УДК 342.9 (477)
DOI https://doi.org/10.32782/2524-0374/2025-1/140

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

ADMINISTRATIVE AND LEGAL REGULATION OF PERSONAL DATA PROTECTION AND INFORMATION SECURITY IN THE FIELD OF ENSURING LIFE SAFETY

Бондар Д.В., к. наук з держ. упр.,
ректор
Львівський державний університет безпеки життєдіяльності
ORCID ID: 0009-0004-9571-7828

Наукова публікація присвячена дослідженню актуальних питань адміністративно-правового регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності.

Зазначається, що в сучасному інформаційному суспільстві захист персональних даних та забезпечення інформаційної безпеки є одним із основних завдань органів публічної адміністрації. Особливої актуальності захист персональних даних та забезпечення інформаційної безпеки набувають в умовах правового режиму воєнного стану.

Формулюється висновок про те, що рівень захисту персональних даних та стан інформаційної безпеки напряму впливають на якість забезпечення безпеки життєдіяльності, адже доступність персональних даних та незахищеність інформаційних ресурсів створюють умови для здійснення протиправної діяльності з використанням інформаційних технологій, зокрема: хакерських атак, шахрайства, протиправного переслідування особи тощо.

За результатами проведеного дослідження пропонується імплементувати в національне законодавство положення європейського Загального регламенту захисту даних (GDPR) та європейського Закону про штучний інтелект (Artificial Intelligence Act, AI Act).

З метою забезпечення інформаційної безпеки у сфері забезпечення безпеки життєдіяльності пропонується зберігати всю службову інформації ДСНС України, а також інформацію про надзвичайні події та їх наслідки, сили та засоби цивільного захисту та іншу важливу інформацію на декількох альтернативних автономних серверах в різних зарубіжних країнах, які мають партнерські відносини з Україною. Також наголошується на необхідності багаторівневого, криптографічного захисту інформації у сфері забезпечення безпеки життєдіяльності, якщо вказана інформація становить державну таємницю або її поширення може завдати шкоди національним інтересам України.

Ключові слова: безпека життєдіяльності, цивільний захист, цифровізація, персональні дані, інформаційна безпека, публічна адміністрація, інформаційні технології, автоматизовані системи, штучний інтелект, правове регулювання.

The scientific publication is devoted to the study of current issues of administrative and legal regulation of personal data protection and information security in the field of ensuring the safety of life.

It is noted that in the modern information society, the protection of personal data and ensuring information security is one of the main tasks of public administration bodies. The protection of personal data and ensuring information security acquire particular relevance in the conditions of the legal regime of martial law.

The conclusion is formulated that the level of personal data protection and the state of information security directly affect the quality of ensuring the safety of life, because the availability of personal data and the insecurity of information resources create conditions for the implementation of illegal activities using information technologies, in particular: hacker attacks, fraud, unlawful persecution of a person, etc.

According to the results of the study, it is proposed to implement the provisions of the European General Data Protection Regulation (GDPR) and the European Law on Artificial Intelligence (Artificial Intelligence Act, AI Act) into national legislation.

In order to ensure information security in the field of ensuring the safety of life, it is proposed to store all official information of the State Emergency Service of Ukraine, as well as information about emergency events and their consequences, civil defense forces and means and other important information on several alternative autonomous servers in various foreign countries that have partnership relations with Ukraine. It is also emphasized the need for multi-level, cryptographic protection of information in the field of ensuring the safety of life, if the specified information constitutes a state secret or its dissemination may harm the national interests of Ukraine.

Key words: safety of life, civil defense, digitalization, personal data, information security, public administration, information technologies, automated systems, artificial intelligence, legal regulation.

Актуальність теми. Безпека життєдіяльності є складною комплексною наукою та навчальною дисципліною про різноманітні загрози та небезпеки, які вливають або можуть вплинути на життєдіяльність людини, а також способи та методи запобігання вказаним загрозам та небезпеками, механізми ліквідації надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру.

Однією із сфер суспільних відносин, в якій наразі актуальними є питання забезпечення життєдіяльності, є сфера інформаційних відносин. Цифровізація суспільного життя створила фактично інший, паралельний світ, який визначають як цифрове середовище.

Цифрове середовище включає в себе всі інформаційно-комунікаційні технології, бази даних та цифрові мережі (Інтернет, мережі мобільного зв'язку), цифрові продукти (контент) та послуги. В цифровому середовищі відбувається постійна взаємодія між людьми, обмін масивами інформації, текстовими, аудіо та відеофайлами, здійснюється електронна торгівля та надання цифрових послуг. Фактично створюється цифровий Всесвіт (віртуальний світ), в якому відображається та відтворюється більша частина реальних суспільних відносин.

Людина як учасник цифрових відносин ідентифікує себе через певний обсяг персональних даних, які завантажує в цифрові мережі, включаючи інформацію про особу, її місцезнаходження, банківські рахунки, вподобання (які визначаються або шляхом опитування або самими алгоритмами пошукових систем, коли мережа пропонує особі в якості рекомендацій той контент, який вона найчастіше шукає).

Природньо, що розвиток цифрових технологій призвів до появи окремого виду протиправної діяльності у вигляді вчинення правопорушень із використанням інформаційних технологій, включаючи несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; поширення шкідливого програмного забезпечення (вірусів), спаму; створення дублікатів офіційних сторінок комерційних установ та органів публічної адміністрації тощо.

Метою протиправної діяльності в цифровому середовищі є отримання доступу до персональних даних особи,

включаючи банківські рахунки, інформацію про власність, протиправне переслідування особи, а також порушення роботи інформаційних (автоматизованих) систем.

Таким чином, в цифровому середовищі актуальним є забезпечення безпеки життєдіяльності особи, тобто її безпеки в цифровому форматі, адже правопорушення у цифровому середовищі призводять до негативних наслідків в реальному житті – втрати особою фінансових заощаджень та власності, завдання шкоди репутації, порушення порядку нормальної життєдіяльності (неможливості отримати адміністративні послуги, укласти угоду) тощо.

Вищезазначене обумовлює актуальність дослідження питань адміністративно-правового регулювання захисту персональних даних та інформаційної безпеки в контексті забезпечення безпеки життєдіяльності.

Актуальні питання забезпечення безпеки життєдіяльності та цивільного захисту завжди знаходились в центрі уваги науковців. Так, питанням забезпечення безпеки життєдіяльності присвятили свої роботи такі відомі науковці як Ф. Апшай, Т. Гринюк, К. Марченко, О. Оришака, О. Остапенко, О. Халак, О. Хитра, О. Чекригін та інші дослідники.

Питання адміністративно-правового регулювання суспільних відносин, включаючи суспільні відносини у сфері забезпечення безпеки життєдіяльності та цивільного захисту, досліджували такі відомі науковці як М. Бабик, В. Бевзенко, Д. Біленька, О. Берназюк, М. Віхляєв, О. Гунбіна, К. Дубова, Т. Ковальова, Т. Коломоєць, О. Комаров, А. Комзюк, А. Краковська, І. Лопушинський, А. Омельченко, І. Тищенкова та інші.

Проте, питання адміністративно-правового регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності ще не були об'єктом окремого дослідження, що актуалізує необхідність підготовки даної публікації.

Постановка завдання. Метою публікації є дослідження актуальних питань адміністративно-правового регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності.

Методологія даної публікації традиційно об'єднує три групи методів наукового пошуку. Першу групу складають філософські методи дослідження, а саме, метод діалектики, його закони та прийоми, а також метод метафізики. Серед загальнонаукових методів дослідження (друга група методів) більшою мірою застосовуються прийоми логіки (аналіз, синтез, дедукція, індукція, порівняння), системний та структурно-функціональний методи. Третю групу складають спеціально-юридичні методи дослідження, серед яких більшою мірою застосовуються формально-юридичний метод та метод юридичного моделювання.

Також, враховуючи тему дослідження, активно використовуються такі наукові підходи як: інструментальний, цивілізаційний, телеологічний та синергетичний.

Результати дослідження. Захист персональних даних та інформаційна безпека є одними із найбільш актуальних питань в сучасному інформаційному суспільстві. Наразі більшість учасників суспільних відносин є активними користувачами Інтернет через смартфон або персональний комп'ютер. Відбувається обмін великими масивами інформації, включаючи тестові, аудіо та відеофайли. Пошукові системи підлаштовуються під типові запроси користувачів, в соціальних мережах формуються спільноти, групи за інтересами. Комерційні компанії активно використовують Інтернет для маркетингу, реклами. В свою чергу органи публічної адміністрації представлені офіційними веб-сайтами та надають широкий спектр електронних (цифрових) адміністративних послуг. Крім того, в мережі відбувається обмін службовою інформацією, створюються та активно наповнюються різноманітні державні реєстри та бази даних.

Водночас цифровий формат даних, які розміщуються в реєстрах, соціальних мережах, пересилаються засобами електронної пошти та через мобільні застосунки (месенджери), робить їх відкритими для інших користувачів, які часто переслідують протиправні цілі. Крім того, люди часто добровільно надають персональну інформацію різноманітним інформаційним ресурсам комерційних компаній, банків, державних установ та організацій, і така інформація також часто стає загальнодоступною.

Професійні хакери з легкістю зламують акаунти, створюють дублікати офіційних веб-сторінок комерційних, банківських установ, отримують несанкціонований доступ до державних реєстрів тощо.

Незахищеність персональних даних значною мірою впливає на безпеку життєдіяльності людини та суспільства в цілому, адже заволодіння персональним даними сторонніми особами із протиправною метою може призвести до вкрай негативних наслідків, включаючи отримання зловмисниками доступу до банківських рахунків особи, використання фото та відеоматеріалів для шантажу (з погрозами поширити конфіденційну, інтимну інформацію), створення клонів сторінок певної особи у соціальних мережах та здійснення від її імені певної діяльності (збирання коштів на нібито лікування та інші потреби; здійснення психологічного тиску на родичів та знайомих з метою схилити їх до певних дій; поширення матеріалів, які дискредитують особу тощо). Не поодинокими є випадки здійснення від імені особи, персональні дані якої викрадено, терористичної діяльності, вчинення інших злочинів проти національної безпеки.

Таким чином, захист персональних даних у сфері забезпечення безпеки життєдіяльності є одним із завдань національних органів публічної адміністрації. Правовою основою виконання даного завдання є Закон України «Про захист персональних даних». Вказаний закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Він поширюється, у тому числі, на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів [1].

В Законі України «Про захист персональних даних» чітко зазначено, що мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством (ст. 6 Закону України «Про захист персональних даних») [1].

Крім того, враховуючи євроінтеграційні прагнення України, важливим є дотримання європейських стандартів у сфері захисту персональних даних.

Так, в Європейському Союзі у 2016 році прийнято Загальний регламент про захист даних (General Data Protection Regulation, GDPR). Цей загальноєвропейський акт суттєво розширює повноваження держав у сфері соціальних мереж – дозволяє видаляти незаконний контент і змушує платформи докладати більше зусиль для боротьби з небезпечними матеріалами [2].

Загальний регламент захисту даних (GDPR) є найсуворішим законом про конфіденційність і безпеку в світі. Незважаючи на те, що він був розроблений і прийнятий в Європейському Союзі, він накладає зобов'язання на підприємства, установи та організації незалежно від місця їх знаходження, якщо вони націлені або збирають дані, пов'язані із громадянами держав-членів ЄС.

Загальний регламент захисту даних (GDPR) набув чинності 25 травня 2018 року. GDPR передбачає стягнення значних за розміром штрафів за порушення стандартів конфіденційності та безпеки, причому штрафи можуть сягати десятків мільйонів євро. За допомогою вказаного акту Європейський Союз демонструє свою тверду позицію щодо необхідності захисту конфіденційності та безпеки даних у той час, коли все більше людей довіряють свої особисті дані хмарним сервісам (службам), а порушення у цій сфері є щоденним явищем [3].

Особливу увагу необхідно приділити питанню захисту персональних даних в процесі використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Так, в Україні наразі відбувається впровадження (тестування) Системи оповіщення та реагування «Я-Доброволець» [4].

Система оповіщення та реагування «Я – доброволець» є інноваційною платформою, яка дозволяє організувати та координувати дії соціально активних громадян, які готові добровільно долучитися до ліквідації надзвичайних ситуацій та їх наслідків, використовуючи свій професійний досвід і навички. Тобто, завдяки додатку для смартфона, кожен охочий може стати на захист своєї громади, отримуючи вказівки та інструкції щодо подолання небезпек. Така платформа також дозволяє вносити всі необхідні відомості про добровольця до інформаційної бази, аби оперативно та своєчасно повідомляти людину про можливість її залучення до ліквідації надзвичайних ситуацій з урахуванням місцезнаходження (геолокації) особи [4].

Отже, враховуючи функціонування загальнодержавної системи цивільного захисту в умовах правового режиму воєнного стану, необхідно забезпечити належний рівень захисту персональних даних добровольців, які вносять відомості про себе в інформаційну базу Системи оповіщення та реагування «Я – доброволець».

На рівні спільного наказу МВС України та Міністерства цифрової трансформації України доцільно затвердити порядок функціонування Системи оповіщення та реагування «Я – доброволець» та заходи щодо криптографічного захисту персональних даних добровольців, які внесені до бази даних вказаної Системи.

На окрему увагу заслуговує питання захисту персональних даних в процесі використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності. Алгоритми штучного інтелекту дозволяють аналізувати великі масиви даних, збирати та систематизувати інформацію з камер зовнішнього відеоспостереження, різноманітну інформацію з Інтернет, включаючи персональні дані. Наприклад, з використанням системи камер відеоспостереження (включаючи як стаціонарні камери, так і камери смартфонів, ноутбуків, відеореєстраторів) та інформації із соціальних мереж за допомогою технології штучного інтелекту може здійснюватися несанкціоноване стеження за певною особою чи групою осіб, що з одного боку полегшує роботу органів безпеки та правопорядку, але з іншого є втручанням в особисте (інтимне) життя людини.

Таким чином, використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності повинно мати чітку правову основу, яка буде передбачати захист персональних даних від несанкціонованого збирання та аналізу.

В Україні наразі відсутнє належне правове регулювання використання технології штучного інтелекту, відповідні проєкти нормативно-правових актів знаходяться на стадії розробки. На даний час прийнятий лише програмний документ загального характеру. Так, Концепція розвитку штучного інтелекту в Україні схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р.

У відповідності до вказаної Концепції, впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою розвитку соціально-економічної, науково-технічної, оборонної, правової та іншої діяльності у сферах загальнодержавного значення [5].

Крім того, в Україні презентована Дорожня карта регулювання штучного інтелекту та розроблена «Стратегія розвитку штучного інтелекту в Україні на 2022-2030» [6, с. 40].

Слід відзначити, що в Європейському Союзі в 2024 році набув чинності запропонований Європейською Комісією у квітні 2021 року та схвалений Європейським парламентом і Радою ЄС у грудні 2023 року Закон про штучний інтелект (Artificial Intelligence Act, AI Act). Вказаний Закон надає розробникам і користувачам систем чіткі вимоги та зобов'язання щодо конкретного використання штучного інтелекту, одночасно зменшуючи адміністративний і фінансовий тягар для бізнесу [7].

В. Місечко зазначає, що Artificial Intelligence Act (AI Act) експерти називають еталоном у сфері регулювання технологій та систем штучного інтелекту і прогнозують, що на нього будуть рівнятися законотворці усіх держав світу [8].

Таким чином, в Україні існує реальна потреба прийняти окремий закон «Про штучний інтелект», яким буде врегульовано основні питання використання штучного інтелекту у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності. Основою для розробки вказаного закону має стати вищезазначений європейський закон про штучний інтелект (Artificial Intelligence Act, AI Act), що забезпечить адаптацію національного законодавства до права ЄС в частині інформаційного права.

Окремої уваги заслуговує питання інформаційної безпеки в контексті забезпечення безпеки життєдіяльності.

Правовою основою діяльності органів публічної адміністрації в цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [9].

Вказаним законом перебачено, серед іншого, функціонування Національної телекомунікаційної мережі (як сукупності спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань) та Національного центру резервування державних інформаційних ресурсів (як організованої сукупності об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій) [9].

У відповідності до ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України», розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій [9].

А згідно із ст. 8 вказаного закону національна система кібербезпеки є сукупністю суб'єктів забезпечення

кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [9].

Слід відзначити, що враховуючи триваючу повномасштабну збройну агресію російської федерації проти України, вразливість національних комунікаційних мереж та серверів, доцільно забезпечити зберігання інформації органів публічної адміністрації на декількох альтернативних серверах, розміщених в зарубіжних країнах, які є надійними партнерами України.

Також слід відзначити важливість Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/202, яка визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [10].

У відповідності до вказаної Стратегії, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. В Стратегії інформаційної безпеки також справедливо зазначається, що розвиток інформаційного простору в умовах глобалізації та пандемія COVID-19 зумовили посилення ролі соціальних мереж у національному та світовому інформаційному просторі, їх вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини, зокрема щодо забезпечення принципів рівності прав користувачів соціальних мереж.

Хоча право на приватність (захист конфіденційної інформації про особу, невтручання в особисте життя) є одним з основних прав людини, що закріплено в Загальній декларації прав людини, Конвенції про захист прав людини і основоположних свобод, інших міжнародних документах, а також конституціях більшості держав світу, цифрові трансформації змінюють і цю сферу. Збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність. Спроби врегулювати цю проблему тривають, формуються нові підходи у забезпеченні балансу права на приватність та інформаційної безпеки держави [10].

Крім того, в Стратегії інформаційної безпеки наголошено на тому, що значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди. Некритичне сприйняття інформації створює загрози політичній та економічній стабільності демократичних держав [10].

Крім того, в якості правової основи забезпечення інформаційної безпеки слід відзначити Стратегією кібербезпеки України, затверджену Указом Президента України від 26 серпня 2021 року № 447, в якій зазначено, що питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію [11].

В Стратегії кібербезпеки України підкреслюється, що в сучасному світі зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою. Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму є об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо [11].

Таким чином, на вищому державному рівні визнано, що забезпечення інформаційної безпеки та кібербезпеки є найважливішими функціями органів публічної адміністрації, причому кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Отже, система забезпечення безпеки життєдіяльності людини в сучасному світі обов'язково повинна включати механізми захисту персональних даних, забезпечення інформаційної безпеки та кібербезпеки.

Наразі в Україні удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту. Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України. З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері [11].

Таким чином, в Україні створюється адміністративно-правова та інституційна основа забезпечення інформаційної безпеки та кібербезпеки, що сприятиме удосконаленню загального механізму забезпечення безпеки життєдіяльності кожної людини та суспільства в цілому.

Висновки. Проведене дослідження актуальних питань адміністративно-правового регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності дозволяє сформулювати висновок про те, що рівень захисту персональних даних та стан інформаційної безпеки напряму впливають на якість забезпечення безпеки життєдіяльності, адже доступність персональних даних та незахищеність інформаційних ресурсів створюють умови для здійснення протиправної діяльності з використанням інформаційних технологій, зокрема: хакерських атак, шахрайства, протиправного переслідування особи тощо.

З метою удосконалення національних механізмів захисту персональних даних та забезпечення інформаційної безпеки, а також враховуючи євроінтеграційні прагнення України та необхідність адаптації національного законодавства до права Європейського Союзу, доцільно імплементувати в національне законодавство положення європейського Загального регламенту захисту даних (GDPR) та європейського Закону про штучний інтелект (Artificial Intelligence Act, AI Act). Зокрема, нагальною є потреба прийняти окремий Закон України «Про штучний інтелект», яким будуть врегульовані основні питання використання технології штучного інтелекту у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності.

З метою забезпечення інформаційної безпеки у сфері забезпечення безпеки життєдіяльності доцільно зберігати всю службову інформації ДСНС України, а також інформацію про надзвичайні події та їх наслідки, сили та засоби цивільного захисту та іншу важливу інформацію на декількох альтернативних автономних серверах в різних зарубіжних країнах, які мають партнерські відносини з Україною. Також слід підкреслити необхідність багаторівневого, криптографічного захисту інформації у сфері забезпечення безпеки життєдіяльності, якщо вказана інформація становить державну таємницю або її поширення може завдати шкоди національним інтересам України.

Перспективність подальшого дослідження даної тематики обумовлена необхідністю формулювання конкретних пропозицій щодо внесення змін до чинного адміністративного законодавства з урахуванням зарубіжного досвіду правового регулювання відповідної сфери суспільних відносин.

ЛІТЕРАТУРА

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20240427#Text (дата звернення: 07.11.2024).

2. Снопок О. Як Верховний суд США поступово стає регулятором у сфері соціальних мереж. Опора. Tech. 10.03.2023. URL: https://www.oporaua.org/polit_ad/iak-verkhovnii-sud-ssha-postupovo-staie-reguliatorom-u-sferi-sotsialnikh-merezh-24609 (дата звернення: 02.06.2024).

3. What is GDPR, the EU's new data protection law? GDPR.EU. URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 07.11.2024).

4. Сергій Тюрін провів нараду щодо впровадження системи «Я – Доброволець». Хмельницька обласна військова адміністрація. Офіційне інтернет-представництво. Новини. 15.08.2024. URL: https://www.adm-km.gov.ua/?p=143081#:~:text=Як%20зауважив%20Сергій%20Тюрін%20на,свій%20професійний%20досвід%20і%20навички. (дата звернення: 07.11.2024).

5. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження КМУ від 2 грудня 2020 р. № 1556-р. Дата оновлення: 29.12.2021. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 02.11.2024).

6. Куракін О.М., Скрябін О.М. Особливості правового регулювання використання штучного інтелекту в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2023. Вип. 36. С. 36-42.

7. Набув чинності Європейський закон про штучний інтелект. Про основні вимоги та зобов'язання при використанні штучного інтелекту. Міжнародні відносини. Liga zakon. Бізнесу. 08 серпня 2024 р. URL: https://biz.ligazakon.net/analitycs/229699_nabuv-chinnost-vropeyskiy-zakon-pro-shtuchniy-ntelekt-pro-osnovn-vimogi-ta-zobovyazannya-pri-vikoristann-shtuchnogo-ntelektu (дата звернення: 02.11.2024).

8. Місечко В. Закон про штучний інтелект в ЄС: що потрібно знати українцям? *Економічна правда.* 14.06.2024. URL: https://epravda.com.ua/columns/2024/06/14/715175/ (дата звернення: 02.11.2024).

9. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.11.2024).

10. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. № 685/2021. Дата оновлення: 30.12.2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 02.11.2024).

11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. Дата оновлення: 28.08.2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 02.11.2024).