Марусинець Маріанна Михайлівна

Регулювання сфери інформаційно-комунікаційних технологій у контексті забезпечення захисту інформації та персональних даних у Республіці Ірландія

УДК 377.7:35(417)
DOI https://doi.org/10.24195/2414-9616.2025-1.30

Марусинець Маріанна Михайлівна
кандидат філологічних наук, доцент,
старший науковий співробітник,
старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського інституту імені Ференца Ракоці II
пл. Кошута, 6, Берегове, Закарпатська область, Україна
ORCID: 0000-0001-7366-9328

Актуальність дослідження зумовлена тим, що сьогодні спостерігається тенденція до зниження ефективності традиційних методів захисту даних. Це робить необхідним пошук та впровадження нових, сучасних підходів. В умовах активного розвитку та повсюдного застосування автоматизованих систем обробки даних питання забезпечення захисту персональних даних стають особливо важливими. Протягом останніх десятиліть Республіка Ірландія домоглася значних успіхів і посіла лідируючі позиції у сфері технологій в світі. Для досягнення цих результатів було вжито стратегічних заходів, що включають залучення прямих іноземних інвестицій у технологічні проекти, зниження корпоративних податків, а також використання соціально-культурних аспектів. Було реалізовано тристороннй підхід, спрямований на зміцнення позицій Республіки Ірландія у світовому технологічному просторі. Однак для забезпечення стабільності та стійкості досягнутих результатів необхідна наявність надійного законодавства та політики, що регулюють кіберпростір.

Головною метою статті є аналіз системи забезпечення захисту інформації в Республіці Ірландія. Ключові завдання полягають у визначенні особливостей регулювання сфери інформаційно-комунікаційних технологій (ІКТ), а також встановленні проблем і перспектив захисту персональних даних Республіки Ірландія як члена Європейського союзу в умовах стрімкого розвитку ІКТ і глобалізації.

Теоретико-методологічне підґрунтя дослідження містить загальнонаукові методи аналізу, синтезу, індукції та дедукції, а також системний метод, метод структурно-функціонального аналізу та правові методи в кібербезпеці. При дослідженні розвитку системи забезпечення кібербезпеки в контексті захисту персональних даних та конфіденційної інформації в Республіці Ірландія було застосовано історичний підхід. системний підхід було застосовано для того щоб зрозуміти суть інформаційної безпеки Республіки Ірландія, а також визначити перспективи та виклики, з якими стикається сучасна національна безпека ірландської держави. Дослідження значної правової бази в рамках регулювання системи захисту персональних даних та інформації зумовило використання міждисциплінарного підходу.

Доведено, що Республіка Ірландія продовжує роботу з удосконалення та адаптації своєї нормативно-правової бази, щоб забезпечити обізнаність та вжиття заходів на національному, індивідуальному та корпоративному рівнях. В умовах постійного розвитку кіберпростору необхідно вживати превентивних заходів для забезпечення захисту від кіберзагроз. Нормативно-правове регулювання має адаптуватися до ризиків, що виникають, тим самим спонукаючи державні структури, навчальні заклади, корпорації та підприємства постійно підвищувати рівень своєї безпеки. У міру розвитку нормативно-правового середовища в Республіці Ірландія воно відображає ширшу глобальну тенденцію до пріоритизації кібербезпеки, що призводить до створення безпечнішої цифрової екосистеми для всіх зацікавлених сторін.

Ключові слова: *Республіка Ірландія, кібербезпека, інформаційна безпека, інформаційно-комунікаційні технології (ІКТ), ЄС, регулювання, «Загальний регламент щодо захисту даних», «Закон про захист даних».*

Вступ. Актуальність дослідження зумовлена тим, що сьогодні спостерігається тенденція до зниження ефективності традиційних методів захисту даних. Це робить необхідним пошук та впровадження нових, сучасних підходів. В умовах розвитку та масового впровадження програм і методів автоматизованої обробки даних питання захисту персональних даних набувають особливої актуальності. У зв'язку з використанням нових інформаційно-комунікаційних технологій (ІКТ) постає необхідність переосмислення права на захист даних та розробки нових міжнародних стандартів захисту від можливих зловживань. Як приклад для інших держав можна розглянути досвід Республіки Ірландія – країни-члена Європейського союзу (ЄС). Республіка Ірландія досягла значних успіхів у розвитку ІКТ і забезпеченні захисту інформації, включно з персональними даними. Цей досвід може бути корисним під час розроблення національних стратегій кібербезпеки та систем захисту інформації, зокрема в Україні.

Протягом останніх десятиліть Республіка Ірландія посіла лідируючі позиції у сфері технологій в світі. Для досягнення цих результатів було вжито стратегічних заходів, що включають залучення прямих іноземних інвестицій (ПІІ) у технологічні проекти, зниження корпоративних податків, а також використання соціально-культурних аспек-

тів. Було реалізовано тристоронній підхід, спрямований на зміцнення позицій Республіки Ірландія у світовому технологічному просторі. Однак для забезпечення стабільності та стійкості досягнутих результатів необхідна наявність надійного законодавства і політики, що регулюють кіберпростір.

Згідно з дослідженнями ірландської компанії «Gartner Ireland Ltd», що займається комерційними фізичними та біологічними дослідженнями і розробками, на 2024 р. 75% населення світу має доступ до своєї особистої інформації відповідно до правил конфіденційності. Величезні обсяги даних, що обробляються сьогодні, і зростаюча залежність від технологій підкреслюють гостру необхідність у забезпеченні безпеки даних. Правила роботи з даними допомагають встановити стандарти захисту конфіденційної інформації та сприяють прозорості, довірі та підзвітності. У більшості організацій та установ відсутній спеціалізований відділ, що займається питаннями конфіденційності. У зв'язку з цим відповідальність за дотримання відповідних вимог покладається на технології і, зокрема, на забезпечення безпеки. У зв'язку з розширенням сфери регулювання конфіденційності в десятках юрисдикцій у найближчі два роки багато організацій усвідомлюють необхідність впровадження програм забезпечення конфіденційності вже зараз. За оцінками «Gartner», у 2024 р. середній річний бюджет великих організацій на забезпечення конфіденційності перевищив 2,5 млн. доларів [1].

Мета та завдання. Головною метою статті є аналіз системи забезпечення захисту інформації у Республіці Ірландія. Ключові **завдання** полягають у визначенні особливостей регулювання сфери інформаційно-комунікаційних технологій, а також встановлені проблем та перспектив захисту персональних даних Республіки Ірландія як члена Європейського союзу в умовах стрімкого розвитку ІКТ технологій та глобалізації.

Методи дослідження. Під час дослідження та систематизації офіційних документів державних органів влади Республіки Ірландія, а також аналізу актуальних фактографічних даних було визначено ключові напрями формування системи кібербезпеки Республіки Ірландія, а також оцінено її потенціал і перспективи подальшого розвитку в контексті системи захисту інформації та персональних даних. У рамках дослідження було застосовано методи сучасної політології, історії та права. Динамічний характер змін у досліджуваній царині зумовив необхідність використання принципів всебічності, об'єктивності та цілісності як методологічної основи. Теоретико-методологічне підґрунтя дослідження містить загальнонаукові методи аналізу, синтезу, індукції та дедукції, а також системний метод, метод структурно-функціонального аналізу та правові методи в кібербезпеці.

Під час дослідження розвитку системи забезпечення кібербезпеки в контексті захисту персональних даних і конфіденційної інформації в Республіці Ірландія було застосовано історичний підхід. Це дало змогу розглянути еволюцію кібербезпеки як напряму наукових досліджень, основною метою якого є розробка та впровадження заходів, що забезпечують захист персональних даних, конфіденційності, цілісності та доступності інформації.

Для того щоб зрозуміти сутність інформаційної безпеки Республіки Ірландія, а також визначити перспективи та виклики, з якими стикається сучасна національна безпека ірландської держави, було застосовано системний підхід. Він дозволяє розглядати систему кібербезпеку як цілісну складну систему, що складається з підсистем та елементів, які знаходяться в постійній взаємодії.

Дослідження значної правової бази в межах регулювання системи захисту персональних даних та інформації обумовило використання міждисциплінарного підходу. У межах використання міждисциплінарного підходу було застосовано правові методи в кібербезпеці, які включають розроблення нормативно-правової бази, що регламентує відносини, пов'язані зі створенням, зберіганням, обміном і доступністю інформації, а також створення методичних рекомендацій, дотримання яких забезпечить збереження персональних даних та конфіденційної інформації.

Результати. Розвиток цифрових технологій у суспільстві відкриває широкі перспективи та надає безліч переваг. Завдяки Інтернету та мобільним мережам люди отримують можливість спілкуватися та обмінюватися інформацією, медіафайлами та даними в глобальному масштабі. Концепції електронного уряду можуть допомогти громадянам отримати доступ до величезної кількості інформації державного сектора, залишаючись при цьому на зв'язку з державними органами. Громадяни дедалі частіше отримують доступ до інформації та формують думку щодо політичних питань, які їх цікавлять, за допомогою цифрових джерел новин і соціальних мереж. Винахід і розвиток «Інтернету речей» (англ. Internet of things, IoT) сприяють створенню «розумних» міст і сервісів, що спрощують повсякденне життя. Триваючий перехід від готівки до електронних платіжних рішень сприяє подальшому прогресу та зручності.

Однак, в умовах стрімкого зростання та додаткових переваг кіберпростору існують різноманітні критичні ризики та шкідливий потенціал. Розширення можливостей підключення як у цифровому, так і у фізичному просторі, а також розробка нових пристроїв, таких як «Інтернет речей» сприяють збору додаткових цифрових даних. Цифрові досьє вже створюються сьогодні за допомогою вбудо-

ваних налаштувань за замовчуванням і сервісів та додатків, що порушують конфіденційність.

З розвитком безлічі взаємопов'язаних цифрових сервісів, платформ і просторів такі цифрові досьє набуватимуть дедалі більшого значення. Вони слугують або інструментом для вчинення кіберзлочинів, зокрема цифрового шахрайства з використанням крадіжки особистих даних або інформації про відсутність удома, небажаного розголосу або вразливостей у системі безпеки для вчинення шахрайських дій, або об'єктом таких злочинів. У всьому світі визнано, що ключовим елементом кібербезпеки є захист усіх цифрових пристроїв. Однак наслідки незаконного опрацювання або розкриття даних також потребують уваги. Конфіденційність та захист даних, а також інформаційна безпека не обмежуються сферою інтересів будь-якої групи або конкретної мережі – вони є обов'язком кожного [2].

У міжнародному співтоваристві Республіка Ірландія часто сприймається як країна, яка жертвує захистом приватного життя на користь національних економічних переваг. Прагнення Республіки Ірландія залучити прямі іноземні інвестиції (ПІІ) для розвитку інформаційно-комунікаційних технологій призвело до лібералізації законодавчо-правової бази. У результаті такого підходу було сформовано недостатньо вимогливу правову основу, яка раніше сприяла залученню інвестицій до Республіки Ірландії та забезпечувала країні конкурентну перевагу на міжнародній арені. Згодом це почало створювати ризики для майбутніх інвестицій. Проте з 2014 р. ситуація змінилася. Республіка Ірландія має один із найкращих у Європі наглядових органів за показником фінансування на душу населення. Це не означає, що всі проблеми розв'язано, оскільки ірландський регулятор має екстериторіальне охоплення і має розглядати фінансування на користувача, а не обмежуватися населенням Республіки Ірландія [3].

У цьому контексті важливим етапом на шляху до захисту персональних даних та інформації стало ухвалення 25 травня 2018 р. постанови ЄС, що посилює та уніфікує захист персональних даних усіх осіб у ЄС – «Загальне положення про захист даних ЄС» (англ. General Data Protection Regulation, GDPR). Основна мета цього положення полягає в тому, щоб дати громадянам контроль над власними персональними даними та спростити нормативну базу для міжнародних економічних відносин через уніфікацію регулювання в рамках ЄС. У законі розширено поняття персональних даних, запроваджено поняття транскордонної передачі даних, встановлено низку прав суб'єктів персональних даних, визначено роль посадової особи із захисту даних. «Загальний регламент щодо захисту даних ЄС» може бути застосовано не лише до країн-учасниць ЄС, а й до будь-якої юридичної особи, яка обробляє персональні дані осіб ЄС [4].

Кібербезпека в Республіці Ірландія регулюється законодавством, спрямованим на захист персональних даних і підвищення загальної безпеки цифрових інфраструктур. Основоположним елементом цієї системи є «Закон про захист даних» 2018 р. (англ. Data Protection Act). «Закон про захист даних» ґрунтується на «Загальних положеннях про захист даних ЄС», який, як зазначалося вище, встановлює правові стандарти для обробки, опрацювання та зберігання особистої інформації. Відтак, «Закон про захист даних» є нормативним актом, що регулює питання захисту даних і конфіденційності в Республіці Ірландія [5].

Загалом «Закон про захист даних» встановлює правові стандарти для обробки, зберігання та передачі персональних даних. Цей закон лежить в основі дотримання Республікою Ірландія «Загального регламенту щодо захисту даних» – всеосяжного регламенту, що діє на території ЄС. «Загальний регламент щодо захисту даних» встановлює суворі вимоги до організацій щодо згоди, прав доступу до даних і протоколів повідомлення про порушення, тим самим істотно впливаючи на те, як підприємства управляють персональними даними в контексті кібербезпеки Таким чином, «Закон про захист даних» дає подальшу дію «Загальному положенню про захист даних ЄС» в Республіці Ірландія та адаптує його положення під національний контекст [5].

На додаток до «Закону про захист даних» і «Загального регламенту щодо захисту даних», «Директива про безпеку мережевих та інформаційних систем» (англ. Security of Network and Information Systems, NIS) відіграє вагому роль у формуванні політики кібербезпеки в Республіці Ірландія. Ця директива спрямована на забезпечення того, щоб постачальники основних послуг і цифрових послуг вживали належних заходів безпеки для управління ризиками та реагування на інциденти. «Директива про безпеку мережевих та інформаційних систем» зобов'язує операторів повідомляти про значні інциденти національній владі, тим самим сприяючи формуванню культури прозорості та попереджувального управління ризиками. Директива охоплює такі сектори, як енергетика, транспорт і охорона здоров'я, накладаючи зобов'язання, які роблять внесок у загальний стан безпеки організацій, що працюють у цих галузях [6].

Також у сфері інформаційної безпеки в Республіці Ірландія діє «Закон про кримінальне правосуддя (злочини, пов'язані з інформаційними системами) 2017 р.» (англ. Criminal Justice (Offences Relating to Information Systems) Act 2017). Він визначає конкретні кримінальні злочини, пов'язані з кіберзлочинами, такими як хакерство, фішинг, електронна крадіжка та інші. Основна мета цього

закону – привести в дію положення «Директиви ЄС 2013/40/ЄС» про атаки на інформаційні системи. Закон вводить нові злочини, пов'язані з: несанкціонованим доступом до систем даних; втручанням в інформаційні системи або в дані на них; перехопленням передання даних з інформаційної системи; використанням інструментів для вчинення таких злочинів [7].

Ухвалення «Закону про кримінальне правосуддя (про злочини, пов'язані з інформаційними системами) 2017 р.» («Закон 2017 р.») може видатися своєчасним і доречним з огляду на великомасштабні хакерські атаки та кіберзлочини, від яких останніми роками страждає весь світ. Однак насправді «Закон 2017 р». уже давно перебуває в законодавчому порядку денному Республіки Ірландія. «Закон 2017 р»., врешті-решт, приводить у дію низку зобов'язань, які Республіка Ірландія взяла на себе на рівні ЄС та міжнародному рівні (наприклад, відповідно до «Конвенції Ради Європи про кіберзлочинність» та «Директиви ЄС про кіберзлочинність»), що вимагають від Республіки Ірландія запровадити у національному законодавстві конкретні злочини, пов'язані зі зломом та іншими шкідливими видами кібердіяльності [8].

Незважаючи на те, що в законодавстві Республіки Ірландія протягом багатьох років існували злочини, пов'язані з комп'ютерними технологіями, ці злочини були створені в рамках законодавства, спрямованого на боротьбу з іншими видами злочинів (такими як заподіяння шкоди, крадіжка і шахрайство). У результаті вони не дуже добре підходять для переслідування за кіберзлочини і, мабуть, недостатньо гнучкі, щоб відповідати поточним змінам у цій галузі. Закон усуває ці недоліки національного законодавства, створюючи в Республіці Ірландія спеціальні і більш технологічно орієнтовані склади злочинів, пов'язаних з кіберзлочинами. З міжнародної точки зору цей закон також приведе Республіку Ірландія у відповідність до міжнародних зобов'язань і зобов'язань на рівні ЄС у цій галузі [8].

Важливість перерахованих законодавчих заходів виходить за рамки дотримання вимог і передбачає комплексний підхід до оцінки ризиків, реагування на інциденти та захисту даних. Організації зобов'язані постійно контролювати й удосконалювати свої методи забезпечення кібербезпеки, включно з навчанням співробітників і впровадженням надійних технологій. Дотримання цих правил не тільки знижує ризик кіберінцидентів, а й підвищує довіру між зацікавленими сторонами та клієнтами, що в кінцевому підсумку забезпечує конкурентну перевагу на цифровому ринку [9].

У зв'язку із залежністю від цифрових технологій, що зростає і збільшенням кількості кіберзагроз, законодавство Республіки Ірландія зобов'язує організації вживати конкретних заходів для забезпечення безпеки конфіденційних даних і дотримання правил кібербезпеки. Ці заходи охоплюють як технічні, так і організаційні аспекти, які в сукупності формують комплексну стратегію кібербезпеки – «Національну стратегію кібербезпеки Республіки Ірландія на 2019–2024 рр.» [10].

Одним із найважливіших технічних заходів, передбачених законодавством Республіки Ірландія, є шифрування. Організаціям рекомендується використовувати протоколи шифрування для зберігання і передачі даних, щоб конфіденційна інформація залишалася в безпеці навіть у разі витоку даних. Крім того, брандмауери відіграють ключову роль у захисті внутрішніх мереж від зовнішніх атак. Ретельно налаштовуючи брандмауери, організації можуть створити захищений периметр, що обмежує несанкціонований доступ і пропускає легітимний трафік [11].

Контроль доступу є ще одним важливим елементом системи безпеки. Впровадження суворих політик контролю доступу забезпечує доступ до систем і даних тільки авторизованому персоналу, що знижує ризик внутрішніх загроз і випадкового розкриття інформації. Це часто включає в себе багатофакторну аутентифікацію, яка підвищує безпеку облікових записів користувачів, вимагаючи додаткових кроків перевірки, крім пароля [11].

Крім технічних заходів, навчання співробітників основам інформаційної безпеки відіграє ключову роль у формуванні культури кібербезпеки в організації. Співробітники мають бути обізнані про потенційні загрози, як-от фішинг і соціальна інженерія, щоб мати можливість розпізнавати підозрілі дії та реагувати на них відповідним чином. Регулярні тренінги допоможуть забезпечити всіх членів команди необхідними знаннями для захисту від кіберзагроз. Впровадження таких заходів, як шифрування, використання брандмауерів, контроль доступу та навчання персоналу, дає змогу організаціям створити надійну систему кібербезпеки, яка не тільки відповідає вимогам законодавства, а й захищає активи компанії, а також зміцнює довіру клієнтів і партнерів. Такий комплексний підхід вкрай важливий у сучасному цифровому світі, де кіберзагрози постійно розвиваються і стають дедалі витонченішими [12].

У Республіці Ірландія діють зобов'язання щодо повідомлення про порушення кібербезпеки. В ірландській державі зобов'язання щодо інформування про порушення кібербезпеки регулюються насамперед згадуваними вище – «Загальним регламентом щодо захисту даних» і «Законом про захист даних» 2018 р. [12]. На основі «Загального регламенту щодо захисту даних ЄС» в Республіці Ірландія засновано нову організацію – «Комісію із захисту даних» (англ. Data Protection Commission). Це незалежний національний орган, який забезпечує конфіденційність персональних даних грома-

дян і регулює обробку персональних даних відповідно до встановлених вимог і положень [13].

Організації, що зіткнулися з витоком даних, зобов'язані повідомити «Комісію із захисту даних» Республіки Ірландія без невиправданих затримок і, за можливості, протягом 72 годин після того, як їм стало відомо про витік. Таке обов'язкове інформування спрямоване на забезпечення своєчасного реагування на інциденти, що вкрай важливо для мінімізації потенційного збитку для постраждалих осіб [12].

У разі виникнення витоку даних організації повинні оцінити характер і масштаби інциденту. Це охоплює визначення персональних даних, категорій і кількості порушених осіб, а також наслідків витоку. Якщо витік даних становить загрозу для прав і свобод фізичних осіб, організації також зобов'язані без зволікання інформувати постраждалих. Це повідомлення має містити детальну інформацію про характер витоку, його можливі наслідки та вжиті або запропоновані заходи щодо усунення витоку.

Документація відіграє найважливішу роль у процесі реагування на порушення. Організації зобов'язані вести докладні записи про всі порушення, незалежно від того, чи були вони повідомлені в «Комісію із захисту даних». Така документація повинна включати факти, пов'язані з порушенням, його наслідки та вжиті заходи щодо виправлення ситуації. Ці записи можуть слугувати не лише важливим інструментом для дотримання законодавства, а й джерелом інформації для поліпшення заходів кібербезпеки в майбутньому. Аналіз попередніх інцидентів допоможе вдосконалити стратегію кібербезпеки організації і тим самим підвищити її захист від потенційних порушень у майбутньому [11].

Таким чином, дотримання зобов'язань щодо інформування про порушення кібербезпеки вкрай важливе для організацій в Республіці Ірландія. Ці вимоги не тільки сприяють дотриманню нормативних вимог, а й формують культуру відповідальності та постійного вдосконалення методів забезпечення кібербезпеки.

«Комісія із захисту даних» Республіки контролює застосування «Загальних положень про захист даних» ЄС, а також має функції та повноваження, пов'язані з іншими важливими нормативними системами. До них відносяться «Правила електронної конфіденційності» Республіки Ірландія 2011 р. і «Директива ЄС щодо правоохоронної діяльності». «Комісія із захисту даних» Республіки Ірландія також сприяє підвищенню обізнаності громадськості щодо правил і прав, пов'язаних з обробкою даних. Вона надає інформацію про права на захист даних, веде список операцій з обробки, які потребують оцінки впливу на захист, обробляє скарги і проводить розслідування, пов'язані з дотриманням закону про захист даних [13].

Отже, «Комісія із захисту даних» Республіки Ірландія відіграє важливу роль у забезпеченні дотримання законодавства та правил кібербезпеки. «Комісія із захисту Даних» створена для забезпечення дотримання законів про захист даних і стежить за тим, як організації поводяться з персональними даними, а також захищає конфіденційність громадян країни. Її роль особливо значуща в контексті «Загального регламенту щодо захисту даних» і «Закону про захист даних» Республіки Ірландія від 2018 р., які визначають стандарти обробки даних і протоколи безпеки, яких повинні дотримуватися організації.

Для забезпечення ефективного правозастосування «Комісія із Захисту Даних» проводить ретельні розслідування витоків даних і заяв про недотримання вимог. Коли стає відомо про потенційне порушення, Комісія ініціює розслідування, які можуть включати в себе вивчення документації, опитування співробітників і оцінку загальної практики захисту даних в організації, що розглядається. Ці розслідування мають вирішальне значення для виявлення областей, в яких організації можуть не відповідати необхідним стандартам кібербезпеки. «Комісія із захисту даних» має право вимагати вжиття заходів щодо виправлення ситуації, тим самим гарантуючи, що організації приведуть свою діяльність у відповідність до чинних правил [14].

Крім того, «Комісія із захисту даних» активно стежить за дотриманням вимог за допомогою регулярних перевірок та оцінок. Такий постійний нагляд дає змогу Комісії притягати організації до відповідальності за методи оброблення даних, тим самим формуючи культуру дотримання вимог і забезпечення безпеки. Якщо буде встановлено, що організація не дотримується вимог, у розпорядженні Комісії є різноманітні заходи, включно з накладенням штрафів, приписами змінити методи обробки даних і навіть порушенням судового розгляду в разі потреби. Можливість накладати значні штрафи підкреслює важливість дотримання правил кібербезпеки. Завдяки цим правозастосовним заходам Комісія відіграє важливу роль у просуванні передових методів захисту даних, тим самим покращуючи загальну ситуацію з кібербезпекою в Республіці Ірландія [14].

Необхідно зазначити, що в деяких випадках, залежно від характеру та обставин обробки персональних даних «Загальний регламент щодо захисту даних» ЄС може не застосовуватися. Замість цього можуть застосовуватися інші правові рамки, що регулюють обробку персональних даних. Конституція Республіки Ірландія не прямо передбачає право на конфіденційність, але суди визнали це право як одне з особистих прав у Конституції.

Відповідно до правил кібербезпеки, встановлених в Республіці Ірландія, недотримання вимог може призвести до серйозних і різноманітних наслідків. Організації, які не дотримуються цих правил, зокрема «Загального регламенту щодо захисту даних», можуть бути піддані значним фінансовим санкціям. Відповідно до «Загального регламенту щодо захисту даних», максимальний штраф може сягати 20 млн. євро або 4% від річного світового обороту, залежно від того, яка сума більша. Цей суворий механізм правозастосування відображає серйозне ставлення до захисту даних і кібербезпеки в Республіці Ірландія [15].

Крім фінансових наслідків, організації можуть зіткнутися з судовими позовами через недотримання встановлених правил. Постраждалі особи можуть подати до суду на відшкодування шкоди, заподіяної витоком персональних даних, що може призвести до дуже коштовних судових розглядів. Також, регулюючі органи, такі як «Комісія із захисту даних» Республіки Ірландія, мають право розслідувати витоки та накладати санкції, що підвищує ймовірність судових розглядів.

Наслідки недотримання вимог виходять за рамки юридичної та фінансової сфер і тягнуть за собою серйозну репутаційну шкоду. Організації, що порушують правила кібербезпеки, ризикують втратити довіру клієнтів і зацікавлених сторін. Такий підрив довіри громадськості може перешкоджати утриманню та залученню клієнтів, тим самим чинячи довгостроковий негативний вплив на становище організації на ринку та її доходи. Крім того, негативний розголос, пов'язаний із витоком даних або штрафними санкціями, може негативно позначитися на партнерських відносинах і майбутніх можливостях для бізнесу. У сучасну цифрову епоху, коли споживачі дедалі більше обізнані про свої права на дані, дотримання нормативних вимог має вирішальне значення для підтримання авторитету організації.

У якості ілюстрації вищезазначених штрафів можна навести рішення «Комісії із захисту даних» Республіки Ірландія, яка наклала значний штраф у розмірі 310 млн. євро на компанію «LinkedIn» – платформу соціальних мереж для професіоналів – за порушення європейських правил конфіденційності даних. Розслідування було зосереджене на тому, як «LinkedIn» обробляє персональні дані користувачів для таргетованої реклами та поведінкового аналізу, зокрема, на законності, прозорості та справедливості цих методів відповідно до «Загального регламенту щодо захисту даних» ЄС [16].

Цей значний штраф демонструє прихильність ЄС суворим стандартам захисту даних і свідчить про постійний контроль за цифровими платформами, що обробляють великі обсяги користувацьких даних. Рішення, ухвалене за результатами всебічного розслідування, включає додаткові вимоги до «LinkedIn» щодо коригування методів обробки даних відповідно до вимог «Загального регламенту щодо захисту даних» ЄС. «Комісія із захисту даних» Республіки Ірландія, що виступає в якості головного наглядового органу «LinkedIn» в ЄС, почала розслідування після отримання скарги від «Управління із захисту даних» Франції. Під час розслідування було вивчено використання «LinkedIn» персональних даних для двох основних цілей: поведінкового аналізу і таргетованої реклами. Ці методи передбачають використання даних користувачів, які створили профілі в «LinkedIn». У зв'язку з цим виникли питання про прозорість і згоду на обробку даних у «LinkedIn» [16].

Іншою резонансною справою, розглянутою «Комісією із захисту даних» Республіки Ірландія у 2023 р., стали штрафні санкції щодо компанії «Meta» у розмірі 390 млн. євро за рекламу на основі користувацьких даних у соціальних мережах «Facebook» та «Instagram». У результаті «Meta» більше не може показувати рекламу з використанням персональних даних користувачів без їхньої явної згоди. Це рішення було ухвалено тільки після масових протестів з боку решти 26 уповноважених із захисту даних з інших європейських країн. Своєю чергою «Європейська рада із захисту даних» (англ. European Data Protection Board, EDPB) заборонила «Meta» «обходити» згоду «Загального регламенту щодо захисту даних» за допомогою пункту у своїх положеннях і умовах. У підсумку компанія «Meta» повинна отримувати «активну» згоду на персоналізовану рекламу і пропонувати користувачам можливість «так/ні» для персоналізованої реклами. Інакше кажучи, «Meta» («Facebook», «Instagram», «WhatsApp») не зможе в майбутньому використовувати персональні дані для реклами в ЄС так, як раніше. Це серйозний удар по бізнес-моделі «Meta» в Європі, який у довгостроковій перспективі може вплинути на основний бізнес групи [17].

Таким чином, штрафи і наслідки за недотримання правил кібербезпеки в Республіці Ірландія значні і включають фінансові зобов'язання, юридичні ризики та репутаційний збиток. Розуміння серйозності цих правил вкрай важливе для організацій, що працюють у цій юрисдикції. У контексті діяльності «Комісії із захисту даних» важливо відзначити, що співпраця Республіки Ірландія як країни-члена ЄС з державами, які не є членами ЄС, у сфері захисту персональних даних ґрунтується на праві ЄС, що регламентує захист персональних даних, та угодах, які укладаються спеціально в цій сфері. Найдинамічніше таке співробітництво розвивається зі США. Від самого початку співробітництво будувалася на відповідній угоді, укладеній з урахуванням норм «Директиви 95/46/ЄС»

Європейського Парламенту та Ради ЄС щодо захисту приватних осіб під час обробки персональних даних та вільного переміщення таких даних від 24 жовтня 1995 р. Відповідно до неї до кінця 2015 р. США входили до обмеженого переліку країн, у яких Європейською комісією було визнано наявність достатнього рівня захисту персональних даних і винесено «рішення про адекватність» (англ. adequacy decision). Поряд зі США до цього переліку входять Андорра, Аргентина, о-ви Гернсі, Джерсі та Мен, Ізраїль, Канада, Нова Зеландія [18].

Щодо США таке рішення вперше було прийнято у 2000 р. З огляду на це між ЄС і США було укладено угоду про «Безпечну гавань», відповідно до якої з ЄС до США допускалося передання персональних даних громадян ЄС операторам, що сертифікувалися при Міністерстві торгівлі США, оскільки сертифіковані організації забезпечують належний рівень конфіденційності та безпеки персональних даних, які передаються, а також відповідні до стандартів ЄС умови їхнього збереження. Однак використання механізму «Безпечної гавані» було поставлене під сумнів і фактично анульоване Рішенням Суду ЄС у справі – «Максиміліан Шремс проти Уповноваженого з питань захисту даних» (англ. Maximillian Schrems v Data Protection Commissioner) від 6 жовтня 2015 р., що стало важливою віхою у визначенні нових підходів до вибудовування співробітництва ЄС із третіми країнами в питаннях захисту персональних даних, зокрема й зі США [19].

Приводом для розгляду став позов австрійського студента М. Шремса до Верховного суду Республіки Ірландія проти «Комісії із захисту даних» Республіки Ірландія. Уомісія відхилила вимогу австрійця призупинити передачу його персональних даних з ірландської філії американської компанії «Facebook» до її головного офісу на території США. З посиланням на викриття Е. Сноудена, М. Шремс вказував на недостатній, на його думку, рівень захисту персональних даних на американській території, зокрема через необмежений доступ спецслужб США до облікових записів користувачів соцмережі. Суддям належало визначити, чи може ухвалене у 2000 р. Рішення Європейської комісії про адекватність рівня захисту персональних даних у США перешкоджати національному наглядовому органу Республіки Ірландія в розгляді скарги фізичної особи на правопорушення у сфері захисту персональних даних під час передання її даних до третьої країни, і, в разі необхідності, призупинення такого передання даних [20].

Суд підтвердив повноваження національних регуляторів держав-членів розглядати такого роду скарги, навіть якщо рівень захисту персональних даних у цій третій країні було визнано таким, що відповідає стандартам ЄС. Більше того, Суд визнав нелегітимним саме «рішення Європейської комісії про адекватність» щодо США в рамках так званої домовленості про «Безпечну гавань» 2000 р., оскільки воно не накладало жодних обмежень на доступ держорганів США до персональних даних громадян ЄС (хоча згідно з нормами права ЄС таке обмеження для компетентних органів держав-членів існувало). Та обставина, що американські спецслужби мали необмежений доступ до змісту електронного листування користувачів з ЄС, на думку суддів, має розглядатися як підрив фундаментального права на недоторканність приватного життя. А відсутність у громадян ЄС можливості відстоювати свої інтереси на американській території в разі правопорушень у сфері захисту персональних даних порушує їхнє право на ефективний судовий захист.

Рішення Суду ЄС від 6 жовтня 2015 р. стало значущим моментом у відносинах ЄС–США у сфері захисту персональних даних. З урахуванням рішення Європейської комісії була змушена піти на заходи, на які доти не наважувалася – анулювати угоду про «Безпечну гавань». Позиція Суду ЄС стала важливим аргументом у переговорах між ЄС і США з питань захисту персональних даних. Вона стала основою для розробки нового регулювання системи персональних даних за межами ЄС. Відповідно до цього рішення, до системи включено норми про захист громадян ЄС в разі порушень у сфері захисту персональних даних. Крім того, посилено вимоги до американських компаній, представлених на ринку ЄС, в частині дотримання норм права ЄС про захист персональних даних. Також запроваджено обов'язковий щорічний огляд результатів моніторингу системи передавання даних з ЄС до США. Крім того, Європейська комісія як одну з обов'язкових умов укладення міжнародних угод із третіми країнами про співробітництво в галузі передання та захисту персональних даних взяла до уваги вказане Рішення Суду та висунула вимогу забезпечення гарантій незалежного статусу іноземного наглядового органу у сфері захисту персональних даних [3].

У контексті вищезазначеного цікавим є те, що одним із найбільш спірних аспектів розслідування, проведеного «Facebook», став спосіб розгляду скарг. Два аудиторські звіти не були офіційними рішеннями за скаргами, поданими М. Шремсом. Замість цього «Комісія із захисту даних» охарактеризувала їх як форму співпраці з «Facebook», результатом якої стали рекомендації, а не вимоги. Це відображає загальне прагнення «Комісії із захисту даних» уникати «змагальних процесів правозастосування, надаючи перевагу дотриманню вимог за допомогою м'яких інструментів правозастосування» [21].

У цьому підході немає нічого поганого, і в розглянутій ситуації він призвів до низки позитивних змін у практиці забезпечення конфіденційності

даних у «Facebook». Дійсно, європейська модель захисту даних передбачає, що наглядові органи виконують низку дублюючих функцій. Британські вчені К. Беннетт і Ч. Рааб описують та порівнюють ці функції як «різні ролі омбудсмена, аудитора, консультанта, педагога, парламентера, радника з питань політики та правозастосовника» [22]. Своєю чергою американський дослідник ірландського походження У. МакГеверан стверджує, що розслідування діяльності «Facebook» слід розглядати як успішний приклад оперативного регулювання. Це стосується не лише самих перевірок, а й встановлення постійних відносин співпраці з регулюючим органом [21].

Однак, незважаючи на це, перевірки виявляють проблеми, пов'язані з неформальними процесами. У 2014 р. М. Шремс відкликав 22 з 23 скарг, висловивши розчарування підходом «Комісії із захисту даних» Республіки Ірландія, який, на його думку, не забезпечував формальних рішень, не надавав процедурної справедливості, відмовляв йому в доступі до матеріалів, наданих «Facebook» із порушених питань, змішував «кращу практику» з вимогами закону та ухвалював інтерпретації закону, які суперечили консенсусному розумінню «Директиви про захист даних», ухваленій іншими органами ЄС із захисту даних [20]. Основною критикою було те, що до 2014 р., через майже три роки після подання багатьох скарг, М. Шремс так і не отримав офіційного рішення. Крім того, він підкреслив, що завдання центру обробки даних – знайти мирне розв'язання проблеми, що сприяє індивідуальному підходу до вирішення системних питань. Як зазначив М. Шремс, «нашої метою є перевірка «Facebook Ireland Ltd.» на предмет дотримання прав усіх користувачів відповідно до законодавства ЄС» [9].

Отже, у сфері регулювання даних в Республіці Ірландія спостерігається тенденція до надання переваги співпраці та неформальним заходам впливу замість формального судового розгляду. Цей підхід характерний не тільки для «Комісії із захисту даних», а й для інших ірландських регулюючих органів. Така практика зумовлена низкою чинників, включно зі встановленим законом зобов'язанням домагатися мирової угоди, обмеженими ресурсами відомства і високою вартістю судових розглядів в Республіці Ірландія. Однак, як показує випадок із М. Шремсом, неформальна взаємодія може поставити під загрозу роль регулюючого органу в розгляді скарг про порушення основних прав.

Скарга М. Шремса містить інформацію про недоліки в роботі «Комісії із захисту даних» Республіки Ірландія, зокрема, про тенденцію до надмірно вузького та ухильного тлумачення законодавства. Скарга була подана після викриттів Е. Сноудена і містила прохання до «Комісії із захисту даних» вжити заходів щодо заборони передання персональних даних із «Facebook Ireland Ltd.» до «Facebook Inc.» на підставі того, що законодавство США не забезпечує належного захисту цих даних, особливо від програм масового стеження. Однак «Комісія із захисту даних» вважала, що не має права проводити розслідування на підставі рішення Комісії «Безпечної гавані» від 2000 р., яке дозволяло передачу даних до США за певних обставин, і відхилила скаргу як «легковажну і прикру». Після судового перегляду і попереднього посилання Європейський суд не погодився з цим рішенням і постановив, що «національний наглядовий орган зобов'язаний розглянути скаргу з усією ретельністю» і, якщо необхідно, має «порушити судовий розгляд для захисту прав людини» [3].

Ірландська дослідницька та консалтингова компанія «Gartner Ireland Ltd», що спеціалізується на ринку інформаційних технологій, виявила п'ять тенденцій у сфері конфіденційності, які є актуальними на 2024 р. Ці тенденції не лише підтримують практику конфіденційності, а й допомагають керівникам компаній зробити їх привабливішими, більш значущими та такими, що швидко приносять прибуток [1].

1. Локалізація даних. В умовах цифровізації та глобалізації прагнення контролювати країну, на території якої знаходяться дані, може здатися нелогічним. Однак такий контроль може бути або обов'язковою вимогою, або побічним ефектом багатьох нових законів про захист персональних даних. Ризики, пов'язані з міжнародною бізнес-стратегією, вимагають нового підходу до вибору і придбання хмарних сервісів у всіх моделях обслуговування. Керівники служб безпеки та управління ризиками стикаються з нерівномірним нормативно-правовим регулюванням у різних регіонах, що вимагає розробки різних стратегій локалізації. У результаті планування локалізації даних стає ключовим аспектом при виборі та придбанні хмарних сервісів.

2. Методи обчислень, що підвищують конфіденційність. Обробка даних у ненадійних середовищах, таких як загальнодоступна хмарне сховище, а також багатосторонній обмін даними та аналітика стали основою успіху організації. Складність механізмів і архітектур аналітики, що зростають вимагає від постачальників впровадження вбудованих функцій забезпечення конфіденційності. Розвиток технологій штучного інтелекту та необхідність їх навчання є лише додатковим аспектом проблеми забезпечення конфіденційності. На відміну від звичайних засобів захисту даних, що зберігаються в резервних копіях, «обчислення, що підвищують конфіденційність» (англ. privacy-enhancing computation, PEC), захищають дані в процесі використання.

У результаті організації можуть впроваджувати обробку даних і аналітику, які раніше були неможливі через проблеми з конфіденційністю або безпекою. За прогнозами «Gartner», у 2025 р. 60% великих організацій використовуватимуть хоча б одну технологію «обчислень, що підвищують конфіденційність» в аналітиці, бізнес-аналітиці та хмарних обчисленнях.

3. Управління штучним інтелектом. Опитування, проведене компанією «Gartne»r, показало, що 40% організацій стикалися з порушенням конфіденційності під час використання штучного інтелекту (ШІ), і що тільки одне з чотирьох таких порушень було навмисним. Незалежно від того, чи використовують організації модуль на основі ШІ, інтегрований у пропозицію постачальника, чи окрему платформу, керовану внутрішньою командою спеціалістів з опрацювання даних, існують ризики, пов'язані з конфіденційністю та потенційним неправомірним використанням персональних даних. В даний час значна частина ШІ, що використовується в організаціях, інтегрована у більші системи. Це ускладнює оцінку його впливу на конфіденційність даних. Вбудовані можливості ШІ використовуються для відстеження поведінки співробітників, оцінки настроїв споживачів і створення «розумних» продуктів, які швидко навчаються. Більше того, дані, які сьогодні надходять у ці моделі навчання, впливатимуть на рішення, які ухвалюватимуть через роки. У разі відсутності належного регулювання у сфері ШІ існує ризик безконтрольного поширення шкідливих даних, отриманих без використання відповідних інструментів управління ШІ. Це може призвести до необхідності масової заміни систем в ІТ-відділах, що спричинить значні фінансові втрати для компаній і негативно позначиться на їхній репутації.

4. Централізований потік конфіденційності. Попит споживачів, що зростає на права суб'єктів і підвищені очікування щодо прозорості призведуть до необхідності «централізованого користувацького досвіду в галузі конфіденційності» (англ. centralized privacy user experience, UX). Прогресивні організації розуміють, що об'єднання всіх аспектів користувацького інтерфейсу для забезпечення конфіденційності – сповіщень, файлів «cookie», управління згодою та опрацювання запитів на надання прав суб'єктів (англ. Subject rights requests, SRR) – в одному порталі самообслуговування – є перевагою. Такий підхід зручний для ключових учасників, клієнтів і співробітників і дає змогу значно заощадити час і кошти.

5. Управління на відстані стає більш різноманітним. В умовах, коли моделі взаємодії на роботі та в повсякденному житті стають гібридними, зростає потреба в ретельнішому відстеженні, моніторингу та обробці персональних даних. Це, своєю чергою, підвищує ризик порушення конфіденційності. Завдяки впливу гібридних моделей взаємодії на конфіденційність, продуктивність і задоволеність балансом між роботою та особистим життям підвищилися в різних галузях і дисциплінах. Організації повинні застосовувати підхід, орієнтований на людину, до питань конфіденційності. Дані моніторингу слід використовувати мінімально і тільки з чіткими цілями, як-от поліпшення умов праці співробітників за рахунок усунення непотрібних перешкод або зниження ризику вигорання за рахунок виявлення потенційних ризиків для благополуччя [1].

На підставі вищевикладеного можна зробити попередній висновок про те, що організаціям в Республіці Ірландія необхідно впроваджувати передові методи для забезпечення дотримання правил кібербезпеки, що діють у країні. Одним з основних методів є проведення регулярних перевірок безпеки. Ці перевірки дають змогу виявляти вразливості в системах і процесах організації та своєчасно усувати їх. Постійний моніторинг та оцінювання не тільки забезпечують дотримання вимог, а й сприяють формуванню культури кібербезпеки в організації. Навчання співробітників – ще одна важлива сфера, якій організаціям слід приділяти першочергову увагу. Комплексні програми навчання дають співробітникам навички та знання, необхідні для розпізнавання потенційних загроз безпеці, як-от фішингові атаки та шкідливе програмне забезпечення. Регулярні семінари, що стосуються нових загроз, можуть знизити ризик людської помилки, яка є поширеним чинником багатьох порушень безпеки. Крім того, організаціям слід забезпечити, щоб політика кібербезпеки була добре задокументованою та легкодоступною для всіх співробітників.

Для організацій, що працюють із персональними даними, вкрай важливо призначити «відповідального за захист даних» (англ. data protection officer). Відповідальна особа здійснюватиме контроль за дотриманням правил захисту даних відповідно до «Загального регламенту щодо захисту даних». Також вона буде контактною особою для власників даних і регулюючих органів. Ця роль вкрай важлива для забезпечення прозорості обробки даних та ефективного реагування на будь-які витоки даних. Планування реагування на інциденти – ще одна ключова практика. Організації слід розробити надійний план реагування на інциденти, в якому будуть викладені чіткі протоколи дій під час інциденту, пов'язаного з кібербезпекою. Цей план має включати конкретні ролі та обов'язки співробітників, а також стратегії комунікації, спрямовані як на внутрішні зацікавлені сторони, так і на зовнішні, наприклад, на клієнтів і регулюючі органи. Необхідно регулярно проводити навчання, щоб переконатися, що організація готова швидко й ефективно реагувати на потенційні інциденти [11].

Останніми роками нормативно-правова база у сфері кібербезпеки в Республіці Ірландія та ЄС загалом стрімко змінюється. Організації все частіше усвідомлюють необхідність адаптуватися до різних нових тенденцій, які змінюють нормативно-правову базу у сфері кібербезпеки. Однією з найбільш значущих тенденцій є використання штучного інтелекту (ШІ) у сфері кібербезпеки. У міру того, як технології ШІ стають дедалі більш інтегрованими в бізнес-операції, їх також використовують для посилення заходів безпеки, оцінювання ризиків і виявлення потенційних загроз. Таким чином, регулюючі органи зосередилися на розробленні керівних принципів, що регулюють етичне використання ШІ у сфері кібербезпеки, щоб організації дотримувалися вимог під час використання цих передових технологій [11].

Ще одна примітна тенденція – посилення правил, безпосередньо пов'язаних із кібербезпекою. ЄС активно розробляє такі нормативно-правові акти, як «Загальний регламент щодо захисту даних» і «Закон про цифрові послуги» (англ. Digital Services Act, DSA), які підкреслюють важливість захисту персональних даних і встановлюють чіткі зобов'язання для компаній. У Республіці Ірландія організації зобов'язані дотримуватися встановлених правил, оскільки їх недотримання може спричинити значні фінансові втрати та шкоду репутації. Нормативно-правове середовище, що змінюється вимагає від компаній не тільки розуміння наявних правил, а й прогнозування майбутніх нормативних вимог, які можуть з'явитися у відповідь на загрози кібербезпеки, що розвиваються [11].

Крім того, характер загроз кібербезпеці постійно змінюється у зв'язку з розвитком технологій та методів, які використовуються кіберзлочинцями. Поява складних кібератак і загроз, таких як програми-здирники та фішингові схеми, змушує організації регулярно переглядати свої стратегії кібербезпеки. Організації можуть підготуватися до майбутніх змін у законодавстві, формуючи культуру поінформованості про кібербезпеку, інвестуючи в надійні інфраструктури безпеки та впроваджуючи комплексні програми навчання для своїх співробітників. Адаптуючись до цих нових тенденцій, організації можуть не тільки дотримуватися нормативних вимог, але й ефективно захищатися від кіберзагроз, що розвиваються [11].

Сьогодні, в умовах активного розвитку інформаційно-комунікаційних технологій, питання забезпечення безпеки персональних даних набувають особливої значущості. У зв'язку з цим особливого значення набувають етичні аспекти і тенденції, пов'язані з даною проблематикою. Правові режими у сфері часто спираються на етичні принципи, які допомагають визначити найкращі варіанти поведінки. Крім того, наявність складного поєднання правових, етичних і, можливо, більш суворих механізмів контролю в даній галузі означає, що поведінка, яка не регулюється правовими нормами, також має регулюватися етичними нормами.

Навіть за строгого дотримання законодавства про захист даних, громадяни змушені ухвалювати виважені рішення, пов'язані з етичними аспектами використання технологій обробки великих даних і методів їхнього застосування організаціями. У процесі впровадження існуючих політик захисту даних виникають проблеми, що робить деякі аспекти регулювання даних етично неоднозначними. У зв'язку з цим, основні дискусії в галузі етики великих даних стосуються наслідків використання даних, обмежень на їх використання, управління на основі принципів, якості даних, свободи дій і згоди. Ці питання спрямовані на те, щоб надати громадянам можливість контролювати систему захисту даних і забезпечити відповідність її інтересам [23].

У перспективі очікується, що тенденція до збільшення обсягів даних і зниження потреби в довірі буде посилюватися. Це зумовлено тим, що постачальниками великих даних дедалі частіше стають машини, а не люди. У результаті постійного розвитку методів збору та обробки даних цей процес може стати закономірним. Ці тенденції не залежать від того, хто є ініціатором – держава, компанія чи організація громадянського суспільства. Зі зростанням довіри до великих даних зростатиме і потреба в захисті особистої інформації. Ця вимога має бути сформульована як повага до конфіденційності в тій чи іншій формі [23].

У сучасних політичних концепціях, які вивчають майбутнє, немає чіткого і рівномірного домінування. Навіть якщо визнати, що етико-правові норми повинні встановлювати відносну перевагу у певних аспектах, вони не завжди узгоджуються між собою. Однак, незважаючи на відмінності у сприйнятті принципів, конкретні практичні умови залишаються незмінними. Ці умови повинні бути в центрі уваги при розгляді системної проблеми, яка може бути прийнятною для держав, компаній та громадян, стурбованих питаннями безпеки даних.

Висновки. Сьогодні людство перебуває на порозі нового етапу свого розвитку, пов'язаного з активним впровадженням цифрових технологій. Унаслідок технологічного прогресу людство вступило в нову еру, у якій держави, транснаціональні корпорації, національні економіки, підприємства й окремі індивіди тісно пов'язані між собою. У цей період держави, які прагнуть стати світовими технологічними лідерами, активно розвивають кіберпростір і розширюють його можливості. Республіка Ірландія є однією з таких держав, що відіграють ключову роль у розвитку технологій і розширенні кіберпростору, який потребує регулювання.

Правила кібербезпеки в Республіці Ірландія зазнали значних змін, щоб протистояти зростаю-

чим загрозам, пов'язаним з кібератаками та витоком даних. Нормативи кібербезпеки в Республіці Ірландія розроблені для вирішення різних аспектів захисту даних, включаючи управління інформаційною безпекою, повідомлення про порушення у сфері захисту даних та обов'язки організацій щодо безпеки персональних даних. До важливих нормативно-правових актів належать «Загальний регламент щодо захисту даних», «Закон про захист даних», «Директива про мережеві та інформаційні системи», «Правила електронної конфіденційності» та «Стратеія кібербезпеки Республіки Ірландія». Вони накладають зобов'язання на організації, які збирають, зберігають та обробляють персональні дані.

Всі вищезазначені законодавчі акти в сукупності встановлюють строгі вимоги до організацій щодо захисту даних та мережевої безпеки. Нормативно-правова база наголошує на необхідності впровадження організаціями комплексних заходів кібербезпеки та забезпечення захисту конфіденційної інформації. Постійна вимога дотримання нормативних вимог наголошує на важливості суворих заходів безпеки. Ці нормативні акти спрямовані не лише на захист прав особистості на недоторканність приватного життя, а й на забезпечення підзвітності організацій, гарантуючи, що вони приділяють першорядну увагу кібербезпеці у своїй операційній діяльності.

Нові повноваження, надані «Загальним регламентом щодо захисту даних», дають «Комісії із захисту даних» Республіки Ірландія можливість більш ефективно виконувати свої функції. Однак питання про те, чи буде цей потенціал реалізовано, залишається відкритим. Однак очевидно, що після ухвалення «Загального положення про захист даних ЄС» динаміка регулювання змінилася. Набрання чинності новими правилами, що регламентують діяльність наглядового органу, має велике значення. Органи захисту даних, які раніше висловлювали критику на адресу «Загального регламенту щодо захисту даних» ЄС, тепер отримали можливість заперечувати будь-які відхилення від цього документа. Можна припустити, що це стане підставою для більш глибокого аналізу методів роботи компаній, зареєстрованих в Республіці Ірландія, таких як «Meta», хоч і не обов'язково в контексті конкуренції. Нові положення «Загального регламенту щодо захисту даних» про співробітництво та спільні операції можуть сприяти більш ефективній взаємодії між національними органами, що здійснюють регулювання у цій сфері.

Однак, незважаючи на ці нові повноваження і ресурси регулятора, в Республіці Ірландія залишаються невирішеними ширші питання захисту даних. Національне законодавство і практика в багатьох сферах не встигають за розвитком інформаційного суспільства, особливо в тому, що стосується боротьби з кіберзлочинністю. Нездатність законодавчо закріпити доступ правоохоронних органів до даних, що зберігаються в Республіці Ірландія, викликає невдоволення інших країн-членів ЄС. Роль Республіки Ірландія як глобального центру обробки даних також зробила її об'єктом триваючих трансатлантичних дискусій про державне спостереження. Незважаючи на це, громадськість практично не брала участі в обговоренні цих питань. Цілком імовірно, що знадобиться ще не один резонансний випадок, подібний до скарги М. Шремса, щоб спонукати до вжиття заходів у цих галузях.

Республіка Ірландія має надійну систему захисту в галузі кібербезпеки. Однак технологічний прогрес не стоїть на місці, і разом з ним зростає рівень кіберзагроз. У зв'язку з цим Республіка Ірландія повинна продовжувати розробляти і реалізовувати стратегії, спрямовані на запобігання і мінімізацію ризиків у сфері кібербезпеки. З огляду на те, що Республіка Ірландія є одним із ключових регіонів, які обробляють глобальні дані, необхідно вживати активних заходів щодо захисту інформаційних систем від кібератак. Ірландська держава має надійну систему захисту у сфері кібербезпеки. Однак технологічний прогрес не стоїть на місці, і загрози в галузі кібербезпеки стають дедалі актуальнішими. У зв'язку з цим Республіка Ірландія повинна продовжувати стратегічно мислити і бути готовою до можливих атак. З огляду на те, що Республіка Ірландія є одним із ключових регіонів, які обробляють глобальні дані, необхідно вживати заходів щодо запобігання і стримування можливих загроз.

Республіка Ірландія продовжує роботу з удосконалення та адаптації своєї правової та нормативної бази, щоб забезпечити обізнаність і вжиття заходів на національному, індивідуальному та корпоративному рівнях. В умовах постійного розвитку кіберпростору необхідно вживати превентивних заходів для забезпечення захисту від кіберзагроз, а нормативно-правове регулювання повинно адаптуватися до ризиків, що виникають, тим самим спонукаючи державні структури, навчальні заклади, організації та підприємства постійно підвищувати рівень своєї безпеки. У міру розвитку нормативно-правового середовища в Республіці Ірландія воно відображає ширшу глобальну тенденцію до пріоритизації кібербезпеки, що призводить до створення більш безпечної цифрової екосистеми для всіх зацікавлених сторін.

Співпраця між урядом Республіки Ірландія, наглядовими органами та компаніями набуває все більшого значення. Зацікавлені сторони повинні спільно працювати над розробкою і впровадженням передових методів, обмінюватися інформацією про загрози і підвищувати стійкість організацій до кіберзагроз. Прогресивний під-

хід, заснований на постійному вдосконаленні, не тільки допоможе забезпечити дотримання нормативних вимог, а й сприятиме формуванню культури безпеки в ірландському бізнесі. Таким чином, майбутнє законодавства в галузі кібербезпеки в Республіці Ірландія залежить від його здатності адаптуватися до нових технологічних досягнень і кіберзагроз. Акцент на превентивних заходах і співпраці підвищить ефективність нормативно-правової бази та забезпечить безпечне цифрове середовище.

У перспективі необхідно забезпечити адаптацію і розвиток правил кібербезпеки в Республіці Ірландія з урахуванням нових технологій і загроз, що виникають. В умовах зростаючої залежності від цифрової інфраструктури організації повинні проявляти пильність і оперативно реагувати на динамічно мінливі ризики у сфері кібербезпеки. Розвиток «Інтернету речей», хмарних обчислень і штучного інтелекту призводить до появи нових проблем у сфері захисту даних, які потребують оновлення та вдосконалення нормативно-правової бази. Необхідно приділити особливу увагу розробленню та впровадженню методів активного захисту від кіберзагроз.

ЛІТЕРАТУРА:

1. Gartner Identifies Top Five Trends in Privacy Through 2024. *Gartner*. May 31, 2022. URL: https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024

2. Chheda J. Cybersecurity laws of Ireland : an analysis. *Pleaders*.

September 21, 2021. URL: https://blog.ipleaders.in/cybersecurity-laws-of-ireland-an-analysis/

3. McIntyre T. Regulating the Information Society: Data Protection and Ireland's Internet Industry / In Farrell and Hardiman (eds), *The Oxford Handbook of Irish Politics.* Oxford University Press, 2020. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590302

4. General data protection regulation. *Access to European Union law*. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_2&from=EN

5. Data Protection Act (DPA) Ireland 2018. *IT-governance*. 2018. URL: https://www.itgovernance.eu/en-ie/data-protection-ie

6. Baker A. NIS Directive – The EU's Directive on security of network and information systems. *IT-governence*. November 18, 2019. URL: https://www.itgovernance.eu/blog/en/nis-directive-the-eus-directive-on-security-of-network-and-information-systems

7. Criminal Justice (Offences Relating to Information Systems) Act 2017. *Electronic Irish Statute Book (eISB).* May 24, 2017. URL: https://www.gov.ie/en/publication/0735b-criminal-justice-offences-relating-to-information-systems-act-2017/?

8. McCann F. New Hacking and Cybercrime Offences. *Lexology*. May 24, 2017. URL: https://www.lexology.com/library/detail.aspx?g=cfff4793-1ff7-437e-81d2-41b10c9b1744

9. Bu-Pasha S. Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law. 2017. Vol. 26(3). P. 213–228. URL: https://doi.org/10.1080/13600834.2017.1330740

10. National Cyber Security Strategy 2019–2024. *The National Cyber Security Centre of Ireland (NCSC).* 2019. URL: https://www.ncsc.gov.ie/strategy/

11. Overview of Cybersecurity Regulations in Ireland. *Generis Global Legal Servicees.* November 19, 2024. URL: https://generisonline.com/overview-of-cybersecurity-regulations-in-ireland/

12. Notification of personal data breach to Commission in Data Protection Act 2018. *Irish Statute Book. 2018*. URL: https://www.irishstatutebook.ie/eli/2018/act/7/section/86/enacted/en/html

13. The Data Protection Commission of Ireland. 2025. URL: https://www.dataprotection.ie/en

14. Li S., Newman A. L. Over the shoulder enforcement in European regulatory networks:the role of arbitrage mitigation mechanisms in the General Data Protection Regulation. *Journal of European Public Policy*. 2022. Vol. 29(10). P. 1698–1720. URL: https://doi.org/10.1080/13501763.2022.2069845

15. GDPR penalties. *IT-governance of Europe.* 2025. URL: https://www.itgovernance.eu/sv-se/dpa-and-gdpr-penalties-se

16. LinkedIn fined €310 million by Ireland's data watchdog for privacy violations. *TIMESOFINDIA.* November 7, 2024. URL: https://timesofindia.indiatimes.com/technology/tech-news/linkedin-fined-310-million-by-irelands-data-watchdog-for-privacy-violations/articleshow/115061307.cms

17. Irish data protection authority fines Meta 390 million euros and appeals it's own decision. *Borncity*. May 1, 2023. URL: https://borncity.com/win/2023/01/05/irish-data-protection-authority-fines-meta-390-million-euros-and-appeals-its-own-decision/

18. Directive 95/46/EC of the European Parliament and of the Counci. *Access to European Union law.* October 24, 1995. URL: l https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng

19. Case note on C-362/14 Maximilian Schrems v Data Protection Commissioner. *Operating Eurovision and Eurobradio*. October 29, 2015. URL: https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20Schrems.pdf

20. Schrems M. Legal Procedure against "Facebook Ireland Limited". *Europe v. Facebook*. 2014. URL: http://europe-v-facebook.org/EN/Complaints/complaints.html.

21. McGeveran W. Friending the Privacy Regulators. *Arizona Law Review.* 2016. *Vol.* 58 (4). P. 959–1025. URL: https://journals.librarypublishing.arizona.edu/arizlrev/article/id/6942/

22. Bennett C., Raab Ch. The Governance of Privacy: Policy Instruments in Global Perspective. 2nd ed. London: Routledge, 2006.

23. Brodowicz M. Measures Ensuring Data Privacy and Security in the Digital Age. *Aithor*. June 9, 2024. URL: https://aithor.com/essay-examples/measures-ensuring-data-privacy-and-security-in-the-digital-age

REFERENCES:

1. Gartner Identifies Top Five Trends in Privacy Through 2024 (2022). *Gartner*. May 31. URL: https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024 [in English].

2. Chheda, J. (2021). Cybersecurity laws of Ireland : an analysis. *Pleaders*.

September 21. URL: https://blog.ipleaders.in/cybersecurity-laws-of-ireland-an-analysis/ [in English].

3. McIntyre, T. (2020). Regulating the Information Society: Data Protection and Ireland's Internet Industry / In Farrell and Hardiman (eds), *The Oxford Handbook of Irish Politics.* Oxford University Press. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590302 [in English].

4. General data protection regulation (2022). *Access to European Union law*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_2&from=EN [in English].

5. Data Protection Act (DPA) Ireland 2018 (2018). *IT-governance*. URL: https://www.itgovernance.eu/en-ie/data-protection-ie [in English].

6. Baker, A. NIS Directive – The EU's Directive on security of network and information systems. *IT-governence.* November 18, 2019. URL: https://www.itgovernance.eu/blog/en/nis-directive-the-eus-directive-on-security-of-network-and-information-systems [in English].

7. Criminal Justice (Offences Relating to Information Systems) Act 2017 (2017). *Electronic Irish Statute Book (eISB).* May 24. URL: https://www.gov.ie/en/publication/0735b-criminal-justice-offences-relating-to-information-systems-act-2017/? [in English].

8. McCann, F. New Hacking and Cybercrime Offences (2017). *Lexology*. May 24. URL: https://www.lexology.com/library/detail.aspx?g=cfff4793-1ff7-437e-81d2-41b10c9b1744 [in English].

9. Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law, 26(3), 213–228. URL: https://doi.org/10.1080/13600834.2017.1330740 [in English].

10. National Cyber Security Strategy 2019-2024 (2019). *The National Cyber Security Centre of Ireland (NCSC).* URL: https://www.ncsc.gov.ie/strategy/

11. Overview of Cybersecurity Regulations in Ireland (2024). *Generis Global Legal Servicees.* November 19. URL: https://generisonline.com/overview-of-cybersecurity-regulations-in-ireland/ [in English].

12. Notification of personal data breach to Commission in Data Protection Act 2018 (2018). *Irish Statute Book.* URL: https://www.irishstatutebook.ie/eli/2018/act/7/section/86/enacted/en/html [in English].

13. The Data Protection Commission of Ireland (2025). URL: https://www.dataprotection.ie/en [in English].

14. Li, S., & Newman, A. L. (2022). Over the shoulder enforcement in European regulatory networks:the role of arbitrage mitigation mechanisms in the General Data Protection Regulation. *Journal of European Public Policy*, 29(10), 1698–1720. https://doi.org/10.1080/1350176 3.2022.2069845 [in English].

15. GDPR penalties. *IT-governance of Europe* (2025). URL: https://www.itgovernance.eu/sv-se/dpa-and-gdpr-penalties-se [in English].

16. LinkedIn fined €310 million by Ireland's data watchdog for privacy violations (2019). *TIMESOFINDIA.* November 7, 2024. URL: https://timesofindia.indiatimes.com/technology/tech-news/linkedin-fined-310-million-by-irelands-data-watchdog-for-privacy-violations/articleshow/115061307.cms [in English].

17. Irish data protection authority fines Meta 390 million euros and appeals it's own decision (2023). *Borncity*. May 1. URL: https://borncity.com/win/2023/01/05/irish-data-protection-authority-fines-meta-390-million-euros-and-appeals-its-own-decision/ [in English].

18. Directive 95/46/EC of the European Parliament and of the Council (1995). *Access to European Union law.* October 24. URL: l https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng [in English].

19. Case note on C-362/14 Maximilian Schrems v Data Protection Commissioner (2015). *Operating Eurovision and Eurobradio*. October 29. URL: https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20Schrems.pdf [in English].

20. Schrems, M. (2014). Legal Procedure against "Facebook Ireland Limited". *Europe v. Facebook*. URL: http://europe-v-facebook.org/EN/Complaints/complaints.html [in English].

21. McGeveran, W. (2016). Friending the Privacy Regulators. *Arizona Law Review, Vol.* 58 (4), 959:1025. URL: https://journals.librarypublishing.arizona.edu/arizlrev/article/id/6942/ [in English].

22. Bennett, C., Raab, Ch. (2006). The Governance of Privacy: Policy Instruments in Global Perspective. 2nd ed. London: Routledge. [in English].

23. Brodowicz, M. (2024). Measures Ensuring Data Privacy and Security in the Digital Age. *Aithor*. June 9. URL: https://aithor.com/essay-examples/measures-ensuring-data-privacy-and-security-in-the-digital-age [in English].

Regulation of information and communication technologies in the context of information and personal data protection in the Republic of Ireland

Marusynets Marianna Mykhaylivna

Candidate of Philological Sciences,
Associate Professor,
Senior Research Fellow, Senior Researcher
Tivodor Legotsky Research Center
of the F. Rakotsi II Transcarpathian Hungarian College of Higher Education
Koshuta Square, 6, Berehove,
Transcarpathian region, Ukraine
ORCID: 0000-0001-7366-9328

The relevance of the study is due to the fact that today there is a tendency to reduce the effectiveness of traditional data protection methods. This makes it necessary to search for and implement new, contemporary approaches. With the active development and widespread use of automated data processing systems, the issues of personal data protection become particularly important. Over the past decades, the Republic of Ireland has made significant progress and taken a leading position in the world's technology sector. To achieve these results, strategic measures have been taken, including attracting foreign direct investment in technology projects, reducing corporate taxes, and using social and cultural aspects. A tripartite approach was implemented to strengthen the Republic of Ireland's position in the global technology space. However, to ensure the stability and sustainability of the results achieved, it is necessary to have reliable legislation and policies governing cyberspace.

The main purpose of the article is to analyse the information security system in the Republic of Ireland. The key tasks are to determine the specifics of regulation of the information and communication technologies (ICT) sector, and also to identify the problems and prospects of personal data protection in the Republic of Ireland as a member of the European Union in the context of rapid development of ICT and globalisation.

The theoretical and methodological basis of the study includes general scientific methods of analysis, synthesis, induction and deduction, as well as the systemic method, the method of structural and functional analysis and legal methods in cybersecurity. The historical approach was used to study the development of the cybersecurity system in the context of protection of personal data and confidential information in the Republic of Ireland. The systematic approach was applied to understand the essence of the information security of the Republic of Ireland, as well as to identify the prospects and challenges faced by the contemporary national security of the Irish state. The study of the extensive legal framework for regulating the system of personal data and information protection has led to the use of an interdisciplinary approach.

It is proved that the Republic of Ireland continues to work on improving and adapting its regulatory framework to ensure awareness and action at the national, individual and corporate levels. In the context of the constant evolution of cyberspace, preventive measures must be taken to ensure protection against cyber threats. Regulations should adapt to the emerging risks, thereby encouraging government agencies, educational institutions, corporations and businesses to continuously improve their security. As the regulatory environment in the Republic of Ireland evolves, it reflects a broader global trend towards prioritising cybersecurity, leading to a safer digital ecosystem for all stakeholders.

Key words: *Republic of Ireland, cybersecurity, information security, information and communications technology (ICT), EU, regulation, General Data Protection Regulation, Data Protection Act.*