ДЯКОВСЬКИЙ О. С.,
orcid.org/0000-0003-3412-9278
кандидат юридичних наук,
викладач кафедри інформаційного,
господарського
та адміністративного права
(Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»)

УДК 347.998.85
DOI https://doi.org/10.32842/2078-3736/2025.6.26

АУДИТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ ТА АДМІНІСТРАТИВНИЙ АСПЕКТ

У статті досліджено правові, організаційні та технічні аспекти захисту інформації, яка ідентифікує особу, з урахуванням найкращих практик країн ЄС, США та інших розвинених держав. Особливу увагу приділено аналізу Загального регламенту захисту даних як взірця регулювання в сфері захисту приватності в ЄС. Розглянуто американський підхід, що базується на секторальному регулюванні, а також підходи країн, які впроваджують комплексні національні стратегії захисту даних.

Висвітлено організаційно-правові аспекти аудиту захисту персональних даних, який є ключовим елементом забезпечення інформаційної безпеки в умовах сучасного розвитку цифрових технологій. Досліджено нормативно-правову базу, яка визначає обов'язки суб'єктів господарювання щодо забезпечення конфіденційності, цілісності та доступності персональної інформації. У роботі окреслено поняття аудиту захисту даних як системного процесу, спрямованого на виявлення слабких місць в існуючих системах управління інформаційною безпекою, та надано характеристику його основних етапів, включно з аналізом ризиків, оцінкою відповідності законодавчим вимогам та формуванням рекомендацій для їх усунення.

Зокрема, акцент зроблено на використанні міжнародних стандартів, таких як ISO/IEC 27001 та ISO/IEC 27701, які регламентують процеси забезпечення інформаційної безпеки та управління приватністю. Зазначено, що ефективний аудит сприяє не лише виявленню недоліків, але й підвищенню рівня довіри до організації з боку клієнтів та партнерів, що є важливим у конкурентному середовищі. У підсумку наголошено на потребі ефективного впровадження організаційно-правових механізмів аудиту захисту персональних даних, що є необхідною умовою для забезпечення прав громадян на приватність, підвищення рівня інформаційної безпеки та зменшення ризиків витоків конфіденційної інформації.

Ключові слова: *аудит, міжнародний досвід, персональні дані, цифрова культура, конфіденційність, добросовісність та розсудливість, адміністративна процедура, принципи.*

Diakovskyi O. S. Audit of personal data protection: organizational and legal aspect

The article examines the legal, organizational and technical aspects of protecting personally identifiable information, taking into account the best practices of the EU,

the USA and other developed countries. Particular attention is paid to the analysis of the General Data Protection Regulation as a model of privacy regulation in the EU. The American approach based on sectoral regulation is considered, as well as the approaches of countries implementing comprehensive national data protection strategies.

The author highlights the organizational and legal aspects of personal data protection audit, which is a key element of information security in the context of modern digital development. The legal framework defining the obligations of business entities to ensure the confidentiality, integrity and availability of personal information is studied. The paper considers the concept of data protection audit as a systematic process aimed at identifying weaknesses in existing information security management systems and describes its main stages, including risk analysis, assessment of compliance with legal requirements and formation of recommendations for their elimination.

In particular, the emphasis is placed on the use of international standards such as ISO/IEC 27001 and ISO/IEC 27701, which regulate the processes of information security and privacy management. It is noted that an effective audit contributes not only to the identification of deficiencies, but also to increasing the level of trust in the organization by customers and partners, which is important in a competitive environment. As a result, the author emphasizes the need for effective implementation of organizational and legal mechanisms for auditing personal data protection, which is a prerequisite for ensuring the rights of citizens to privacy, improving information security and reducing the risks of confidential information leakage.

Key words: *audit, international experience, personal data, digital culture, privacy. good faith and prudence, administrative procedure, principles.*

Вступ. Концепт «персональних даних» прийнято розглядати із позиції різних сфер наукового пізнання, включаючи право, цифрові технології, публічне управління та адміністрування тощо. Подібного роду тенденція спричинена активним проникненням проблематики їх захисту у кожен із перелічених сегментів. І це не випадково, адже в умовах стрімкого розвитку інформаційних технологій, глобалізації та цифровізації значна частина життєдіяльності суспільства перемістилася у віртуальний простір, що створює нові виклики щодо захисту персональних даних, оскільки їхній обсяг, збирання, обробка та використання суттєво зросли. Дані про людину, такі як її ідентифікаційна інформація, фінансові показники, медичні записи чи навіть вподобання, стали об'єктом інтересу як державних органів, так і приватних компаній, що породжує ризики неправомірного їх використання.

Важливим аспектом є і той факт, що персональні дані мають амбівалентну природу: вони є одночасно об'єктом захисту з боку права та економічним ресурсом для суб'єктів господарювання. Баланс між правами особи та інтересами бізнесу, а також прозорість правових механізмів, є одними з ключових завдань сучасної правової науки, а вивчення цього питання дає можливість розробити правові норми, які будуть відповідати викликам часу та враховувати інтереси різних сторін. Різні аспекти оптимізації захисту персональних даних через призму вітчизняного законодавства розглядають такі вчені як Бем М. В., Городиський І. М. та ін. [2], Борисенко О. С., Тимошенко А. Г. [3], Голод О. [4], Пристай Р. [6].

В свою чергу, **метою** нашої **роботи** є теоретичне обґрунтування підходів до аудиту персональних даних, включаючи визначення їхньої правової природи, створення інструментів для ефективного захисту приватності та балансування інтересів особи, держави й бізнесу в умовах глобалізації та цифровізації.

Постановка завдання. Формування культури захисту персональних даних – складний і довготривалий процес, що не можна реалізувати за один день, місяць чи навіть рік. Європейському союзу знадобилося декілька років плідної праці, щоб значно підвищити рівень обізнаності серед своїх громадян, а також пояснити, чому реалізація заходів із захисту

персональних даних є важливим процесом, і що для цього необхідно робити. Більш того, масштабне заохочення та просування правової культури дозволило підвищити рівень довіри та комунікацій міждержавними органами, бізнес організаціями та громадянами. При цьому, слід зауважити, що Загальний регламент про захист даних (GDPR) [7] та європейський правовий підхід не є єдиним варіантом вирішення проблем із забезпечення захисту персональних даних.

Результати дослідження. Європейські країни докладають різних зусиль, розробляють і приймають закони, створюють профільні органи, щоб займатися питаннями захисту інформації в умовах масового розвитку кібертехнологій і намагаються боротися з ще більш інноваційними цифровими злочинами, часто пояснюючи вживані заходи необхідністю забезпечення національної безпеки та протидії тероризму, при цьому помітно обмежуючи права та свободи як офлайн, так і онлайн просторі.

Наприклад, в Естонії, яка тривалий час займає лідируючі позиції за показником Інтернет-свободи [8], розробили унікальну національну модель із захисту персональних даних. Мова йде про платформу X-Road для безпечного обміну даними працює на основі естонської технології blockchain під назвою KSI8, за допомогою якою всі вхідні та вихідні транзакції проходять автентифікацію та шифруються [9]. Серед інших переваг платформи важливо наголосити на тому, що громадяни отримують повідомлення, коли до їх даних звертаються державні органи (за винятком випадків розслідувань, що продовжуються). Враховуючи сильну правову базу Естонії щодо прав на недоторканність приватного життя та визнану на міжнародному рівні репутацію передового гравця у забезпеченні кібербезпеки для цифрового суспільства, система формує надійніший захист, ніж у країнах, де дані громадян зберігаються у незашифрованому вигляді на диференційованих серверах, і при цьому відсутній механізм інформування їх про те, хто володіє інформацією або як він використовується.

У США деякі штати ухвалили свої власні закони про конфіденційності особистих даних:

– у Колорадо в 2018 році було прийнято закон, який змушує підприємства вживати розумних заходів безпеки, коли мова заходить про особисту інформацію;

– Массачусетс вимагає від кожної бізнес-організації, яка володіє або ліцензує особисту інформацію, реалізовуватиме письмові програми інформаційну безпеку;

– Вермонт нещодавно прийняв закон, націлений на компанії, які збирають та продають особисту інформацію;

– Нью-Йорк розробив аналогічне законодавство, яке вимагає від компанії надавати споживачам копію інформації, що зберігається в архів.

Захист персональних даних у різних частинах планети набуває інших відтінків, оскільки більшою мірою пов'язаний з управлінням та контролем над Інтернетом і, як наслідок, масштабним зростанням авторитаризму. Власне, Інтернет перетворився на сучасну публічну сферу, а соціальні мережі та пошукові системи володіють величезною силою та вагомою відповідальністю за забезпечення того, щоб їхні платформи служили суспільному благу. Необмежений збір особистих даних редукує право людини на приватність, без якої світ, процвітання та свобода особистості – плоди демократичного світу – неможливо зберегти чи використовувати.

Покищо деякі країни домагаються реального прогресу у сфері свободи Інтернету, як наприклад країни ЄС, інші ж, навпаки, посилюють і обмежують.

Прогресивним та відносно новим є законодавство в ОАЕ, де діє Федеральний закон про захист персональних даних (PDPL) № 45 від 2.01.2022 [6]. Основна мета – забезпечити належний захист персональних даних громадян та резидентів ОАЕ шляхом встановлення правил збирання, зберігання, використання та передачі персональних даних. Відповідно до ст. 2 (1), Федерального Закону ОАЕ «Про захист персональних даних», його вимоги застосовуються до всіх організацій та компаній, що оперують на території ОАЕ, включаючи іноземні компанії, які мають представництва або філії у країні. Така норма означає, що незалежно від масштабів та галузі діяльності, всі компанії зобов'язані дотримуватися вимог закону та

забезпечувати безпеку персональних даних своїх клієнтів й співробітників. Варто зазначити, що закон не застосовується до опрацювання даних державних органів ОАЕ, медичної, банківської та кредитної інформації, так як ці сегменти в Еміратах регулюють окреме законодавство. Компанії, створені та зареєстровані у вільних зонах, таких як Дубайський міжнародний фінансовий центр (DIFC) та Глобальний ринок Абу-Дабі (ADGM), також не підпадають під дію закону. Незважаючи на те, що Закону ОАЕ «Про захист персональних даних» має деяку подібність до вимог Загального регламенту про захист даних (GDPR), він також має низку відмінних рис. Ключовим можна назвати факт того, що основною правовою основою для обробки даних є згода (за винятком окремих випадків). Однак існують певні ситуації, коли обробка можлива без згоди суб'єкта, наприклад:

1) укладання договору із суб'єктом даних, внесення змін чи розірвання договору;
2) якщо суб'єкт даних зробив персональні дані загальнодоступними;
3) з метою фактичного захисту інтересів суб'єкта даних;
4) якщо обробка необхідна для відстоювання законних прав або в рамках судових процедур чи процедур безпеки;
5) коли обробка необхідна для певних медичних цілей чи питань охорони здоров'я.

Крім цього, в ОАЕ діє Регламент Комітету захисту персональних даних ОАЕ (Personal Data Protection Committee Regulations), який містить положення про процедури та регулювання, пов'язані із застосуванням Федерального Закону «Про захист персональних даних», включаючи політику захисту персональних даних, керівництва та стандарти.

Також важливим документом є Закон про електронну комерцію (Electronic Commerce Law), який також охоплює питання, пов'язані з обробкою персональних даних у сфері електронної комерції. Він містить положення про збирання, використання та зберігання персональних даних у контексті електронної комерції. Існують й інші законодавчі акти, які можуть мати відношення до захисту персональних даних в ОАЕ, наприклад, закони про банківську таємницю, медичну конфіденційність тощо.

В цілому, недотримання вимог захисту персональних даних може мати серйозні наслідки для компаній. У разі порушення закону органи державної влади ОАЕ в праві застосувати адміністративні санкції, включаючи накладення штрафів, призупинення діяльності компанії, позбавлення ліцензії або обмеження права на укладення державних контрактів. Крім того, порушення вимог захисту персональних даних може призвести до кримінальної відповідальності керівників компаній. Штрафи є одним із найпоширеніших адміністративних заходів, які можуть бути застосовані до компаній за порушення вимог закону про захист персональних даних. Їх розмір залежить від характеру порушення. Штрафи можуть сягати до 5 млн. дірхам (близько 1,36 млн. $) або певного відсотка від річного обороту компанії, залежно від тяжкості порушення. У разі серйозних порушень, які можуть бути класифіковані як кримінальний злочин, керівники компаній також можуть бути піддані кримінальній відповідальності: арешту, штрафам або ув'язненню залежно від тяжкості порушення.

Компетентні органи державної влади ОАЕ мають право приймати рішення щодо застосування заходів відповідно до законодавства та своїх повноважень. До речі, основним органом державної влади, який відповідає за дотримання вимог законодавства про захист персональних даних є Data Office, створений відповідно до окремого Федерального закону ОАЕ. Діяльність структури націлена на формування політики та стандартів у галузі захисту персональних даних, а також проведення перевірок та розслідувань порушень закону. Окрім зазначеного, кожен емірат ОАЕ має свій власний орган захисту персональних даних, який відповідає за нагляд та контроль за дотриманням вимог закону про захист персональних даних на своїй території. Відповідно, органи можуть проводити перевірки та розслідування порушень згідно покладених на них повноважень законодавством.

Тут варто згадати і Комісію з мережевої безпеки та інформаційних технологій (Telecommunications Regulatory Authority) – федеральний орган, який також відіграє роль у сфері захисту персональних даних. Комісія здійснює нагляд за сектором інформаційних

технологій та телекомунікацій в ОАЕ, наділена правом проводити перевірки/розслідування порушень у цій галузі, включаючи порушення закону про захист персональних даних. В рамках контрольно-наглядової діяльності, уповноважені особи можуть (на виконання поставлених завдань) вимагати надання інформації та документів, пов'язаних з опрацюванням персональних даних, а також застосовувати адміністративні та кримінальні заходи у разі виявлення порушень. Вони також надають керівництва та консультації компаніям, приватним особам з питань захисту персональних даних в ОАЕ.

Варіативність підходів до правового регулювання інституту персональних даних чітко відображає плюралізм методів дотримання правопорядку у даному сегменті з точки зору різних держав. Очевидною також є інтенсифікація відповідальності за порушення, особливо, здійснених зі сторони суб'єктів господарювання, котрі є розпорядниками персональних даних значної кількості людей (працівників, клієнтів, партнерів тощо). Звісно, питання захисту персональних даних із техніко-правової точки зору є настільки об'ємним, що інколи представники бізнес-сегменту допускають помилки виключно через необізнаність, а не через намагання навмисно порушити чиїсь права чи інтереси. Оптимальним способом уникнення даної проблеми та наслідків, які вона в собі несе, – провести якісний аудит захисту персональних даних [3, с. 34]. Надаючи дефініцію даному поняттю ми можемо зазначити, що мова йде про комплекс заходів, який дозволяє оцінити захищеність інформаційних систем та перевірити, чи відповідають вони чинним стандартам безпеки – на даний час це ISO 27001, ISO 27002, а також рекомендації загального регламенту захисту даних GDPR. Іншими словами, аудит інформаційної безпеки – це спосіб виявити потенційні загрози та вразливі місця у конкретній організації [аудит].

Аналізуючи зміст GDPR ми виявимо, що на суб'єктів господарювання покладають значну кількість обов'язків, де уникнути процедури аудиту апріорі неможливо. Ми виділяємо п'ять основних етапів (випадків), у яких дана процедура є необхідною:

По-перше, на початку та кінці діяльності компанії (в т.ч. в процесі її реорганізації). У такий спосіб виявляються бізнес-процеси, що не відповідають вимогам GDPR і, разом з тим, за результатами перевірки компанія має на руках документ, що підтверджує, яким саме чином суб'єкт господарювання дотримуються вимог щодо захисту персональних

Таблиця 1

Етапи проведення внутрішнього аудиту

Етапи проведення внутрішнього аудиту	Характеристика етапу
Підготовчий етап	складаються та узгоджуються внутрішні документи. Слід визначитися, що саме перевірятимуть відповідальні особи та з якими стандартами порівнюватимуть
Перший етап	призначаються відповідальні за проведення аудиту інформаційної безпеки співробітники служби безпеки та інформаційного відділу, зокрема інженери, які відповідають за функціонування IT-інфраструктури в організації
Другий етап	відповідальні фахівці перевіряють бізнес-процеси та сервіси відповідно до заздалегідь підготовленого списку. Їхнє завдання- виявити потенційні вразливості чи можливості для вторгнення.
Третій етап	результати перевірки документуються та аналізуються, після чого підбиваються підсумки і, якщо необхідно, вживаються додаткові заходи щодо захисту інформаційних систем

даних. Відповідно, таким чином відбувається дотримання принципу підзвітності та реалізовуються засади комплаєнсу у всій їх динаміці.

По-друге, кожен рік/півроку (планово). Мова йде про періодичний аудит, націлений на підтримку стану узгодженості в системі «діяльність компанії – вимоги чинного законодавства».

По-третє, при початку формування взаємовідносин із новим контрагентом (бізнес-партнером). Зокрема, аудит на даному етапі буде наділений завданням із перевірки добросовісності опонента і достатності заходів щодо захисту персональних даних, відповідно до вимог GDPR.

По-четверте, перед проведенням ризикових операцій, в тому числі в процесі яких є ризик витоку персональних даних. Зазначений пункт включає випадки проведення обробки персональних даних автоматизованим способом чи здійснення профайлингу; обробляються чутливі персональні дані, або ж персональні дані, що належать особам, на яких контролер має вплив (наприклад, це може стосуватися студентів, пацієнтів, працівників компанії); обробляються персональні дані у великих масштабах, або вони зібрані в публічних місцях [голод].

По-п'яте, за фактом виявлення порушень безпеки. Зазвичай, у подібних випадках обґрунтовано провести екстрений аудит, щоб у щонайбільш короткий час виявити, які саме із організаційних або технічних заходів призводять до витоку персональних даних.

Вітчизняне законодавство, на жаль, не містить згадки стосовно регулювання аудиту захисту персональних даних. Так, суб'єкт за загальними правилом має право отримувати інформацію щодо джерел отримання його персональних даних володільцем, складу та змісту даних, а також інформацію про те, кому вони передавалися (ч. 2 ст. 8 Закону України «Про захист персональних даних» [5]). Володілець, своєю чергою, повинен забезпечити можливість отримання цієї інформації та можливість її матеріального підтвердження (документами, витягами з роботи програмного забезпечення автоматизованих систем обробки персональних даних, у вигляді звітів, електронних журналів обліку або аудиту, витягів з автоматизованих систем тощо) [2, с. 109]. Іншими словами, його правове регулювання обмежується принципом диспозитивності: «все, що не заборонено законом – дозволено».

В свою чергу, вважаємо, що аудит персональних даних має віднайти своє відображення у чинному законодавстві України в тому числі з урахуванням принципів добросовісності та розсудливості як складової адміністративної процедури.

Перш за все, аудит захисту персональних даних має стати обов'язковою процедурою для всіх суб'єктів, які обробляють персональні дані у значних обсягах. Запровадження таких вимог сприятиме систематичній оцінці відповідності діяльності суб'єктів законодавству, а також виявленню потенційних ризиків у системах захисту даних. У цьому контексті варто визначити критерії, за якими буде оцінюватися масштаб обробки даних, наприклад, кількість суб'єктів даних, обсяг інформації, що зберігається, або ступінь її конфіденційності.

Друге важливе положення має стосуватися періодичності проведення аудиту. Закон має чітко встановлювати часові рамки для здійснення перевірок, наприклад, раз на рік або залежно від змін у системах обробки даних, тим самим це забезпечить постійний моніторинг та швидке реагування на нові загрози. При цьому, у разі порушень, виявлених у ході аудиту, необхідно передбачити обов'язок суб'єктів усувати недоліки у визначений строк.

Третім важливим аспектом є регламентація суб'єктів, які мають право здійснювати аудит. Такі послуги наразі пропонує львівська юридична компанія MS Partners, столична BSO Privacy Group, ТОВ «Систем Менеджмент», команда PeopleForce та ін. У цьому контексті доцільно створити реєстр акредитованих аудиторів чи організацій, які відповідають встановленим критеріям компетентності та неупередженості. В комплексі, аналогічні заходи дадуть змогу уникнути конфлікту інтересів й гарантувати об'єктивність проведення перевірок. Також закон має визначити процедуру документування результатів аудиту. Звіти про аудит повинні містити детальну інформацію про виявлені недоліки, ризики та рекомендації щодо їх усунення. В перспективі вони стануть важливим інструментом для контролю з боку

уповноважених органів, а також будуть слугувати основою для вдосконалення внутрішніх політик суб'єктів щодо захисту даних.

Ще одним важливим компонентом є встановлення відповідальності за недотримання вимог щодо аудиту. Закон має передбачати дієві санкції за ухилення від проведення перевірок, ненадання необхідної інформації або невиконання рекомендацій аудиторів, що стимулюватиме суб'єктів належним чином виконувати вимоги щодо захисту персональних даних. В цілому, на нашу думку, запровадження вищезазначених положень до Закону України «Про захист персональних даних» сприятиме створенню ефективної системи моніторингу та вдосконалення механізмів захисту персональної інформації.

Висновки та перспективи подальших наукових пошуків. Регулярний аудит дає змогу не лише знизити ризики витоку даних, але й підвищити довіру громадян до суб'єктів, які обробляють їхні персональні дані, забезпечуючи баланс між інтересами бізнесу, держави та правами людини. Вдосконалення закону шляхом впровадження аудиту захисту персональних даних стане важливим кроком до зміцнення інформаційної безпеки України. Наразі європейське законодавство залишається передовим у питаннях оптимізації вимог щодо захисту, обробки персональних даних та значно підвищує рівень відповідальності у випадку виявлення порушень. Окремі норми доцільно імплементувати у вітчизняне законодавство, враховуючи поточний стан забезпеченості захисту персональних даних в Україні. Перспективи подальших наукових пошуків вбачаємо у порівняльному аналізі організаційно-правових підходів до аудиту захисту персональних даних у різних країнах.

Список використаних джерел:

1. Аудит інформаційної безпеки: що це і навіщо потрібно, коли проводити. GoloBridge. 2023. URL: http://surl.li/stilcp

2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.

3. Борисенко О. С., Тимошенко А. Г. Огляд методів захисту персональних даних у хмарному середовищі. Інфокомунікаційні та комп'ютерні технології. Вип. № 1 (07). 2024. с. 31–34. https://doi.org/10.36994/2788-5518-2024-01-07-04

4. Голод О. GDPR аудит: як проводити та що таке Data Protection Impact Assessment? Legal IT Group. 2024. URL: https://legalitgroup.com/gdpr-audit-osnovni-kroki/

5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

6. Пристай Р. Захист персональних даних в ОАЕ: аспекти для бізнесу. Legal IT Group. 2024. URL: https://legalitgroup.com/zahist-personalnih-danih-v-oae-aspekti-dlya-biznesu/

7. Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 «On the protection of individuals with regard to the processing of personal data and on the free movement of such data». Official Journal. L 281, 1995. p. 31–50.

8. Freedom on the Net 2024: The Struggle for Trust Online. Freedom House's. 2024. 45 p.

9. Weekly press review: X-Road not to be confused with blockchain. *e-Estonia*. 2018. URL: https://e-estonia.com/why-x-road-is-not-blockchain/

Дата першого надходження рукопису до видання: 27.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025