

Інформаційне право

УДК 342:351(477)

ПИЛИПЧУК В.Г., доктор юридичних наук, професор, дійсний член (академік)
Національної академії правових наук України
ORCID: <https://orcid.org/0009-0008-5691-6823>

**ТЕОРЕТИКО-ПРАВОВІ ПРОБЛЕМИ РОЗВИТКУ ЗАКОНОДАВСТВА У СФЕРІ
НАЦІОНАЛЬНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ**DOI: [https://doi.org/10.37750/2616-6798.2025.2\(53\).334015](https://doi.org/10.37750/2616-6798.2025.2(53).334015)

Анотація. У запропонованій статті розглядається комплекс актуальних теоретичних та прикладних проблем щодо розвитку національного законодавства у сфері національної та інформаційної безпеки України. Висвітлено історико-правові засади трансформації моделей законодавчого регулювання у сфері національної безпеки наприкінці XX – на початку XXI століття та визначено першочергові заходи щодо розвитку національного законодавства з цих питань згідно з вимогами Конституції України. Також розглянуто комплекс актуальних проблем у сфері захисту інформаційної безпеки та розроблено конкретні пропозиції щодо внесення змін до Закону України “Про національну безпеку України”, надано пропозиції щодо концептуальних положень підготовки законопроекту “Про інформаційну безпеку України”. В контексті євроінтеграції України розглянуто основні стандарти та вимоги законодавства ЄС з питань інформаційної безпеки людини, зокрема захисту персональних даних та приватності життя людини. Крім цього, виокремлено базові принципи та надано системні пропозиції щодо розбудови нової моделі системи захисту персональних даних в Україні та розвитку національного законодавства у цій сфері відповідно до стандартів країн-членів Європейського Союзу.

Ключові слова: законодавство, національна безпека, інформаційна безпека, захист даних, персональні дані, приватність життя людини.

Summary. The article considers a set of topical theoretical and applied problems regarding the development of national legislation in the field of national and information security of Ukraine. The historical and legal principles of the transformation of models of legislative regulation in the field of national security in the late 20th - early 21st centuries are highlighted and priority measures for the development of national legislation on these issues are identified in accordance with the requirements of the Constitution of Ukraine. A set of topical problems in the field of information security protection is also considered and specific proposals are developed for amending the Law of Ukraine "On National Security of Ukraine", proposals are provided for the conceptual provisions for the preparation of the draft law "On Information Security of Ukraine". In the context of Ukraine's European integration, the main standards and requirements of EU legislation on human information security, in particular the protection of personal data and the privacy of human life, are considered. In addition, basic principles are identified and systemic proposals are provided for the development of a new model of the personal data protection system in Ukraine and the development of national legislation in this area in accordance with the standards of the European Union member states.

Keywords: legislation, national security, information security, data protection, personal data, privacy of human life

Постановка проблеми. В сучасних умовах глобальних міжнародно-правових трансформацій змінюється політика практично усіх країн-членів ЄС і НАТО, а також

роль і місце військово-політичних механізмів забезпечення безпеки й оборони. З геополітичної точки зору нова інформаційна ера, процеси цифрової трансформації, практика протидії інформаційній та збройній агресії РФ проти України кардинально змінює традиційні уявлення про символи могутності й способи досягнення світового панування, що були характерними у попередні століття. Нині розпочато формування нових систем національної, європейської та міжнародної безпеки, що мають включати усі наявні безпекові інститути за чіткого розподілу їх функцій і повноважень. Відповідно, потребує системного перегляду і розвитку національне законодавство у сфері національної та інформаційної безпеки.

Метою статті є висвітлення теоретико-правових проблем розвитку законодавства у сфері національної та інформаційної безпеки України, передусім щодо проблем визначення моделі законодавчого регулювання у сфері національної безпеки, розвитку законодавства у сфері інформаційної безпеки, зокрема, підготовки змін до чинного законодавства, а також проблем правового регулювання з питань захисту персональних даних та приватності життя людини в контексті вимог законодавства Європейського Союзу.

Виклад основного матеріалу.

1. Проблема визначення моделі законодавчого регулювання у сфері національної безпеки України.

Історія становлення законодавства з питань національної безпеки свідчить, що основними системними правовими актами у цій сфері стали Конституція України (1996 р.), Закон України “Про основи національної безпеки України” (2003 р.), а також Закон “Про національну безпеку України” (2018 р.). В контексті системного аналізу варто звернути увагу на основні підходи щодо виокремлення сфер забезпечення національної безпеки у вказаних правових актах. Зокрема, відповідно до частин 1, 2, 3 ст. 17 Конституції України передбачено наступне [1]:

«Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України.

Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом”.

Тобто, згідно зі статтею 17 Конституції України визначено ключове завдання – захист суверенітету і територіальної цілісності України, а також виокремлено такі **сфери забезпечення національної безпеки:**

- 1) сфера економічної безпеки;*
- 2) сфера інформаційної безпеки;*
- 3) сфера оборони України;*
- 4) сфера державної безпеки;*
- 5) сфера захисту державного кордону України.*

Подальшого системного розвитку це питання набуло з прийняттям Закону України “Про основи національної безпеки України”, яким було визначено базовий понятійно-категоріальний апарат, пріоритети захисту національних інтересів людини, суспільства і держави та систему забезпечення національної безпеки України.

Відповідно до статей 7, 8 вказаного Закону також визначено основні виклики і загрози та пріоритети державної політики у таких **сферах національної безпеки** [2]:

- 1) зовнішньополітична сфера;
- 2) сфера державної безпеки;
- 3) воєнна сфера;
- 4) сфера безпеки державного кордону України;
- 5) внутрішньополітична сфера;
- 6) економічна сфера;
- 7) соціальна та гуманітарна сфера;
- 8) науково-технологічна сфера;
- 9) сфера цивільного захисту;
- 10) екологічна сфера;
- 11) інформаційна сфера.

Тобто, вказаним Законом було запроваджено більш системну, **комплексну модель** правового регулювання у сфері національної безпеки, яка охоплювала основні сфери життєдіяльності людини, суспільства і держави.

Водночас, в контексті євроатлантичної інтеграції України з прийняттям у 2018 р. Закону України “Про національну безпеку України” розпочався процес розбудови нової моделі сектору безпеки і оборони.

Передусім варто звернути увагу на структуру Закону: розділи I, II визначають *основні положення та засади забезпечення національної безпеки*, розділ III – *систему управління та організацію цивільного демократичного контролю*, розділ IV – *складові сектору безпеки і оборони*, розділ V – *організацію планування у сферах національної безпеки і оборони*. Згідно з положеннями розділів I, V цього Закону також запроваджено систему стратегічного планування та комплекс відповідних документів: *Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія кібербезпеки України, Стратегія розвитку оборонно-промислового комплексу України*.

Відповідно до ст. 12 визначено перелік суб’єктів сил безпеки і оборони, зокрема: Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту України, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба надзвичайних ситуацій України, Служба безпеки України, Антитерористичний центр при Службі безпеки України, Служба судової охорони, Управління державної охорони України, Державна служба спеціального зв’язку і технічного захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику.

Згідно з розділом IV “Сектор безпеки і оборони” Закону також визначено основні завдання і функції вказаних державних органів, тобто, запроваджено **інституційну (функціональну) модель** правового регулювання у сфері національної безпеки. Як наслідок, згідно з чинним законодавством сучасна модель системи забезпечення національної безпеки України включає такі основні складові [2]:

- 1) сили безпеки;
- 2) сили оборони;
- 3) оборонно-промисловий комплекс;
- 4) систему цивільного демократичного контролю, у т.ч. складові громадянського суспільства.

Загалом, проведений аналіз національного законодавства надає можливість виокремити *комплексну* та *інституційну (функціональну) моделі* правового регулювання у сфері національної безпеки.

Також слід зауважити, що запроваджена 2018 року в Україні інституційна (функціональна) модель законодавчого регулювання у сфері національної безпеки в цілому відповідає сучасним трансформаціям систем національної та міжнародної безпеки, особливостям глобальної військово-політичної обстановки і тенденціям її розвитку на найближчу історичну перспективу.

Водночас нагальною є потреба розвитку законодавства з питань інформаційної безпеки й захисту прав та безпеки людини в інформаційній сфері. Крім цього, як видається, проблеми правового забезпечення безпеки у зовнішньо- та внутрішньополітичній, в економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах, а також в інших важливих сферах життєдіяльності людини, суспільства і держави мають бути врегульовані та покладатися на відповідні центральні органи виконавчої влади, що відповідають за формування та реалізацію державної політики у вказаних сферах.

2. Проблема законодавчого регулювання у сфері інформаційної безпеки України.

Сучасні глобальні трансформації в інформаційній (цифровій) сфері стрімко формують новітні виклики і загрози, які вже становлять реальну небезпеку усьому людству та міжнародному правопорядку.

З початком збройної та інформаційної агресії рф проти України світова спільнота уже увійшла у глобальне інформаційне та кіберпротистояння. В інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції. Більшість країн світу зіштовхнулася з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об'єкти критичної інфраструктури. Наслідки використання сучасної *інформаційної зброї* (дезінформація, пропаганда, інформаційно-психологічні операції тощо), яка отримала назву *“зброя масових руйнувань”* (*weapon of mass disruption*), є співставними із застосуванням зброї масового ураження та можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу. За цих умов вкрай актуальною постає проблема розвитку національного законодавства у сфері інформаційної безпеки.

З цього приводу звернемося до положень частини першої ст. 17 Конституції України, згідно з якою *забезпечення інформаційної безпеки віднесено до основних функцій держави та визнано справою всього Українського народу* [1]. Тобто, Україна ще 30 років тому на етапі підготовки та прийняття Конституції України стала однією із перших держав світу, яка юридично виокремила важливість проблеми забезпечення інформаційної безпеки. В порядку порівняння слід зауважити, що в Європейському Союзі перша директива з цього питання, у т.ч. щодо російської інформаційної агресії, була прийнята лише 2016 року. Подальші події 2014-2025 років, пов'язані зі збройною та інформаційною агресією рф проти України, наочно підтвердили виключну актуальність вказаної проблеми.

Водночас, як свідчить аналіз, Законом України *“Про національну безпеку України”* взагалі не передбачено системної організації діяльності з питань забезпечення інформаційної безпеки, що в умовах сучасної інформаційної війни становить реальну загрозу для суспільства і держави. Лише у ст. 19 цього Закону йдеться про

контррозвідувальний захист інформаційної безпеки держави при визначенні функцій Служби безпеки України [1].

В контексті зазначеного Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки, було б доцільно прискорити розгляд пропозицій стосовно законопроекту “Про внесення змін до Закону України “Про національну безпеку України” щодо забезпечення інформаційної безпеки”, розроблені ДНУ ІБП НАПрН України¹. Вказаним законом, як свідчить аналіз, передусім доцільно врегулювати такі основні питання:

1) Доповнити ст. 1 цього Закону визначеннями термінів:

інформаційна безпека – стан захищеності суверенітету, територіальної цілісності та інших життєво важливих інтересів людини, суспільства і держави в інформаційній сфері, за якого забезпечується додержання безпеки, інформаційних прав, свобод та приватності життя людини, запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій;

стратегія інформаційної безпеки України – документ довгострокового планування, що визначає актуальні зовнішні та внутрішні загрози інформаційній безпеці України, стратегічні цілі та завдання, спрямовані на протидію цим загрозам та систему забезпечення безпеки людини, суспільства і держави в інформаційній сфері.

2) Частину 2 ст. 12. “Склад сектору безпеки і оборони” Закону “Про національну безпеку України” пропонується доповнити новим державним органом – **центральный орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері**, а також новою статтею 22⁻¹ у такій редакції:

“Стаття 22⁻¹. Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері.

1. Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері:

1) визначає перспективи та пріоритетні напрями розвитку інформаційної сфери та сфери інформаційної безпеки України;

2) здійснює в межах компетенції нормативно-правове регулювання в інформаційній сфері та сфері інформаційної безпеки України;

3) аналізує стан і тенденції розвитку інформаційної сфери України, розробляє та організовує виконання державних програм розвитку інформаційної сфери та сфери інформаційної безпеки України;

4) разом із Міністерством закордонних справ України сприяє популяризації та формуванню позитивного іміджу України у світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту національних інтересів, зміцнення національної безпеки та відновлення територіальної цілісності України.

2. Головним завданням у сфері інформаційної безпеки є захист суверенітету і територіальної цілісності України, забезпечення інформаційних прав і свобод людини і громадянина, законних інтересів суспільства і держави, сприяння розвитку і захисту національного інформаційного простору України”.

¹ Лист ДНУ ІБП НАПрН України до Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки вих. № 216 від 26.11.2024 з пропозиціями стосовно законопроекту “Про внесення змін до Закону України “Про національну безпеку України” щодо забезпечення інформаційної безпеки”.

Крім цього, доцільно доповнити ст. 33 Закону новою частиною 3⁻¹ у такій редакції:

“3⁻¹. Керівник центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері, забезпечує підготовку і подання державної цільової програми з питань розвитку інформаційної сфери та забезпечення інформаційної безпеки України”.

3) Доповнити перелік документів стратегічного планування у сфері національної безпеки, визначений частиною 3 ст. 25 Закону, новим правовим актом – **Стратегія інформаційної безпеки України**, а також новою статтею 29⁻¹ у такій редакції:

“Стаття 29⁻¹. Стратегія інформаційної безпеки України

1. Стратегія інформаційної безпеки України розробляється за дорученням Президента України центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері, з використанням спроможностей Центру протидії дезінформації після затвердження Стратегії національної безпеки України.

Стратегія інформаційної безпеки України схвалюється рішенням Ради національної безпеки і оборони України та затверджується указом Президента України.

2. Стратегія інформаційної безпеки визначає:

- 1) актуальні виклики і загрози національній безпеці України в інформаційній сфері;*
- 2) стратегічні цілі та завдання, спрямовані на протидію цим загрозам;*
- 3) напрями, механізми та очікувані результати реалізації визначеної мети і завдань у сфері інформаційної безпеки;*
- 4) основні напрями діяльності та систему взаємодії державних органів, органів місцевого самоврядування та суспільства з питань розвитку інформаційної сфери, стратегічних комунікацій та сфери інформаційної безпеки України;*
- 5) пріоритети розвитку міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.*

3. Стратегія інформаційної безпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення інформаційної безпеки України”.

Реалізація зазначеного, як видається, сприятиме приведенню тексту чинного Закону України “Про національну безпеку України” у відповідність до вимог ст. 17 Конституції України.

Також варто звернути увагу на необхідність розробки і прийняття **Закону України “Про інформаційну безпеку України”** (по аналогії з чинним Законом “Про основні засади забезпечення кібербезпеки України”). З погляду історії становлення національного законодавства слід зауважити, що подібний законопроект “Про засади інформаційної безпеки України” вже був розроблений і зареєстрований у Верховній Раді України (реєстр. № 4949 від 28.05.2014), але так і залишився не прийнятим. У вказаному Законі, за попередніми оцінками, передусім доцільно врегулювати такі основні питання:

1) надати визначення основних термінів, правових основ та принципів забезпечення інформаційної безпеки, життєво важливих інтересів людини, суспільства і держави в інформаційній сфері;

2) врегулювати засади формування та реалізації державної політики в інформаційній сфері та сфері інформаційної безпеки, основні напрями діяльності держави з питань забезпечення інформаційної безпеки;

3) визначити систему забезпечення інформаційної безпеки, перелік та функції суб'єктів цієї системи, порядок організації, координації та контролю за їх діяльністю;

4) сформулювати засади та механізми міжнародного співробітництва у сфері інформаційної безпеки.

Втім, ця проблема потребує додаткового опрацювання з урахуванням сучасних особливостей і тенденції розгортання глобального інформаційного простору та перебігу глобального інформаційного протиборства. Крім цього, потребує законодавчого врегулювання проблема становлення і розвитку *системи стратегічних комунікацій*. Загалом, вказані системні організаційно-правові проблеми залишаються вкрай актуальними в сучасних умовах та потребують подальшої наукової розробки.

3. Проблема правового регулювання з питань захисту персональних даних та приватності життя людини в контексті євроінтеграції України.

Проблеми розбудови систем захисту даних та інформаційної безпеки людини є предметом низки наукових досліджень [3], але продовжують викликати багато питань в галузі права. Зокрема, новітні інформаційні (цифрові) технології можуть надавати не лише нову якість результатів їх застосування, але й створювати нові виклики і загрози, передусім з питань захисту персональних даних та приватності життя людини.

Захист персональних даних розглядається у країнах ЄС як невід'ємний елемент демократії та правової держави, а більшість законів у цій сфері мають типову назву – закон про захист даних. Під “*захистом даних*” (*data protection*) розуміють будь-які правові, організаційні, технічні (технологічні, криптографічні, програмні) засоби щодо захисту інформації персонального змісту. Для комплексного захисту даних на міжнародному рівні використовується термін “*безпека даних*” (*data security*).

У травні 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних – **General Data Protection Regulation** (далі – *GDPR*, з англ. “*Пакет захисту даних*”), який передбачає створення умов забезпечення узгодженої нормативно-правової бази на європейському рівні.

Головним документом, який визначає на території держав-членів ЄС порядок застосування обов'язкових правил, є Регламент (ЄС) 2016/679 “*Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних*, а також про скасування Директиви № 95/46/ЄС (Загальні Положення про захист даних)” від 27.04.2016 р. [4]. Важливою новацією Регламенту *GDPR* є те, що вперше у документах сфери захисту персональних даних офіційно констатовано, що:

– захист фізичних осіб у зв'язку з обробкою персональних даних є основоположним правом (п. 1 Преамбули Регламенту);

– ефективний захист персональних даних на усій території ЄС вимагає зміцнення та детального визначення прав суб'єктів даних та обов'язків осіб, які визначають та здійснюють обробку персональних даних (п. 11 Преамбули);

– державам-членам надається можливість введення національних положень з метою подальшого уточнення застосування правил, передбачених цим Регламентом, більш точно визначаючи умови, за яких обробка персональних даних є законною (п. 10 Преамбули).

До “Пакету захисту даних” (*GDPR*) також включено Директиву (ЄС) 2016/680 “*Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення чи судового переслідування*

кримінальних правопорушень або виконання кримінальних покарань, та про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД” [4, с. 104-156], а також Директиву (ЄС) 2016/681 “Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину” [4, с. 157-176]. Крім цього слід звернути увагу на те, що у 2016 р. Європейським Парламентом також була затверджена Директива ЄС “Про безпеку мережевих та інформаційних систем” (NIS Directive) [5].

З урахуванням зазначеного видається за доцільне розглянути низку актуальних питань.

1) Ключові аспекти NIS Directive.

Основне завдання директиви – забезпечення високого рівня інформаційної безпеки для операторів критичної інфраструктури і провайдерів цифрових послуг. Тобто, йдеться не лише про захист персональних даних, але й про безпеку взагалі будь-яких даних.

Для виконання цього завдання державам-членам ЄС запропоновано підвищити свою готовність і поліпшити співробітництво один з одним, а також зобов’язати операторів, які надають критично важливі послуги, пов’язані з певними об’єктами інфраструктури, і провайдерів окремих цифрових послуг вжити відповідних заходів з керування ризиками безпеки й повідомляти про серйозні інциденти компетентним національним органам.

2) Ключові аспекти Регламенту GDPR.

Згідно з його положеннями обробка персональних даних має здійснюватися на основні таких принципів:

законність, справедливість і прозорість – персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб’єкта даних;

цільове обмеження – збиратися для певної, конкретної і законної мети та не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою;

зведення до мінімуму даних – бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються;

точність – бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілей, для яких вони обробляються, слід видаляти або виправляти без затримки;

обмеження зберігання – зберігається у формі, що дозволяє ідентифікувати суб’єкта даних не довше, ніж це необхідно для цілей, для яких вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно з метою архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей;

цілісність і конфіденційність – оброблятися так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів;

підзвітність – будь-яка установа (бізнес-компанія тощо) несе відповідальність перед наглядовими органами і повинна бути здатна довести дотримання положень Регламенту.

Правові новації Регламенту GDPR стосуються питань посилення прав суб’єктів персональних даних. Це знайшло відображення у ст. 17 Регламенту GDPR яка встановлює за суб’єктом персональних даних “*право бути забутим*” (англ. – “*right to be forgotten*”).

Стаття уточнює право на видалення даних і визначає їх умови, включаючи обов'язок володільця, який оприлюднив персональні дані, повідомляти треті сторони про вимогу суб'єкта даних щодо усунення будь-яких посилань на відповідні персональні дані, а також видалення будь-яких копій чи примірників таких персональних даних.

Варто зауважити, що **вимоги “Пакету захисту даних”** мають застосовуватися до обробки даних фізичних осіб у компаніях, закладах, установах, організаціях та підприємствах, розташованих **не тільки на території держав-членів ЄС, але і тих, що здійснюють свою діяльність за його межами та пов'язані з обробкою персональних даних в рамках ЄС**. Ці правила не поширюються на обробку даних про юридичних осіб, а також на дані, які відносяться до анонімної інформації і померлих осіб.

Персональні дані, які обробляються державними органами з метою запобігання, розслідування, виявлення чи судового переслідування злочинів або виконання покарань регулюються іншим правовим актом ЄС – Директивою (ЄС) 2016/680 Європейського Парламенту і Ради. При цьому, кожна держава-член ЄС може мати свої особливі погляди та відповідне національне законодавство, але коли справа стосується та пов'язана зі співпрацею з будь-якими організаційними структурами держав-членів ЄС слід керуватися приписами, що визначаються у Регламентах ЄС. У разі недодержання зазначеного можуть бути накладені такі **санкції**:

- попередження у письмовій формі у разі першого й не навмисного недотримання приписів щодо захисту персональних даних;

- призначення регулярних або періодичних перевірок діяльності щодо захисту даних;

- призначення санкцій (в межах ЄС, на організацію, бізнес-компанію та ін.) - штрафів у розмірі до 20.000.000 EUR або до 4 % від загального річного обсягу фінансування (від показників поточного і попереднього фінансового року, виходячи з того, яка сума більше);

- призначення санкцій (при транскордонній передачі персональних даних) - штрафів у розмірі до 10,000,000 EUR або до 2 % від загального річного обсягу фінансування (від показників поточного і попереднього фінансового року, виходячи з того, яка сума більше).

Поряд з Регламентом GDPR, в Європейському Союзі була прийнята Директива 2002/58/ЄС “Про обробку персональних даних та захист таємниці (“privacy”) в секторі електронних комунікацій” від 12 липня 2002 року [6, с. 379-392]. Водночас, передбачене подальше регулювання у сфері приватного життя – “e-Privacy Regulation”.

Як свідчить аналіз [7], розробку ідеї про необхідність розгляду сукупності інформації про фізичну особу як об'єкта правової охорони одними з перших розпочали американські правознавці. Розвиток цієї ідеї знайшов відображення у так званій концепції “**права на приватність**” (right to privacy) – **права особи “на саму себе”, права “бути залишеною на самоті”** (privacy). За матеріалами узагальнення прецедентної практики в США “делікти проти приватності” (privacy torts) було розділено на такі групи:

- **втручання в усамітненість** (intrusion upon seclusion) – вторгнення в “особистий простір” індивіда;

- **публічне розголошення інтимних фактів** (publication of private facts);

- **спотворене представлення особи перед громадськістю** (false light);

- **використання чужого імені або образу в корисливих цілях** (appropriation).

Джерелом права власності на персональні дані є природно-конституційне право людини на унікальні, особливі й делікатні відомості, які не лише ототожнюють чи ідентифікують людину, характеризують її особистість, але й містять у собі предмет споживчої та мінової вартості. Виходячи зі світових тенденцій забезпечення прав і свобод людини та беручи до уваги, що право власності – це один із найважливіших інститутів будь-якої системи права, а право людини на персональні дані належить їй від народження і є результатом природно-конституційної даності, виникає необхідність і правомірність у формуванні інституту права приватної власності людини на свої персональні дані, як основної складової загальної системи захисту прав людини.

Відповідно до статті 32 Конституції України *“Ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини”* [1].

Вказаний конституційний припис отримав конкретизацію 2010 року в Законі України *“Про захист персональних даних”*, який врегульовує відносини у сфері обігу персональних даних та декларує його *“спрямованість на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних”* [8].

Заслуговує на увагу й рішення Конституційного Суду України, що *“інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов’язані з особою та членами її сім’ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною”* [9]. Ще раніше у 1997 році Конституційний Суд України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України *“Про інформацію”* та статті 12 Закону України *“Про прокуратуру”* (справа К.Г. Устименка) відніс до конфіденційної інформації такі відомості як освіта, сімейний стан, релігійність, стан здоров’я, дата і місце народження, майновий стан та інші персональні дані людини [10].

Тобто, право людини на недоторканність особистого (у європейському розумінні – *“приватного”*) життя відповідно до законодавства України передбачає правовий захист відомостей про неї, за якого основним об’єктом правовідносин є персональні дані. Водночас, вирішення проблеми забезпечення приватності та безпеки персональних даних в усіх сферах життєдіяльності людини, суспільства і держави залишається нагальною проблемою та одним із найважливіших чинників становлення інформаційного законодавства і права.

З урахуванням зазначеного та в контексті опрацювання нової редакції Закону України *“Про захист персональних даних”* передусім видається за доцільне врахувати відповідні рекомендації експертів ЄС та РЄ щодо цього законопроекту [11], а саме:

- уникнення положень законопроекту, які є занадто складними або неможливими для реалізації на практиці, оскільки вони не матимуть жодної цінності для захисту прав і свобод людини;

- зобов’язання державних органів, залучених до законотворчого процесу, включати до правових актів, що регулюють обробку персональних даних, ціль обробки, про яку йдеться, та іншу необхідну інформацію залежно від обставин;

- передбачення процедури здійснення контролерами даних оцінки впливу на захист даних у процесі ухвалення законодавчих актів;
- встановлення основних принципів обробки персональних даних органами державного і недержавного секторів;
- визнання в законопроекті застосування механізмів ЄС з боку українських контролерів даних і операторів даних, передбачених у GDPR – кодексу поведінки (стаття 40) і зобов'язальних корпоративних правил (стаття 47);
- створення незалежного контролюючого органу з питань захисту персональних даних.

Головна проблема у цій сфері, як свідчить аналіз, полягає у відсутності ефективної загальнодержавної системи захисту персональних даних, а також належного організаційно-правового механізму регулювання відносин та відповідальності за здійснення правопорушень. З урахуванням зазначеного актуальною постає **проблема розробки і впровадження в Україні нової моделі системи захисту персональних даних**, зокрема:

- 1) опрацювання і затвердження Верховною Радою України відповідно до правових стандартів ЄС ефективної державної політики з питань захисту персональних даних та захисту приватності життя людини;
- 2) організація належного парламентського контролю з питань захисту персональних даних, а також контролю Уповноваженого Верховної Ради України з прав людини та представника Уповноваженого з питань захисту персональних даних;
- 3) законодавче визначення центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики з питань захисту персональних даних відповідно до правових стандартів ЄС (ця функція може бути покладена на Міністерство юстиції України або відновлену Державну службу з питань захисту персональних даних, що скеровується Мін'юстом);
- 4) покладання на центральні органи виконавчої влади, їх територіальні підрозділи та органи місцевого самоврядування (у межах їх компетенції) відповідних функцій з питань захисту персональних даних, зокрема:
 - покладання на Державну службу спеціального зв'язку і захисту інформації України функцій організації забезпечення технічного захисту персональних даних;
 - віднесення до компетенції Державного бюро розслідувань України проведення досудового слідства щодо правопорушень, які стосуються захисту персональних даних, а також покладання на Національну поліцію України функції сприяння у проведенні перевірок та розслідування правопорушень у цій сфері;
- 5) опрацювання питання (з урахуванням п. 20 Преамбули Регламенту (ЄС) 2016/679, що його правила застосовуються у діяльності судів та інших судових органів, а також досвіду Суду із захисту даних Великої Британії) щодо **створення** окремих судових палат у складі апеляційних судів і Верховного Суду та **Спеціалізованого суду** з питань захисту інформації (даних) з можливим покладанням на вказані органи розгляду справ щодо порушення права приватності життя людини і захисту персональних даних, правопорушень у сфері обігу інформації, надання доступу до публічної інформації, діяльності засобів масової інформації та використання інформаційно-комунікаційних систем і мереж, єдиних державних реєстрів та інформаційних ресурсів, роботи з інформацією, що становить державну таємницю або містить відомості з обмеженим доступом;

б) запровадження в органах, установах, закладах, підприємствах та організаціях (згідно з нормами ЄС) посад фахівців з питань захисту персональних даних або покладання цих функцій на окремих працівників цих організацій.

Розвиток національної системи захисту персональних даних також потребуватиме кардинальної **зміни національного законодавства**, зокрема:

- імплементації правових стандартів ЄС з питань захисту персональних даних, визначених законодавством ЄС, зокрема, Регламентом (ЄС) 2016/679 від 27.04.2016 р., Директивою (ЄС) 2016/680 від 27.04.2016 р. Європейського Парламенту і Ради, Директивою (ЄС) 2016/681 від 27.04.2016 р. Європейського Парламенту і Ради та внесення необхідних змін до законодавства України;

- приведення понятійного апарату, визначеного Законом “Про захист персональних даних”, у відповідність до визначень понятійного апарату у актах “Пакету захисту даних” ЄС 2016 р.;

- запровадження в органах та організаціях (зокрема, для контролерів, процесорів та фахівців із захисту даних) організаційно-розпорядчих документів щодо організації захисту персональних даних, а також удосконалення механізмів сертифікації автоматизованих засобів захисту персональних даних, про що йдеться у Розділі 5 Регламенту (ЄС) 2016/679;

- прийняття Кодексу поведінки у сфері захисту персональних даних та поширення його принципів у закладах, установах, організаціях та підприємствах будь-якої форми власності;

- опрацювання питання щодо юридичного визначення понять “власник персональних даних”, “право приватної власності на персональні дані”.

При цьому, слід виходити з того, що людина, її життя і здоров’я, недоторканність та безпека віднесені до найвищих цінностей демократичного суспільства. Відповідно, у національному законодавстві мають бути відображені базові критерії з питань захисту та безпеки персональних даних за такою можливою формулою: *“право приватної власності людини і громадянина (фізичної особи) на персональні дані – це право володіння, користування та виключного розпорядження своїми персональними даними, за умов збалансованості та узгодженості цього права з правами інших громадян та законними інтересами суспільства і держави у безпеці”*.

При цьому, володіння, користування та розпорядження персональними даними мають передбачати: а) *володіння персональними даними* – наявність можливості людини та нормативно-правових умов для забезпечення приватності персональних даних в незмінному вигляді; б) *користування персональними даними* – наявність можливості людини та нормативно-правових умов для забезпечення використання відомостей про себе на власний розсуд; в) *розпорядження персональними даними* – наявність можливості та нормативно-правових умов для забезпечення виключного права людини щодо порядку доступу до своїх персональних даних.

Запропонована формула, як видається, відповідає здобуткам історико-правової науки щодо загальної ідеї прав людини на життя, приватну власність і свободу, корелюється з приписами п. 1 Преамбули Регламенту GDPR, що **захист персональних даних фізичних осіб є основоположним правом**, а також може стати основою для законотворчості, правозастосування та оцінки ефективності діяльності у сфері захисту персональних даних.

Загалом, реалізація запропонованих змін щодо моделі розвитку системи захисту персональних даних та внесення змін до чинного законодавства сприятиме усуненню наявних системних проблем у сфері захисту персональних даних та впровадженню

визначених законодавством Європейського Союзу стандартів і механізмів захисту персональних даних у правове поле України.

Висновки та пропозиції.

1. Проведений аналіз національного законодавства надає можливість виокремити *комплексну та інституційну (функціональну) моделі* правового регулювання у сфері національної безпеки, що були сформовані в Україні у 2003 та 2018 роках відповідно. Сучасна інституційна модель законодавчого регулювання у сфері національної безпеки в цілому відповідає процесам трансформації систем національної, європейської та міжнародної безпеки, особливостям глобальної військово-політичної обстановки і тенденціям її розвитку на найближчу історичну перспективу.

Водночас, як видається, проблеми правового забезпечення безпеки у *зовнішньо- та внутрішньополітичній, в економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах*, а також в інших важливих сферах життєдіяльності людини, суспільства і держави мають бути врегульовані та покладатися на відповідні центральні органи виконавчої влади, що відповідають за формування та реалізацію державної політики у вказаних сферах.

2. З початком збройної та інформаційної агресії рф проти України світова спільнота увійшла у глобальне інформаційне та кіберпротиборство. В інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції. Більшість країн світу зіштовхнулася з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об'єкти критичної інфраструктури. Наслідки використання сучасної інформаційної зброї, яка отримала назву "*зброя масових руйнувань*" (*weapon of mass disruption*), є співставними із застосуванням зброї масового ураження та можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу.

За цих умов вкрай актуальною постає проблема розробки і прийняття *Закону України "Про інформаційну безпеку України"*, у якому передусім доцільно врегулювати такі основні питання:

- надати визначення основних термінів, правових основ та принципів забезпечення інформаційної безпеки, життєво важливих інтересів людини, суспільства і держави в інформаційній сфері;
- врегулювати засади формування та реалізації державної політики в інформаційній сфері та сфері інформаційної безпеки, основні напрями діяльності держави з питань забезпечення інформаційної безпеки;
- визначити систему забезпечення інформаційної безпеки, перелік та функції суб'єктів цієї системи, порядок організації, координації та контролю за їх діяльністю;
- врегулювати питання становлення і розвитку системи стратегічних комунікацій з урахуванням стандартів країн-членів НАТО та особливостей цивільно-військового співробітництва на деокупованих територіях України;
- сформулювати засади та механізми міжнародного співробітництва у сфері інформаційної безпеки.

3. Потребує перегляду та оптимізації законодавство України з питань захисту персональних даних та приватності життя людини, передусім це стосується:

- врахування у Законі України "Про захист персональних даних" та інших правових актах вимог законодавства ЄС з питань захисту персональних даних, визначених зокрема, Регламентом (ЄС) 2016/679 від 27.04.2016 р., Директивою (ЄС)

2016/680 від 27.04.2016 р. Європейського Парламенту і Ради, а також Директивою (ЄС) 2016/681 від 27.04.2016 р. Європейського Парламенту і Ради;

– приведення понятійно-категоріального апарату, визначеного законодавством України, у відповідність до визначень понятійного апарату в актах “Пакету захисту даних” ЄС, у т.ч. опрацювання питання щодо юридичного визначення понять “власник персональних даних”, “право приватної власності на персональні дані”;

– розробки і запровадження (для фахівців із захисту даних) організаційно-розпорядчих документів, механізмів сертифікації автоматизованих засобів захисту персональних даних (згідно з Розділом 5 Регламенту (ЄС) 2016/679), а також Кодексу поведінки у сфері захисту персональних даних та поширення його принципів в органах, закладах, установах, організаціях та підприємствах усіх форм власності.

Використана література

1. Закон України «Про прийняття Конституції України та введення її в дію» від 28.06.1996 № 254/96-ВР (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 142).
2. Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV. *Відомості Верховної Ради (ВВР)*. 2003. № 39. ст. 351).
3. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. № 4(19)/2016. С. 60-70; Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*: зб. наук. праць. № 3(90)/2017. С. 36-50; Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. № 1(32)/2020. С. 33-46 та ін.
4. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних / І. Майстренко – переклад з англ.; В. Брижко – редагування тексту. – НДІП НАПрН України. Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 177 с. С. 2-103.
5. The Directive on Security of Network and Information Systems (NIS Directive). URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651
6. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв’язку з автоматизованою обробкою даних у правоохоронній діяльності”: посібник. Кн. 2 / В. Брижко, М. Швець та ін. Київ: ТОВ “Пан Тот”, 2006. 509 с.
7. Пилипчук В.Г., Брижко В.М., Баранов О.А., Мельник К.С. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за ред. В.М. Брижко, В.Г. Пилипчука. – К.: ТОВ “Видавничий дім “АртЕк”, 2017. 226 с.
8. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI. *Відомості Верховної Ради України (ВВР)*. 2010. № 34. Ст. 481.
9. Рішення Конституційного Суду України від 20.01.12 р. № 2-рп/2012 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. – Режим доступу : <http://zakon1.rada.gov.ua/laws/show/v002p710-12>
10. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К.Г. Устименка) від 30 жовтня 1997 року. *Офіційний вісник України*. 1997. № 46. С. 126.
11. Новий законопроект про захист персональних даних – експертні консультації за підтримки спільного проекту ЄС та Ради Європи. – (Україна). URL: <https://www.coe.int/uk/web/kyiv/-/new-draft-law-of-ukraine-on-personal-data-protection-expert-consultations-with-support-of-join-eu-and-coe-project>.