22. Діхтієвський П. В. Адміністративно-правове забезпечення захисту персональних даних громадян в умовах воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. (10). 2023. URL: https://doi.org/10.54929/2786-5746-2023-10-01-15 (дата звернення: 11.12.2021).

23. Про захист персональних даних: Закон України від 01 червня 2010 р. № 2297–VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 11.12.2021).

24. Про інформацію : Закон України від 13 січня 2011 р. № 2938-VI / Верховна Рада України. URL https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.10.2022).

25. Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19 жовтня 2017 р. № 2168-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2168-19#Text (дата звернення: 15.10.2022).

26. Сенюта І. Я. Захист персональних даних у сфері охорони здоров'я: алгоритм змін. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2014. Випуск 6-1/2014. С. 216-221.

27. Про адміністративні послуги: Закон України від 6 вересня 2012 р. № 5203-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text (дата звернення: 11.12.2021).

28. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 р. № 1689-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/ 1689-20#Text (дата звернення: 11.12.2021).

29. Про публічні електронні реєстри: Закон України від 18 листопада 2021 р. № 1907-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Tex (дата звернення: 11.12.2021).

30. Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців та громадських формувань: Закон України 15 травня 2003 р. № 755-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/755-15#Text (дата звернення: 11.12.2021).

31. Про державну реєстрацію актів цивільного стану: Закон України від 1 липня 2010 р. 2398-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2398-17#Text (дата звернення: 11.12.2021).

32. Кодекс законів про працю України: Закон України від 10 грудня 1971 р. № 322-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/322-08#Text (дата звернення: 11.12.2021).

33. Цивільний кодекс України: Закон України від 16 січня 2003 р. № 435-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 11.12.2021).

34. Про введення воєнного стану в Україні: Указ Президента України від 24 лютого 2022 року №64/2022 / Верховна Рада України. URL:

https://www.president.gov.ua/documents/642022-41397 (дата звернення: 11.12.2021).

35. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12 березня 2022 р. № 263. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263 (дата звернення: 30.05.2022)

36. Artificial Intelligence Act: MEPs adopt landmark law. URL: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-la.M5rp8rD6VJMckEwOVeo (дата звернення: 14.04.2024).

37. Концептуальні засади розвитку вітчизняного адміністративного права та процесу: тенденції, перспективи, практика: колективна монографія / Є. Герасименко, П. Діхтієвський, Н. Задирака,Т. Коломоєць, В. Клинчук та ін.; за заг. ред. П. Діхтієвського, В. Пашинського. Рига, Латвія : “Baltija Publishing”, 2022. 986 с. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/256/7156/14911-1 (дата звернення: 14.04.2024).

38. Камінська Н. В. Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. *Науковий вісник Національної академії внутрішніх справ*. 2015. № 3. С. 106-114. URL: http://nbuv.gov.ua/UJRN/Nvknuvs_2015_3_15 (дата звернення: 15.10.2022).

39. Джинджоян В.В., Саленко А.С., Сазонець І.Л. Соціальні детермінанти розвитку сфери послуг в концепції формування постіндустріального суспільства. Рівне. Волин. Оберег. 2021. 190 с.

40. Саленко А. С. Інформація та знання як рушійна сила постіндустріального розвитку. *Ефективна економіка*. 2021. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=9062 (дата звернення: 12.11.2022).

41. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України: автореф. дис. ... канд. юрид. наук: 12.00.03. Київ, 2010. 19 с.

42. Концевой Р. С. До питання визначення поняття «персональні дані». *Інформація і право*. 2012. № 2. С. 23–28.

43. Майданик Р. А. Аномалії в цивільному праві України: навч.-практ. Посіб: Київ: Юстініан, 2007. 912 с.

44. Сопілко І. М. Сучасне поняття персональних даних: доктринальний та нормативний аспекти. *Юридичний вісник. Повітряне і космічне право*. 2013. № 3. С. 63-68. URL: http://nbuv.gov.ua/UJRN/Npnau_2013_3_14 (дата звернення: 15.10.2022).

45. Саєнко М.І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні. *Право і суспільство*. 2015. № 3. С. 103.

46. Речицький В. В. Проект Конституції України 2009. Перспектива прав людини. Харків: Права людини, 2009. 144 с.

47. Брижко В.М. Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук: 12.00.07. Київ, 2004. 251 с.

48. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні: навчальний посібник. Київ: Юстініан, 2006. 171 с.

49. Дяковський О. С. Визначення поняття персональних даних як правової категорії: сучасні проблеми та шляхи вирішення. Інформація і право. 2017. № 3. С. 51-56. URL: http://nbuv.gov.ua/UJRN/Infpr_2017_3_7 (дата звернення: 15.10.2022).

50. Серебряник О. О. Інформація про особу як об’єкт цивільних справ: дис. ... канд. юрид. наук: 12.00.03. Івано-Франківськ, 2016. 209 с.

51. Кардаш А. В. Інформація про особу та персональні дані: окремі аспекти співвідношення. *Форум права: електрон. наук. фахове вид*. 2017. № 4. С. 87–92. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_4_15.pdf. (дата звернення: 15.10.2022).

52. Василюк В.Я., Климчук С.О. Інформаційна безпека держави. Київ, 2008. 135 с.

53. Брель О.С. Персональні дані як об'єкт інформаційних правовідносин за участю суб'єктів господарювання. *Право України*.2011. № 4. С.220–224.

54. Бєлова Ю.Д. Цивільні правовідносини щодо персональних даних: монографія: Хмельницький: ФОП Мельник А.А., 2019. 192 с.

55. Цимбалюк В. С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства: монографія. Київ: «Освіта України», 2011. 268 с.

56. Інформація. Юридична енциклопедія: в 6 т. / за ред. Ю.С. Шемшученка. Київ: «Укр. енциклопедія» ім. М.П. Бажана, 1998. Т. 2: Д-Й. 744 с.

57. Бебик В. Інформація. Політична енциклопедія. Київ. Парламентське видавництво, 2011. С. 300.

58. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. URL: http:// zakon5.rada.gov.ua/laws/show/254%D0%B (дата звернення: 15.10.2022).

59. Про звернення громадян: Закон України від 2 жовтня 1996 р. № 393/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text (дата звернення: 15.10.2022).

60. Про доступ до судових рішень: Закон України від 22 грудня 2005 р. № 3262-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3262-15#Text (дата звернення: 15.10.2022 р.).

61. Про організацію формування та обігу кредитних історій: Закон України від 23 червня 2005 року № 2704-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2704-15#Text (дата звернення: 15.10.2022).

62. Про телебачення і радіомовлення: Закон України в редакції Закону від 12 січня 2006 р. № 3317-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3759-12#Text (дата звернення: 15.10.2022).

63. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012. *Офіційний вісник України*. 2012. № 9. Ст. 332.

64. Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Adopted on 20th June, Article 29 Data Protection Working Party. URL : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (дата звернення: 15.10.2022).

65. Про державний захист працівників суду і правоохоронних органів: Закон України від 23 грудня 1993 р. № 3781-XII / Верховна Рада України. URL: http://zakon3.rada.gov. ua/laws/show/3781-12 (дата звернення: 15.10.2022).

66. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві Закон України від 23 грудня 1993 р. № 3782-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3782-12#Text. (дата звернення: 15.10.2022).

67. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 15.10.2022).

68. Про розвідку: Закон України від 17 вересня 2020 р. № 912-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 15.10.2022).

69. Про Службу безпеки України: Закон України від 25 березня 1992 р. № 2229-XII / Верховна Рада України. URL: http://zakon0.rada.gov.ua/laws/show/2229-12 (дата звернення: 15.10.2022).

70. Про Державне бюро розслідувань: Закон України від 12 листопада 2015 р. № 794-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/794-19/card2#Card (дата звернення: 15.10.2022).

71. Лютіков П.С. Персональні дані: доктринальне тлумачення категорії у науках адміністративного та інформаційного права. *Аналітично-порівняльне право*. 2023. № 6. С. 472-477.

72. Класифікація. Юридична енциклопедія: в 6 т. / за ред. Ю.С. Шемшученка. Київ: «Укр. енциклопедія» ім. М.П. Бажана, 2001. Т. 3. 792 с.

73. Шишка Р. Б. До проблеми індивідуалізації фізичної особи. *Еволюція цивільного законодавства: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції.* Академія правових наук України, НДІ приватного права і підприємництва, НДІ інтелектуальної власності, Національна юридична академія ім. Я. Мудрого (29-30 квітня 2004 р.). Харків, 2004. С.153–162.

74. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. 2013. Вип. 6-3(1). С. 90–94.

75. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (дата звернення: 15.10.2022).

76. Цьоменко А. В. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. *Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки*. 2023. № 1 (53). С. 41-45. URL: https://miljournals.knu.ua/index.php/visnuk/article/view/1028/955 (дата звернення: 25.04.2024).

77. Скакун О. Ф. Теорія права і держави. Підручник. Київ: Алерта, 2021. 528 с.

78. Фатхутдінов В. Г. Поняття суб'єктів, об'єктів та змісту адміністративно-правових відносин у сфері громадської безпеки. *Держава та регіони. Серія: Право.* 2018. № 1 (59). С. 127-132.

79. Кунєв Ю.Д., Дувінг В.О. Публічно-адміністративна діяльність – об'єкт адміністративно-правової науки. *Правова позиція*. 2019. № 4 (25). С. 40-48.

80. Авер'янов В. Б. Адміністративне право України. Академічний курс: в двох томах. Київ: ТОВ «Видавництво «Юридична думка», 2007. Том 1: Загальна частина : підручник / ред. колегія Авер'янов В. Б. та ін. 592 с.

81. Адміністративне право України: навч. посіб. для здобув. ступ. вищ. освіти бакалав. спец. «Право» освіт.-проф. прогр. «Правознавство» / за заг. ред. Т. О. Коломоєць. Запоріжжя: Гельветика, 2018. 84 с.

82. Адміністративне право України. Повний курс: підручник / за ред. В. Галунька, О. Правоторової. Видання третє. Київ: Академія адміністративно-правових наук, 2020. 466 с.

83. Бліхар М.М., Крикавська І.В. Правова характеристика взаємодії органів судової влади та інститутів громадянського суспільства. *Науковий вісник Ужгородського Національного Університету*. 2022. Випуск 70. С. 283-287.

84. Адміністративне право України. Повний курс: підручник / В. Галунько, П. Діхтієвський, О. Кузьменко та ін.; за ред. В. Галунька, О. Правоторової. Видання четверте. Херсон: ОЛДІ-ПЛЮС, 2021. 656 с.

85. Теорія держави і права: підруч. / Ю. А. Ведєрніков, І. А. Сердюк, О. М. Куракін та ін.; кер. авт. кол. канд. юрид. наук, проф. Ю. А. Ведєрніков. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ, 2015. 468 с.

86. Теорія держави та права: навч. посіб. / Є.В. Білозьоров, В.П. Власенко, О.Б. Горова, А.М. Завальний, Н. В. Заяць та ін.; за заг. ред. С. Д. Гусарєва, О. Д. Тихомирова. Київ: НАВС, Освіта України, 2017. 320 с.

87. Мацелик Т.О. Суб'єкти адміністративного права: поняття та система: Ірпінь: Видавництво Національного університету державної податкової служби України, 2013. 342 с.

88. Різак М.В. Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні. автореф. дис. ... д-ра юрид. наук: 12.00.07. Харків, 2018. 39 с.

89. Про правовий статус іноземців та осіб без громадянства від 22 вересня 2011 р. № 3773-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3773-17#Text (дата звернення: 20.12.2022).

90. Про біженців та осіб, які потребують додаткового або тимчасового захисту: Закон України від 08 липня 2011р. № 3671-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3773-17#Text. https://zakon.rada.gov.ua/laws/show/3671-17#Text (дата звернення: 20.12.2022).

91. Положення про Єдину державну електронну базу з питань освіти, в редакції постанови Кабінету Міністрів України від 12 липня 2017 р. № 550 / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/752-2011-%D0%BF (дата звернення: 20.12.2022).

92. Про забезпечення хімічної безпеки та управління хімічною продукцією: Закон України від 01 грудня 2022 р. № 2804-IX / Верховна Рада України. URL:https://zakon.rada.gov.ua /laws/show/2804-20#Text (дата звернення: 20.12.2022).

93. Порядок надання відомостей з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань: Наказ Міністерства юстиції України від 10 червня 2016 р. № 1657/5 / Верховна Рада України.URL:http://zakon0.rada.gov.ua/laws/show/z0839-16 (дата звернення: 20.12.2022).

94. Порядок обробки персональних даних у базі персональних даних – Державному реєстрі фізичних осіб – платників податків, затверджений Наказом Міністерства фінансів України від 24 лютого 2015 р. № 210 / Верховна Рада України.URL: http://zakon2.rada.gov.ua/laws/show/z0278-15 (дата звернення: 20.12.2022).

95. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 20.12.2022).

96. Про державний реєстр виборців: Закон України від 22 лютого 2007 р. № 698-V / Верховна Рада України. URL :https://zakon.rada.gov.ua/laws/show/698-16#Text. (дата звернення: 25.07.2023)

97. Барсуков К.В. Адміністративно-правове забезпечення проходження служби працівниками органів внутрішніх справ у складі міжнародних миротворчих підрозділів: автореф. дис. … канд. юрид. наук: 12.00.07. Київ, 2010. 20 с.

98. Плескач М.В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. *Часопис Київського університету права.* 2020. № 4. С. 201–209. URL: https://chasprava.com.ua/index.php/journal/issue/view/81/%E2%84%964-2020 (дата звернення 25.06.2023).

99. Сидоренко О.П. Правове забезпечення: до питання інтерпретації поняття legal provision: interpretation of the concept. *Актуальні проблеми вітчизняної юриспруденції*. 2018. №1. С.39-46.

100. Гумін О.М. Адміністративно-правове забезпечення: поняття та структура. *Наше право*. 2014. № 4. С. 46-50. URL: http://nbuv.gov.ua/UJRN/Nashp_2014_4_9 (дата звернення: 25.06.2023).

101. Терзі О.О. Концепція адміністративно-правового забезпечення охорони здоров'я в Україні: автореф. дис. ... доктора. юрид. наук: 12.00.07. Київ, 2021. 44 с. URL: https://drive.google.com/file/d/1LTnOxC-XCIiu5w7jfEe-f4Ykb2bWXhj-/viewт (дата звернення: 25.06.2023).

102. Лук'янова Г. Ю. Адміністративно-правове забезпечення координації суб'єктів протидії корупції в сучасних умовах державотворення: проблеми теорії і практики: автореф. дис. ... доктора. юрид. наук: 12.00.07. Київ, 2021. 41 с. URL: https://drive.google.com/file/d/1Nd-NZp9Idf9LTTMWgSrWDQPvsgyQ0UCC/view. (дата звернення: 25.06.2023).

103. Замрига А.В. Адміністративно-правове забезпечення господарської діяльності в Україні: автореф. дис. ... доктора. юрид. наук: 12.00.07. Київ, 2021.

40 с. URL: https://drive.google.com/file/d/176BhR7krRZTX9YxudgU-JYC5RCxbV3zT/view (дата звернення: 25.06.2023).

104. Кудін А. В. Адміністративно-правове забезпечення патентної діяльності в Україні: автореф. дис. ... доктора. юрид. наук: 12.00.07. Київ, 2021. 42 с. URL: https://drive.google.com/file/d/16JI6Tspr8VHge11jbWOyLi8YjHHAlief/view (дата звернення: 25.06.2023).

105. Гвоздик С. П. Адміністративно-правовий механізм забезпечення прав пацієнта психіатричного закладу в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2021. 23 с. URL: https://drive.google.com/file/d/1GOT16Rmuf8wokv7Lk4xGhY1eVaWci2va/view (дата звернення: 25.06.2023).

106. Пашинський В.Й. Адміністративно-правове забезпечення оборони України: теорія і практика: дис. ... доктора. юрид. наук: 12.00.07. Київ, 2020. http://scc.univ.kiev.ua/upload/iblock/ee5/dis_Pashynskyi_V.Yo.pdf (дата звернення: 25.06.2023).

107. Дручек О. М. Поняття адміністративно-правового забезпечення прав, свобод та інтересів дитини органами внутрішніх справ України. *Форум права*. 2013. № 2. С. 123–128. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2013_2_22.pdf (дата звернення: 25.06.2023).

108. Гомон Д.О. Адміністративно-правове та організаційне забезпечення охорони здоров'я в Україні: дис... канд. юрид. наук: 12.00.07. Одеса, 2018. 250 с.

109. Римарчук Г.С. Адміністративно-правове забезпечення права інтелектуальної власності: автореф. дис. ... канд. юрид. наук: 12.00.07. Львів, 2013. 18 с.

110. Циверенко Г.П. Адміністративно-правове забезпечення народного волевиявлення в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07. Запоріжжя, 2011. 21 с.

111. Марчук В.І. Адміністративно-правове забезпечення встановленого порядку управління в Україні органами внутрішніх справ: автореф. дис. … канд. юрид. наук: 12.00.07. Львів, 2011. 16 с.

112. Чистоклетов Л., Хитра О. Поняття адміністративно-правового забезпечення та його механізму. *Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки".* 2020. № 3 (27). С.173-180.

113. Адміністративне право України: монографія / за ред. В.В. Галунько.: Київ: Академія адміністративно-правових наук, 2020. 466 с.

114. Царенко С. І. Механізм адміністративно-правового забезпечення прикордонного режиму Державною прикордонною службою України. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2015. Вип. 5(3). С.83−86.

115. Ігонін Р. Проблема доктринального визначення поняття "адміністративно-правове забезпечення". *Вісник Національної академії прокуратури України*. 2015. № 2 (40). С. 37–43. URL: http://nbuv.gov.ua/UJRN/Vnapu_2015_2_7 (дата звернення: 25.06.2023).

116. Гумін О.М., Пряхін Є.В. Адміністративно-правове забезпечення: поняття та структура. *Наше право*. 2014. №4. С.46-50.

117. Сірко В. С. Поняття адміністративно-правового забезпечення волонтерської діяльності в Україні. *Правова просвіта*. 2018. № 8. URL: http://www.pravo.nayka.com.ua/?n=8&y=2018 (дата звернення: 25.06.2023).

118. Руснак Л.М. Адміністративно-правове забезпечення права на охорону здоров'я в Україні: дис. ... канд. юрид. наук : 12.00.07. Київ, 2016. 207 с.

119. Гресько В.І. Поняття та елементи адміністративно-правового забезпечення охорони здоров'я в Україні. *Юридичний науковий електронний журнал.* 2021. № 6. С.123-127. URL: http://www.lsej.org.ua/6_2021/35.pdf. DOIhttps://doi.org/10.32782/2524-0374/2021-6/33 (дата звернення: 25.06.2023).

120. Ярова А.Є. Адміністративно-правове забезпечення запобігання та врегулювання конфлікту інтересів у сфері охорони здоров'я: науково-

термінологічний пошук. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2021. № 67. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/250313 (дата звернення: 25.06.2023).

121. Кохановська О. В. Теоретичні проблеми інформаційних відносин у цивільному праві. Київ: Видавничо-поліграфічний центр «Київський університет», 2006. 463 с.

122. Мартинова А. М. Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних: дис. наукового ступеня доктора філософії: Київ, 2023. URL: https://ir.library.knu.ua/server/api/core/bitstreams/53528fda-67cc-4ef2-8ba6-326f67af8ce7/content (дата звернення: 25.06.2023).

123. Малаховська І. Б. Адміністративно-правове забезпечення захисту персональних даних в діяльності Національної поліції України: автореф. дис. канд. юрид. наук: Кривий Ріг, 2020. 21 с.

124. Лютіков П. С., Маслова А. Б. Гарантії забезпечення захисту персональних даних суб'єктами публічної адміністрації. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2023. № 10. URL: https://reicst.com.ua/pmtl/article/view/2023-10-01-06/2023-10-01-06. (дата звернення: 25.06.2023).

125. Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян: поняття та структура. *Наукові перспективи.* 2023. Випуск № 10(40). С. 678-688. URL: DOI: https://doi.org/10.52058/2708-7530-2023-10(40)-678-688 (дата звернення: 25.06.2023).

126. Адміністративне право: підручник / Ю.П. Битяк, В.М. Гаращук, В.В. Богуцький та ін.; за заг. ред. Ю.П. Битяка, В.М. Гаращука, В.В. Зуй. Харків: Право, 2013. 656 с.

127. Поняття та система суб'єктів публічного адміністрування. Тести на державну службу. URL: https://testderz.com/zno-pravo/admin-law-lecture (дата звернення: 25.06.2023).

128. Адміністративне право України. Повний курс: підручник / Галунько В., Діхтієвський П., Кузьменко О., Стеценко С. та ін. Херсон: ОЛДІ-ПЛЮС, 2018. 446 с.

129. Про Кабінет Міністрів України: Закон України від 27 лютого 2014 р. №794-VII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення: 25.06.2023).

130. Про центральні органи виконавчої влади: Закон України від 17 березня 2011 р. № 3166-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text (дата звернення: 25.06.2023).

131. Про місцеві державні адміністрації: Закон України від 09 квітня 1999 р. № 586-XIV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/586-14#Text (дата звернення: 25.06.2023).

132. Про військово-цивільні адміністрації: Закон України від 03 лютого 2015 р. № 141-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/141-19#Text (дата звернення: 25.06.2023).

133. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації / Верховна Рада України. URL: http://w1.c1.rada.gov.ua /pls/zweb2/webproc4_1?pf3511=72992 (дата звернення: 25.06.2023).

134. Духовна О. Захищені та здорові: як регламентується захист персональних даних пацієнтів в Україні. *Юридична газета онлайн*. URL: https://yur-gazeta.com/dumka-eksperta/zahishcheni-ta-zdorovi-yak-reglamentuetsya-zahist-personalnih-danih-pacientiv-v-ukrayini.htm (дата звернення: 25.06.2023).

135. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03 липня 2013 р. № 383-VII / Верховна Рада України. URL: https://web.archive.org/web/20150119014632 (дата звернення: 20.12.2022).

136. Про державну службу: Закон України від 10 грудня 2015 р. № 889-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/889-19#Tex. (дата звернення: 20.12.2022).

137. Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів: Закон України від 16 березня 2017 р. № 1951-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1951-19#Text (дата звернення: 20.12.2022).

138. Про поштовий зв'язок: Закон України від 03 листопада 2022 р. № 2722-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2722-20#Text (дата звернення: 20.12.2022).

139. Про офіційну статистику: Закон України від 16 серпня 2022 р. № 2524-IX // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2524-20#n61 (дата звернення: 20.12.2022).

140. Про державну реєстрацію геномної інформації людини: Закон України від 9 липня2022 р. № 2391-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text (дата звернення: 20.12.2022).

141. Про хмарні послуги: Закон України від 17 лютого2022 р. № 2075-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 20.12.2022).

142. Положення про Міністерство оборони України: Постанова Кабінету Міністрів України від 26 листопада 2014 р. № 671 / Верховна Рада України. URL: https://zakon.rada.gov.ua /laws/show/671-2014-%D0%BF#Text (дата звернення: 20.12.2022).

143. Порядок обробки і захисту персональних даних у Міністерстві оборони України: Наказ Міністерства оборони України 26 грудня 2014 р. № 926 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z0071-15#Text (дата звернення: 25.07.2023).

144. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. *Вісник Київського національного університету імені Тараса Шевченка. Серія*

*Військові науки*. 2022. № 4 (52). С. 50-53. URL: https://miljournals.knu.ua/index.php/visnuk/ article/view/1006/945 (дата звернення: 25.07.2023).

145. Положення про Міністерство у справах ветеранів: Постанова Кабінету Міністрів України від 27 грудня 2018 р. № 1175 (в редакції Постанови Кабінету Міністрів України від 15.04.2020р. № 276) / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1175-2018-%D0%BF#Tex (дата звернення: 25.07.2023).

146. Порядок обробки та захисту персональних даних, володільцем яких є Міністерство у справах ветеранів України: Наказ Міністерства у справах ветеранів України 20 липня 2021 р. № 159 / Верховна Рада України». URL: https://zakon.rada.gov.ua/laws/show/z1037-21#Text (дата звернення: 25.07.2023).

147. Положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 878 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF#Text (дата звернення: 25.07.2023).

148. Повідомлення про обробку персональних даних сервісом центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ «Єдине вікно для громадян». *Міністерства внутрішніх справ України. Офіційний сайт.* URL: https://services.mvs.gov.ua/personal_dat (дата звернення: 25.07.2023).

149. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів: Постанова Кабінету Міністрів України від 14 листопада 2018 р. № 1024 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#Text. (дата звернення: 25.07.2023).

150. Положення про Адміністрацію Державної прикордонної служби України: Постанова Кабінету Міністрів України від 16 жовтня2014 р. № 533 /

Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/533-2014-%D0%BF#Text (дата звернення: 25.07.2023).

151. Про Національну гвардію України: Закон України від 13 березня 2014 р. № 876-VII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/876-18#Text (дата звернення: 25.07.2023).

152. Державна міграційна служба України. Загальна інформація. URL: https://dmsu.gov.ua/pro-dms/zagalna-informacziya.html (дата звернення: 25.07.2023).

153. Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua/laws/main/580-19 (дата звернення: 25.07.2023).

154. Костенко І. В. Проблеми правового захисту персональних даних у діяльності Національної поліції. *Юридичний часопис Національної академії внутрішніх справ.* 2018. № 1 (15). С. 296–302.

155. Заярний О. Адміністративна деліктність у сфері використання персональних даних та засоби її запобігання. *Вісник Київського національного університету імені Тараса Шевченка. Серія «Юридичні науки».* 2013. Вип. 95. С. 57–63.

156. Шадська У. Захист персональних даних в діяльності Національної поліції України. URL: https://ecpl.com.ua/comments/zahyst-personalnyh-danyh-v-diyalnosti-natsionalnoji-politsiji-ukrajiny/ (дата звернення: 25.07.2023).

157. Михайлова В. Безстрокове зберігання в поліцейській базі біометричних даних неприпустиме ЄСПЛ. *Газета «Закон і бізнес».* URL: https://zib.com.ua/ua/141566-bezstrokove_zberigannya_v_policeyskiybazi_biometrichnih_dan.html (дата звернення: 25.07.2023).

158. Клімушин П.С., Бєляєва Є.Г. Захист персональних даних в діяльності національної поліції України. *Харківський гаціональний університет внутрішніх справ.* URL: https://univd.edu.ua/general/publishing/konf/18_12_2019/pdf/14.pdf (дата звернення: 25.07.2023).

159. Заярний О. До питання щодо забезпечення правомірної обробки біометричних даних в діяльності національної поліції національні та міжнародні стандарти. *Юридичний вісник* 2021. № 6. С. 160–164. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/2278/2552 (дата звернення: 25.07.2023).

160. Найдюк Н. Зниклі безвісти: як і де шукати військового, з яким втратили зв'язок. *Українська правда*. URL: https://life.pravda.com.ua/society/2023/02/20/252916/ (дата звернення: 25.07.2023).

161. В Україні запрацював реєстр зниклих безвісти. *Українська правда*. URL: https://www.pravda.com.ua/news/2023/05/2/7400268/ (дата звернення: 25.07.2023).

162. Павлюк А. Скільки українців є зниклими безвісти? Дані від омбудсмена. *Українська правда*. URL: https://life.pravda.com.ua/society/v-ukrajini-37-tisyach-lyudey-vvazhayutsya-zniklimi-bezvisti-ombudsmen-301092/#:~:text=%D0%92%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96%20%D0%BC%D0%B0%D0%B9%D0%B6%D0%B5%2037%20%D1%82%D0%B8%D1%81%D1%8F%D1%87,%D0%B7%20%D0%BF%D1%80%D0%B0%D0%B2%20%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8%20%D0%94%D0%BC%D0%B8%D1%82%D1%80%D0%B0%20%D0%9B%D1%83%D0%B1%D1%96%D0%BD%D1%86%D1%8F (дата звернення: 25.07.2023).

163. Положення про Міністерство охорони здоров'я України: Постанова Кабінету Міністрів України від 25 березня 2015 р. № 267. (в редакції постанови Кабінету Міністрів України від 24 січня 2020 № 90) / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/267-2015-%D0%BF#Text (дата звернення: 25.07.2023).

164. Деякі питання електронної системи охорони здоров'я: Постанова Кабінету Міністрів України від 25 квітня 2018 № 411. URL:

https://zakononline.com.ua/documents/show/373528_757283 (дата звернення: 25.07.2023).

165. Цифрова трансформація системи охорони здоров'я. *Електронна система охорони здоров'я в Україні*. URL: https://ehealth.gov.ua (дата звернення: 25.07.2023).

166. Про захищеність персональних даних пацієнта в ЕСОЗ. *Vikisoft.* URL: https://vikisoft.kiev.ua/nhealth/pro-zahishenist-personalnih-danih-paciyenta-v-esoz/. (дата звернення: 25.07.2023).

167. НСЗУ розповіла, як проводить верифікацію даних в ЕСОЗ. *Медична справа*. URL: https://medplatforma.com.ua/news/66902-nszu-rozpovila-yak-provodit-verifikatsiyu-danikh-v-esoz (дата звернення: 25.07.2023).

168. Пунда О.О. Арзянцева Д.А., Захаркевич Н.П. Організаційно-правові засади формування електронної системи охорони здоров'я з умовах проведення медичної реформи. *Наука, технології, інновації*. 2020. №2(14) С. 67–73.

169. Положення про Міністерство юстиції України: Постанова Кабінету Міністрів України від 02 липня 2014 р. № 228 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/228-2014-%D0%BF#n8 (дата звернення: 25.07.2023).

170. Положення про Міністерство фінансів України: Постанова Кабінету Міністрів України від 20 серпня 2014 р. № 375 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/375-2014-%D0%BF#Text (дата звернення: 25.07.2023).

171. Положення про Міністерство освіти і науки України: Постанова Кабінету Міністрів України від 16 жовтня 2014 р. № 630 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/630-2014-%D0%BF#Text (дата звернення: 25.07.2023).

172. Про затвердження положень про реєстри Єдиної державної електронної бази з питань освіти: Наказ Міністерства освіти і науки України від 16 лютого 2021 р. № 204**.** України від / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z0536-21#Text (дата звернення: 25.07.2023).

173. Положення про Міністерство цифрової трансформації України: Постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856 / Верховна Рада України. URL: https://zakon.rada.gov.ua /laws/show/856-2019-%D0%BF#n12 (дата звернення: 25.07.2023).

174. Порядок обробки та захисту персональних даних, володільцем яких є Міністерство цифрової трансформації України: Наказ Міністерства цифрової трансформації України від 20 травня 2020 р. № 72 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z0495-20#Text (дата звернення: 25.07.2023).

175. Малинка А. Захист персональних даних на рівні місцевих громад у воєнний час. *Простір.* URL: https://www.prostir.ua/?blogs=zahyst-personalnyh-danyh-na-rivni-mistsevyh-hromad-u-vojennyj-chas (дата звернення: 25.07.2023).

176. Титикало Р.С. «Власні» та «делеговані» повноваження місцевого самоврядування. *Наукові записки: Серія право*. 2023. № 14. С. 123-127. URL: https://pravo.cuspu.edu.ua/index.php/pravo/article/view/269/271 (дата звернення: 25.07.2023).

177. Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08 січня 2014 р. № 1/02-14 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 20.12.2022).

178. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Наказ Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 р. № 1/02-14. / Верховна Рада України. URL: https://ombudsman.gov.ua/uk/oprilyudnennya-informaciyi-na-vimogu-statti-9-ta-

24-zakonu-ukrayini-pro-zahist-personalnih-danih/poryadok-ta-formi-zdijsnennya-povidomlen-dodatkova-informaciya (дата звернення: 20.12.2022).

179. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 р. № 1/02-14. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14/paran92#n92. (дата звернення: 20.12.2022).

180. Адміністративне право України: підручник / П. Діхтієвський, Ю. Ващенко, Н. Задирака, В. Пашинський, В. Клинчук та ін; за заг. ред. П. Діхтієвського. Київ. «Видавництво Людмила», 2023. 772 с.

181. Примаков К. Сучасні підходи до розуміння інструментів діяльності публічної адміністрації. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 4 (119). С.188-193. URL:https://er.dduvs.in.ua/bitstream/123456789/11040/1/27.pdf. (дата звернення: 20.12.2022).

182. Резніченко В.О. Поняття та класифікація інструментів публічного адміністрування забезпечення вищої освіти в Україні. *Науковий вісник публічного та приватного права.* 2021. Вип. 5. Том. 2.С. 115-120. URL: http://www.nvppp.in.ua/vip/2021/5/part_2/20.pdf (дата звернення: 20.12.2022).

183. Михайловська О.В. Формування взаємодії в системі публічного управління на засадах партнерства. *Наукові перспективи. Серія: Державне управління*. 2020. № 6 (6). С. 169–174. DOI: https://doi.org/10.32689/2708-7530-2020-6(6)-169-174 (дата звернення: 25.07.2023).

184. Жуков М. С. Форми та методи адміністративно-правового регулювання чи інструменти діяльності публічної адміністрації: порівняльний аналіз. *Юридичний науковий електронний журнал*. 2020. № 2. URL: http://lsej.org.ua/2_2020/57.pdf. (дата звернення: 25.07.2023).

185. Правоторова О. Форми адміністративної діяльності публічної адміністрації в механізмі адміністративно-правової охорони. *Актуальні проблеми вітчизняної юриспруденції*. 2019. № 5. С. 123–127.

186. Сукманова О. Публічне адміністрування охорони права власності в Україні : дис. … докт. юрид. наук: Київ, 2019. 559 с.

187. Мельник Р.С., Бевзенко В.М. Загальне адміністративне право: навчальний посібник / за заг. ред. Р.С. Мельника. Київ: Ваіте, 2014. 376 с.

188. Патерило І. Інструменти діяльності публічної адміністрації: сутність та зміст. *Науковий вісник Ужгородського національного університет. Серія «Право».* 2014. Ви. 27. Т. 2. С. 174–178.

189. Толкованов В. В. Розвиток і впровадження інструментів політики державного управління: вітчизняний та зарубіжний досвід. *Демократичне врядування*. 2013. Вип. 12. URL: http://nbuv.gov.ua/UJRN/DeVr_2013_12_29 (дата звернення: 25.07.2023).

190. Кравцова Т.М. Інструменти публічного адміністрування у сфері державної допомоги суб'єктам господарювання. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Юридичні науки*. 2020. Том 31 (70). Ч. 2. № 2. С. 80–84.

191. Кількість платників податків зросла на 60 тис. *Укрінформ.* URL: https://www.ukrinform.ua/rubric-economy/3124729-kilkist-subektiv-pidpriemnickoi-dialnosti-zrosla-na-60-tisac-lubcenko.html (дата звернення: 25.04.2024).

192. Про адміністративну процедуру: Закон України від 17 лютого 2022 р. № 2073-IX / Верховна Рада України. URL:https://zakon.rada.gov.ua/laws/show/2073-0?find=1&text=%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%96+%D0%B4%D0%B0%D0%BD%D1%96#w1_1 (дата звернення: 25.04.2024)

193. Жиляєв І. Б. Інструменти державного стратегічного управління: Національна програма інформатизації. *Інформація і право*. 2018. № 1. С. 44–58.

194. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20 листопада 2012 р. № 5492-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення 25.07.2023).

195. Положення про технічний захист інформації в Україні: Затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/ 1229/99#Text (дата звернення 25.07.2023).

196. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. 2014. Т. 7, № 2. С. 73–82.

197. Report on the initial assessment of the progress in the implementation of the European Union legal Acts (EU ACQUIS). *Кабінет Міністрів України.* URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/Zvit_EN.pdf (дата звернення 25.07.2023).

198. Ukraine 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels, 8.11.2023 SWD (2023) 699 final. *European Neighbourhood Policy and Enlargement Negotiation*s. URL:https://neighbourhood-enlargement.ec.europa.eu/ system/files/2023-11/SWD_2023_699%20Ukraine%20report.pdf (дата звернення: 20.11.2023).

199. Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. *Кабінет Міністрів України.* URL: https://www.kmu.gov.ua/en/yevropejska-integraciya/ugoda-pro-asociacyu /https:.eurlex.europa.eu/legalcontent/EN/TXT/?qid=1413961918333&uri=CELEX: 22014A0529%2801%29 (дата звернення: 25.07.2023).

200. Баранов О. А., Брижко В. М. Захист персональних даних в сфері інтернет речей. *Інформація і право.* 2016. № 2. С. 85-91.

201. Case of Leander v. Sweden, App. №. 9248/81. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-57519 (дата звернення: 20.11.2023).

202. Case of Amann v. Switzerland, App. №. 27798/95. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-58497 (дата звернення: 20.11.2023).

203. Case of Rotaru v. Romania, App. №. 28341/95. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-58586 (дата звернення: 20.11.2023).

204. Case of Gaskin v. The United Kingdom, App. №. 10454/83. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-57491 (дата звернення: 20.11.2023).

205. Case of K.H. and others v. Slovakia, App. №. 32881/04. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-145421 (дата звернення: 20.11.2023).

206. Case of Haralambie v. Romania, App. №. 21737/03. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=002-1286 (дата звернення: 20.11.2023).

207. Case of Odievre v. France, App. №. 42326/98. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-60935 (дата звернення: 20.11.2023).

208. Case of Ciubotaru v. Moldova, App. №. 27138/04. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-98445 (дата звернення: 20.11.2023).

209. Case of Segerstedt-Wiberg and others v. Sweden, App. №. 62332/00. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-125941 (дата звернення: 20.11.2023).

210. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.

211. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. 2016. № 3. С. 45-57.

212. Kanstantsin Dzehtsiarou. *European Consensus and the Legitimacy of the European Court of Human Rights.* Cambridge University Press. 2015. 230 p.

213. Діхтієвський П.В., Задирака Н.Ю. Контроль за додержанням законодавства про захист персональних даних Уповноваженого Верховної Ради України з прав людини. *Юридичний науковий електронний журнал*. 2024. № 1. С. 45–56.

214. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція від 28 січня 1981 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 25.07.2023).

215. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance). *Eur-lex.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807&qid=1673276776969#ntr1-L_2018303EN.01005901-E0001 (дата звернення: 25.07.2023).

216. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). *Eur-lex.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid= 1672950557346. (дата звернення: 25.07.2023).

217. Кабанов О., Олексіюк Т. Відповідність законодавства України окремим положенням правового регулювання сфери відкритих даних у Європейському Союзі. Аналітичний звіт. Міністерство цифрової трансформації України URL: https://data.gov.ua/uploads/files/2023-07-03-093206.832183.pdf (дата звернення: 25.07.2023).

218. Kelvin Chan. Europe reaches a deal on the world's first comprehensive AI rules. *Aapnews.* URL: https://apnews.com/article/ai-act-europe-regulation-59466a4d8fd3597b04542ef25831322c (дата звернення: 14.04.2024).

219. Європарламент схвалив закон про штучний інтелект. *Збруч.* URL: https://zbruc.eu/node/117949 (дата звернення: 14.04.2024).

220. Італія першою із західних країн заблокувала ChatGPT. *Українська правда*. URL: https://www.pravda.com.ua/news/2023/03/31/7395927/ (дата звернення: 25.07.2023).

221. Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. *Garante Per La protezione dei dati personali.* URL: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870847 (дата звернення: 25.07.2023).

222. Пилипів І. Країни G7 виступають за прийняття законів для регулювання ШІ. *Українська правда*. URL: https://www.epravda.com.ua/news/2023/04/30/699615/ (дата звернення: 25.07.2023).

223. Пунда О.О., Арзянцева Д.А. Забезпечення захисту персональних даних фізичних осіб в умовах розвитку штучного інтелекту. *Наука і техніка перспективи*. *Серія «Право, економіка, педагогіка, техніка, фізико-математичні науки».* 2024. № 2(30). С.132–143.

224. Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 rev.01. *Newsroom*. URL: https://ec.europa.eu/newsroom/article29/items/612052 (дата звернення: 25.07.2023).

# ДОДАТКИ

## ДОДАТОК 1

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Цьоменко А. В. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 1 (53), 2023. Київ, С 41-45. URL:https://miljournals.knu.ua/index.php/visnuk/article/view/1028/955 (дата звернення 25.04.2024 р.)
2. Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян : поняття та структура. Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія» ) Випуск № 10(40) 2023. С. 678-688. DOI: https://doi.org/10.52058/2708-7530-2023-10(40)-678-688.
3. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 4 (52), 2022. Київ, С. 50-53. URL:https://miljournals.knu.ua/index.php/visnuk/article/view/1006/945. (дата звернення 25.07.2023 р.)
4. Pashynskyi Volodymyr, Tsomenko Alina. Administrative-legal support for the protection of citizens personal data: contemporary theoretical approaches. Visegrag journal on human rights № 4 (2023) P. 55 -61.

які засвідчують апробацію матеріалів дисертації:

1. Цьоменко А.В. Захист персональних даних органами публічної влади в умовах війни. Права людини та публічне врядування в сучасних умовах : Матеріали V Міжнародного правничого форуму, 10 червня 2022 р., м. Чернівці / Уклад. І.В. Ковбас, І.І. Бабін, О.І. Ющик, І.Ж. Торончук, П.І. Крайній. Чернівці: Технодрук, 2022. С.268-270.

2. Цьоменко А.В. Європейська рада щодо захисту персональних даних, як незалежний орган спеціальної компетенції європейського союзу. Права людини як індикатор розвитку сучасної держави: матеріали Міжнародної науково-практичної конференції (13 грудня 2021 року) / За ред. О. Васильченко; Є. Герасименко, О. Сінькевич, А. Матат. Київський національний університет імені Тараса Шевченка. Київ: «Видавництво Людмила», 2021. С.209-211.

3. Цьоменко А.В. Забезпечення захисту персональних даних військовослужбовців в умовах війни. Адаптація правової системи України до Європейського союзу: теоретичні та практичні аспекти Всеукраїнська науково-практична конференція з нагоди 20-ї річниці заснування Полтавського юридичного інституту Національного юридичного університету імені Ярослава Мудрого (29 вересня 2022 року) Полтава: зб.наук.пр./ укладачі В.М. Божко, П.П. Нога. С. 308-310.

4. Цьоменко А.В. Публічно-правовий контроль за обігом персональних даних як засіб захисту від зловживання правом. Актуальні питання розвитку юридичної науки і практики в умовах воєнного стану та мирної розбудови: матеріали Міжнародної науково-практичної конференції (5 травня 2023 року): ел. збірник. Київ: Київський національний університет імені Тараса Шевченка, 2023., С.241-243.

5. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян у контексті використання програм «штучного інтелекту» VI Міжнародно правовий форму Права людини та публічне врядування в сучасних умовах: матеріали V Міжнародного правничого форуму (10 червня 2022) м.

Чернівці/ Уклад. І.В. Ковбас, І.І. Бабін, О.І. Ющик, І.Ж. Торончук, П.І. Крайній,. Чернівці: Технодрук, 2022. С. 237-240.

6. Пашинський В.Й., Цьоменко А.В. Міжнародно-правовій звичай у сфери захісту персональних даних. Актуальні питання державотворення та захисту прав людини в Україні: зб. наук. пр. / гол. ред. Л. Г. Білий. Хмельницький: Вид-во Хмельниц. ін-ту МАУП, 2024. Вип. 13. 249-255 с.

7. Цьоменко Аліна. Європейські стандарти адміністративно-правового забезпечення захисту персональних даних громадян: Публічна влада: проблеми реалізації повноважень в умовах воєнного стану та відбудовного періоду. Матеріали Міжнародної науково-практичної конференції (22 лютого 2024 року): електр. збірник / Ред. кол.: О. Васильченко; П. Діхтієвський; Т. Коломоєць; А. Мамула; В. Мушенок; В. Пашинський. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 134-139.

8. Цьоменко Аліна, Цьоменко Алла. Публічна інформація як важливий ресурс та результат процесу адміністрування. Матеріали Міжнародної науково-практичної конференції (22 лютого 2024 року): електр. збірник / Ред. кол.: О. Васильченко; П. Діхтієвський; Т. Коломоєць; А. Мамула; В. Мушенок; В. Пашинський. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 371-374.

# ДОДАТОК 2

**ДОВІДКА**
**про впровадження результатів дисертаційного дослідження Цьоменко Аліни Володимирівни на тему: «Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації»**

Видана аспірантці Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Цьоменко Аліні Володимирівні про те, що результати її дисертаційної роботи на тему: «Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації» за спеціальністю 081 Право були використані при обговоренні та підготовці ряду законодавчих ініціатив в Комітеті Верховної Ради України з питань фінансів, податкової та митної політики, зокрема, щодо :

1. Вдосконалення адміністративно-правового механізму забезпечення захисту персональних даних платників податків, які використовуються контролюючими органами при адмініструванні податків, зборів, платежів та проведенні податкового контролю відповідно до положень Податкового кодексу України.

2. Вдосконалення адміністративно-правового механізму забезпечення захисту персональних даних щодо підприємств, громадян , а також товарів, транспортних засобів комерційного призначення, що переміщуються ними через митний кордон України, що збирається, використовується та формується митними органами відповідно до Митного кодексу України.

3. Вдосконалення адміністративно-правового механізму забезпечення захисту персональних даних щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним, або стала відомою третім особам при наданні послуг банку.

Керівник секретаріату Комітету
Верховної Ради України з питань
фінансів, податкової та митної політики Прийма І.М.

Управління кадрів
Апарату Верховної Ради України

# ДОДАТОК 3

ЗАТВЕРДЖУЮ
Начальник Військового інституту
Київського національного університету
імені Тараса Шевченка
бригадний генерал
Анатолій ШЕВЧЕНКО
"15" 04 2024 року

**АКТ**
**впровадження результатів дисертаційної роботи**
**Цьоменко Аліни Володимирівни**
**на тему: "Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації"**
**у навчальний процес Військового інституту**
**Київського національного університету імені Тараса Шевченка**

Комісія у складі голови - заступника начальника військового факультету міжнародних відносин та права з навчальної роботи підполковника Полтавського М.В., членів - начальника кафедри інформаційно-аналітичних технологій військового факультету міжнародних відносин та права полковника Степанишина Р.Д., начальника кафедри військового права військового факультету міжнародних відносин та права полковника юстиції Коропатніка І.М., начальника кафедри спеціальної мовної підготовки військового факультету міжнародних відносин та права полковника Гончарук Л.М., склала даний акт про те, що розроблені за наслідками дисертаційної роботи асистента кафедри адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Цьоменко Аліни Володимирівни наукові висновки і пропозиції використовуються у навчальному процесі у Військовому інституті Київського національного університету імені Тараса Шевченка при викладанні наступних навчальної дисципліни: "Правова робота у Збройних Силах України", де у якості рекомендованих джерел подані наступні публікації автора:

**Монографії:**

1. Цьоменко А.В. «Генеза нормативно-правового забезпечення захисту персональних даних громадян»: монографія / за заг. ред. П.Діхтієвського, В. Пашинського. Рига, Латвія: "Baltijf Publishing" 2022. С.941-973.

**Наукові статті:**

2. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни.

*Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки.* № 4 (52), 2022. Київ, С. 50-53 .

3. Цьоменко А. В. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. *Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки.* № 1 (53), 2023. Київ, С 41-45.

4. Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян: поняття та структура Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія» ) Випуск № 10(40) 2023. С. 678-688. DOI: https://doi.org/10.52058/2708-7530-2023-10(40)-678-688

5. Pashynskyi Volodymyr, Tsomenko Alina. ADMINISTRATIVE-LEGAL SUPPORT FOR THE PROTECTION OF CITIZENS PERSONAL DATA: CONTEMPORARY THEORETICAL APPROACHES. VISEGRAG JOURNAL ON HUMAN RIGHTS № 4 (2023) p. 55 -61.

**ВИСНОВОК:** результати дисертаційної роботи асистента кафедри адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Цьоменко Аліни Володимирівни на тему: " Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації" вважати впровадженим в навчальний процес Військового інституту Київського національного університету імені Тараса Шевченка та такими, що актуалізують питання викладені в матеріалах дисциплін кафедри щодо адміністративно-правового забезпечення правового режиму воєнного стану та сприятимуть якісній підготовці військових юристів за спеціальністю "Правоохоронна діяльність у Збройних Силах України".

Голова комісії:
Заступник начальника військового факультету міжнародних відносин та права з навчальної роботи
підполковник Микола ПОЛТАВСЬКИЙ

Члени комісії:
Начальник кафедри інформаційно-аналітичних технологій військового факультету міжнародних відносин та права
полковник Руслан СТЕПАНИШИН

Начальник кафедри військового права військового факультету міжнародних відносин та права
полковник юстиції Ігор КОРОПАТНІК

Начальник кафедри спеціальної мовної підготовки військового факультету міжнародних відносин та права
полковник Лілія ГОНЧАРУК

# ДОДАТОК 4

**ЗАТВЕРДЖУЮ**
Начальник факультету забезпечення
державної безпеки Київського інституту
Національної гвардії України
доктор юридичних наук, професор
полковник
**Олександр КОБЗАР**
«27» 04 2024 року

**АКТ**
**впровадження результатів дисертаційного дослідження Цьоменко Аліни Володимирівни на тему: «Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації»**

Комісія у складі: голови - заступника начальника факультету забезпечення державної безпеки з навчальної та наукової роботи - начальника навчальної частини, доктора юридичних наук, професора Комісарова О.Г., начальника кафедри правового забезпечення діяльності НГУ, кандидата юридичних наук, доцента Волуйка О.М., начальника кафедри державної безпеки, кандидата юридичних наук, доцента Комісарової Н.О. цим актом засвідчили, що результати дисертаційного дослідження Цьоменко Аліни Володимирівни на тему: «Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації» впровадженні в освітній процес кафедра державної безпеки і правового забезпечення діяльності НГУ щодо підготовки фахівців у галузях знань 08 Право та 25 Воєнні науки, державна безпека, безпека державного кордону, за освітніми програмами першого бакалаврського рівня «Правове забезпечення службово-бойової діяльності частин та підрозділів НГУ», «Забезпечення державної безпеки підрозділами НГУ» та використовуються у науково-дослідній діяльності факультету.

У списку літератури у робочих програмах та навчально-методичних комплексах дисциплін рекомендовано опрацювання наступних наукових праць Цьоменко А.В. :

**Публікації:**

1) Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 4 (52), 2022. Київ, С. 50-53 .

2) Цьоменко А.В. «Генеза нормативно-правового забезпечення захисту персональних даних громадян»: Концептуальні засади розвитку вітчизняного адміністративного права та процесу: тенденції, перспективи, практика : колективна монографія / Є. Герасименко, П. Діхтієвський, Н. Задирака,Т. Коломоєць, В. Клинчук та ін.; за заг. ред. П. Діхтієвського, В. Пашинського. Рига, Латвія : "Baltija Publishing", 2022. С. 941-973.

3) Цьоменко А. В. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 1 (53), 2023. Київ, С. 41-45.

4) Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян: поняття та структура Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія» ) Випуск № 10(40) 2023. С. 678-688.

5) Pashynskyi Volodymyr, Tsomenko Alina. Administrative-legal support for the protection of citizens personal data: contemporary theoretical approaches VISEGRAD JOURNAL ON HUMAN RIGHTS № 4 (2023) P. 55 -61.

**Тези:**

1) Цьоменко А.В. Захист персональних даних органами публічної влади в умовах війни.Права людини та публічне врядування в сучасних умовах : Матеріали V Міжнародного правничого форуму, 10 червня 2022 р., м. Чернівці/ Уклад. І.В. Ковбас, І.І. Бабін, О.І. Ющик, І.Ж. Торончук, П.І. Крайній. Чернівці: Технодрук, 2022. С. 268-270.

2) Цьоменко А.В. Європейська рада щодо захисту персональних даних, як незалежний орган спеціальної компетенції європейського союзу. Права людини як індикатор розвитку сучасної держави: матеріали Міжнародної науково-практичної конференції (13 грудня 2021 року) / За ред. О. Васильченко; Є. Герасименко, О. Сінькевич, А. Матат. Київський національний університет імені Тараса Шевченка. Київ: «Видавництво Людмила», 2021. С. 209-211.

3) Цьоменко А.В. Забезпечення захисту персональних даних військовослужбовців в умовах війни. Адаптація правової системи України до Європейського союзу: теоретичні та практичні аспекти Всеукраїнська науково-практична конференція з нагоди 20-ї річниці заснування Полтавського юридичного інституту, С. 308-310.

4) Цьоменко А.В. Публічно-правовий контроль за обігом персональних даних як засіб захисту від зловживання правом. матеріали Міжнародної науково-практичної конференції «Актуальні питання розвитку юридичної науки і практики в умовах воєнного стану та мирної розбудови», С. 241-243.

5) Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян у контексті використання програм «штучного

інтелекту» VIМіжнародно правовий форму «Права людини та публічне врядування в сучасних умовах», С. 237-240.

6) Пашинський В.Й.,Цьоменко А.В. Міжнародно-правовій звичай у сфери захисту персональних даних . Актуальні питання державотворення та захисту прав людини в Україні: зб. наук. пр. / гол. ред. Л. Г. Білий. Хмельницький : Вид-во Хмельниц. ін-ту МАУП, 2024. Вип. 13. С. 249-255.

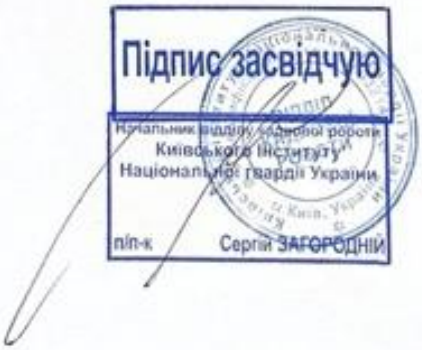
7) Цьоменко Аліна. Європейські стандарти адміністративно-правового забезпечення захисту персональних даних громадян: Публічна влада: проблеми реалізації повноважень в умовах воєнного стану та відбудовного періоду. Матеріали Міжнародної науково-практичної конференції (22 лютого 2024 року): електр. збірник / Ред. кол.: О. Васильченко; П. Діхтієвський; Т. Коломоєць; А. Мамула; В. Мушенок; В. Пашинський;. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 134-139.

8) Цьоменко Аліна, Цьоменко Алла. Публічна інформація як важливий ресурс та результат процесу адміністрування. Матеріали Міжнародної науково-практичної конференції (22 лютого 2024 року): електр. збірник / Ред. кол.: О. Васильченко; П. Діхтієвський; Т. Коломоєць; А. Мамула; В. Мушенок; В. Пашинський;. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 371-374.

**Голова комісії:**
**полковник**
**« __ » _____ 2023 року** **Олександр КОМІСАРОВ**

**Члени комісії:**
**полковник**
**« __ » _____ 2023 року** **Олексій ВОЛУЙКО**

**полковник**
**« __ » _____ 2023 року** **Наталія КОМІССАРОВА**



# ДОДАТОК 5

ЗАТВЕРДЖУЮ
Директор
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
**Оксана ВАСИЛЬЧЕНКО**
"01" 05 2024 року

**АКТ**
**впровадження результатів дисертаційної роботи аспірантки кафедри адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Цьоменко Аліни Володимирівни на тему: " Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації" у навчальний процес Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка**

Комісія у складі голови - доктора юридичних наук, професора, завідувача кафедри адміністративного права та процесу Діхтієвського П.В, членів – доктора юридичних наук, доцента, доцента кафедри адміністративного права та процесу Пашинського В.Й., доктора юридичних наук, професора, професора кафедри адміністративного права та процесу Мушенка В.В. склали даний акт про те, що розроблені за наслідками дисертаційної роботи асистента кафедри адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Цьоменко Аліни Володимирівни наукові висновки і пропозиції використовуються у навчальному процесі у Навчально-науковому інституті права Київського національного університету імені Тараса Шевченка при викладанні наступних навчальних

дисциплін: «Електронне урядування і права людини», «Права громадян та система їх захисту у публічному адмініструванні (публічному управлінні)», «Військово- адміністративне право: сучасні проблеми розвитку» , де у якості рекомендованих джерел подані наступні публікації автора:

**Монографії:**

1. Цьоменко А.В. «Генеза нормативно-правового забезпечення захисту персональних даних громадян»: монографія / за заг. ред. П.Діхтієвського, В. Пашинського. Рига, Латвія: "Baltijf Publishing" 2022. С.941-973.

**Наукові статті:**

2. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 4 (52), 2022. Київ, С. 50-53 .

3. Цьоменко А. В. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 1 (53), 2023. Київ, С 41-45.

4. Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян: поняття та структура Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія» ) Випуск № 10(40) 2023. С. 678-688. DOI: https://doi.org/10.52058/2708-7530-2023-10(40)-678-688

5. Pashynskyi Volodymyr, Tsomenko Alina. Administrative-legal support for the protection of citizens personal data: contemporary theoretical approaches. Visegrad journal on human rights № 4 (2023) p. 55 -61.

**ВИСНОВОК:** результати дисертаційної роботи аспірантки кафедри адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Цьоменко

Аліни Володимирівни на тему: «Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації» вважати впровадженим в навчальний процес Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка та такими, що актуалізують питання викладені в матеріалах дисциплін кафедри адміністративного права та процесу та сприятимуть якісній підготовці здобувачів за спеціальністю «081 Право».

Затверджено на засіданні кафедри адміністративного права та процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка №9 від 24.04.2024.

**Голова Комісії:**
Завідувач кафедри адміністративного права
та процесу,
д.ю.н., професор **Петро ДІХТІЄВСЬКИЙ**

**Члени комісії:**
Доцент кафедри адміністративного права
та процесу,
д.ю.н., доцент **Володимир ПАШИНСЬКИЙ**

Професор кафедри адміністративного права
та процесу
д.ю.н., професор **Віктор МУШЕНОК**