11. Панченко, В. Ю. Моделі та методи оцінки інформаційної безпеки / В. Ю. Панченко, О. В. Коваленко. Одеса : Астропринт, 2018. 250 с.
12. ISO-27001. [Electronic resource]. https://www.dqsglobal.com/uk-ua/sertifikujte/sertifikaciya-iso-27001
13. Мельниченко, О. П. Оцінка ризиків інформаційної безпеки: методологія та інструменти / О. П. Мельниченко. Львів : Видавництво ЛНУ, 2017. 180 с.
14. IriusRisk. Threat Modeling Methodology: STRIDE. [Electronic resource]. https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.
15. Microsoft Security. STRIDE chart. [Electronic resource]. https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/.
16. Microsoft Build. The future is yours. [Electronic resource] 2025, May 19-22. https: // developer. microsoft. com/en-us/.
17. IriusRisk. Threat Modeling Methodology: OCTAVE. [Electronic resource]. https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies.
18. The NIST Cybersecurity Framework (CSF) 2.0. [Electronic resource] 2024, February 26. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
19. nist-cybersecurity-framework-20. [Electronic resource]. https: // my-itspecialist.com / nist-csf-2.0-six-cybersecurity-functions.
20. What is security information and event management (SIEM)? [Electronic resource]. https:// www.ibm.com /think/topics/siem.
21. Nessus vs. Qualys vs. OpenVAS. [Electronic resource] 2024, July 29. https://www.infosectrain.com/blog/nessus-vs-qualys-vs-openvas/.
22. 25 Best Vulnerability Scanning Software Reviewed in 2025. [Electronic resource]. https://thectoclub.com/tools/best-vulnerability-scanning-tools/.

Надійшла 10.09.2025

УДК 004.056.53
DOI: 10.31673/2409-7292.2025.041202

Ветлицька О. С.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРБЕЗПЕЦІ: ІНТЕГРАЦІЯ РИЗИК-МЕНЕДЖМЕНТУ ТА ПРАВОВИХ МОДЕЛЕЙ

У статті досліджено критичну необхідність інтеграції законодавчих вимог (зокрема, GDPR) та технічних механізмів кібербезпеки для ефективного захисту персональних даних (ПД). Центральною тезою є те, що відповідність (compliance) не є тотожною безпеці, і вимагає впровадження проактивного підходу «приватність за дизайном» (Privacy by Design). Проаналізовано застосування оцінки впливу на приватність (PIA/DPIA) як діагностичного інструменту для виявлення зон ризику в життєвому циклі ПД. Запропоновано модель комплексного ризик-орієнтованого захисту ПД (МКРОЗ), що поєднує техніки мінімізації даних (токенизація, анонімізація) з принципами правового контролю. Обґрунтовано, що практичні аспекти захисту включають не лише посилення шифрування, але й архітектурну сегрегацію даних та впровадження методології управління доступом на основі ролей (RBAC), що підкріплена постійним правовим аудитом. Дослідження акцентує увагу на методологічному розриві між абстрактними юридичними вимогами (як-от «право на забуття» чи «мінімізація даних») та їхнім конкретним технічним втіленням. Для подолання цього розриву пропонується формалізована модель «правового ризику», що дозволяє кількісно оцінити потенційні регуляторні та фінансові наслідки невідповідності (штрафи, позови) і інтегрувати цю метрику в традиційні матриці технічних кіберризиків. Цей підхід забезпечує керівництву IT-безпеки можливість приймати економічно обґрунтовані рішення, пріоритизуючи інвестиції у ті засоби захисту, які одночасно мінімізують як технічні вразливості, так і регуляторні загрози. Практична значущість статті полягає в детальному обґрунтуванні архітектурних рішень, необхідних для реалізації МКРОЗ, включаючи принципи сегрегації даних (розділення ідентифікаторів та чутливої інформації) та використання токенізації для зниження периметра впливу порушення. Запропоновані механізми управління доступом, зокрема вдосконалена RBAC, інтегровані з юридичними ролями (наприклад, DPO чи комплаєнс-офіцер), дозволяють забезпечити, що технічні дозволи прямо відображають правові обмеження доступу до ПД. Це створює надійну основу для захисту даних не лише від зовнішніх загроз, але й від внутрішніх порушень, обумовлених неналежним управлінням правами.

Ключові слова: персональні дані, GDPR, privacy by design, data loss prevention, ризик-менеджмент, токенізація, правові моделі, конфіденційність.

Вступ

У цифрову епоху персональні дані (ПД) перетворилися на критичний актив, а їхній захист став центральним викликом у сфері кібербезпеки. Інтенсивна цифровізація послуг, поширення Інтернету речей (IoT) та хмарних обчислень призвели до експоненційного зростання обсягів оброблюваних ПД [1].

Паралельно цьому, запровадження суворих правових актів, таких як загальний регламент про захист даних (GDPR) в ЄС, визначило не лише технічні, але й юридичні вимоги до обробників і контролерів даних [2, 3].

Традиційні підходи до кібербезпеки, засновані на периметровому захисті та реактивному усуненні інцидентів, виявляються недостатніми для забезпечення права на приватність як фундаментального права людини [4].

Таким чином, існує наукова та практична необхідність розробки інтегрованих моделей, які б гармонійно поєднували юридичний фреймворк (комплаєнс) із проактивними інженерними рішеннями (кібербезпека), щоб забезпечити захист ПД на кожному етапі їхнього життєвого циклу [4].

Ефективний захист персональних даних у сучасному цифровому середовищі вимагає відходу від традиційного, реактивного підходу, зосередженого лише на запобіганні кібератакам. Ключовим завданням є створення цілісної системи, де правові норми та вимоги ризик-менеджменту взаємно підсилюють один одного.

Формулювання проблеми

Проблема полягає у стратегічному розриві між динамічними, технічно орієнтованими практиками кібербезпеки (Risk Management) та статичними, реактивними вимогами законодавства щодо захисту персональних даних (Legal Compliance). Сучасні практики кібербезпеки зосереджені на швидкому реагуванні та запобіганні загрозам (наприклад, оцінка вразливостей, пентести), але часто розглядають правові норми (GDPR, CCPA, українське законодавство) лише як додаткове, а не інтеграційне навантаження.

Водночас, постійне зростання обсягів чутливих даних, які обробляються у хмарних середовищах та Big Data-системах, вимагає переходу від ізольованих підходів до єдиної моделі, що поєднує безперервне управління ризиками (Continuous Risk Management, CRM) із засадами «приватності за дизайном» (Privacy by Design, PbD). Існуючі моделі управління (ISO 27001, NIST CSF) надають рамки, але не пропонують деталізованого операційного фреймворку для трансляції юридичних зобов’язань (таких як право на забуття, мінімізація даних) у конкретні, технічно вимірні та керовані показники ризику та контролю.

Відсутність такого інтегрованого фреймворку призводить до кількох критичних наслідків:

1. Формальний комплаєнс: організації витрачають значні ресурси на відповідність «галочці» (checklist compliance), але не підвищують реальний рівень захисту даних від нових кіберзагроз;
2. Неефективне управління ризиками: ризики, пов'язані з правовими та репутаційними наслідками витоку даних, часто недооцінюються або розглядаються відокремлено від технічних ризиків;
3. Складність аудиту: неможливість легко продемонструвати відповідність юридичним вимогам через технічні засоби контролю ускладнює аудит та підвищує ймовірність штрафних санкцій.

Аналіз дотичних робіт

Питання інтеграції кібербезпеки та захисту персональних даних є міждисциплінарним полем, яке динамічно розвивається.

1. Нормативно-правові моделі (Compliance-driven Models): дослідження, що ґрунтуються на GDPR (статті 25, 32, 35) та інших регуляторних актах, підкреслюють ключові принципи: Privacy by Design (PbD), Privacy by Default (PbD) та оцінка впливу на захист даних

© Ветлицька О. С. (2025) Захист персональних даних у кібербезпеці: інтеграція ризик-менеджменту та правових моделей. Сучасний захист інформації, 4(64), 16–23.
https://doi.org/10.31673/2409-7292.2025.041202

(Data Protection Impact Assessment, DPIA). Ці роботи окреслюють що має бути захищено, але часто не дають як це зробити з точки зору архітектури кібербезпеки. Вони є відправною точкою, встановлюючи юридичні вимоги, які необхідно перетворити на технічні контролі.

2. Фреймворки управління ризиками (Risk Management Frameworks): стандарти NIST Cybersecurity Framework (CSF), ISO/IEC 27005 та OCTAVE пропонують структуровані підходи до ідентифікації, оцінки та пом'якшення кіберризиків. Однак ці моделі є переважно технічно-нейтральними і не містять специфічних механізмів для прямої інтеграції юридичних прав суб'єктів даних (наприклад, ефективного відстеження та видалення даних для реалізації «права на забуття») у процес оцінки ризиків.

3. Концепція GRC (Governance, Risk, and Compliance): сучасні роботи у сфері GRC намагаються об’єднати управління (Governance), ризики (Risk) та комплаєнс (Compliance) під єдиним дахом. Вони визнають необхідність злиття цих сфер, але більшість рішень є інструментальними (програмні платформи GRC) і не пропонують фундаментальної математичної або архітектурної моделі, яка б дозволяла кількісно оцінити вплив юридичних зобов’язань на загальний кіберризик.

4. Моделі децентралізованого захисту: дослідження в області самосуверенної ідентичності (SSI) та блокчейну пропонують радикальне вирішення проблеми шляхом передачі контролю користувачеві, що є втіленням PbD. Хоча ці моделі усувають ризики централізованого зберігання, вони створюють нові виклики, пов'язані з інтеграцією, масштабованістю та правовою відповідальністю у розподіленому середовищі.

Таким чином, наявні дослідження надають потужні правові (GDPR) та технічні (NIST, ISO) інструменти, але демонструють прогалину в операційному моделюванні. Необхідна інтегрована модель, яка слугуватиме «перекладачем» між юридичними вимогами захисту даних та інженерними практиками управління кіберризиками, що і є об'єктом цього дослідження.

Мета статті – розробка інтегрованого операційного фреймворка для захисту персональних даних, який забезпечує безперервну синергію між підходами кібербезпеки, що ґрунтуються на управлінні ризиками (Risk-Based Security), та юридичними зобов'язаннями щодо приватності (Legal Compliance Models), з метою мінімізації правових, репутаційних та фінансових втрат організації в епоху Big Data.

Для досягнення мети роботи потребують вирішення окремі завдання дослідження, зокрема:

1. Розробити універсальний операційний фреймворк Privacy-Integrated Cyber-security (PIC), що забезпечує циклічну взаємодію між DPIA (оцінкою впливу на захист даних), CRM (безперервним управлінням ризиками) та автоматизованим аудитом комплаєнсу;

2. Розробити набір конкретних, технічно вимірних контролів (Compliance Controls), які безпосередньо транслюють абстрактні юридичні вимоги (наприклад, «право на забуття», «мінімізація даних») у параметри, керовані засобами кібербезпеки (наприклад, криптографічні механізми, політики доступу, TTL для даних);

3. Апробувати розроблений PIC-фреймворк на прикладі типової хмарної архітектури обробки чутливих даних з метою підтвердження його ефективності у підвищенні рівня захисту персональних даних та спрощенні комплаєнсу.

Виклад основного матеріалу

Наукова новизна отриманих результатів полягає у розробці та теоретичному обґрунтуванні інтегрованого підходу, який систематично поєднує юридичні зобов'язання щодо захисту даних із динамічними інструментами управління кіберризиками. Вперше розроблено інтеграційний операційний фреймворк Privacy-Integrated Cyber-security (PIC-Framework), який концептуально об'єднує процеси оцінки впливу на захист даних (DPIA) та безперервного управління ризиками (CRM). Новизна полягає у створенні циклічної моделі, де висновки юридичного комплаєнсу автоматично ініціюють технічні коригувальні дії в системі

ризик-менеджменту. Набула подальшого розвитку теорія «приватності за дизайном» (Privacy by Design) шляхом її формалізації як обов'язкового, вимірюваного етапу в життєвому циклі розробки інформаційних систем, а не лише як декларативного принципу.

Розроблено та формалізовано модель кількісної оцінки юридичного ризику, яка вперше дозволяє транслювати нетехнічні показники (суворість регулятора, максимальний розмір штрафу, юрисдикційна відповідальність) у метрику, сумісну з технічною матрицею кіберризику.

Удосконалено методику ідентифікації та реалізації «комплаєнс-контролів» (Compliance Controls), що передбачає пряме перетворення абстрактних юридичних вимог (наприклад, «право на забуття») на конкретні, технічно вимірні параметри контролю (наприклад, криптографічні механізми, політики TTL, мандатний контроль доступу).

Запропоновано методологію безперервного аудиту комплаєнсу, засновану на постійному моніторингу статусу технічних контролів, які безпосередньо корелюють із юридичними вимогами, що усуває необхідність у періодичних, реактивних перевірках.

Створений PIC-фреймворк є готовою до впровадження моделлю для IT-архітекторів та CISO, що дозволяє органічно вбудовувати вимоги GDPR та інших регуляторів без додаткового дублювання інструментів чи процесів.

Забезпечується значне зниження часу та ресурсів, необхідних для демонстрації відповідності (Compliance Demonstration) під час зовнішніх аудитів, оскільки юридичний комплаєнс стає вимірним результатом технічних механізмів кібербезпеки.

Запропонована модель кількісної оцінки ризику дозволяє керівництву приймати економічно обґрунтовані рішення, пріоритизуючи інвестиції у ті технічні засоби захисту, які одночасно мінімізують як технічні, так і регуляторні ризики.

Принцип «приватність за дизайном» (PbD) центральною методологічною основою сучасного захисту ПД є концепція privacy by design (PbD), започаткована Анною Кавукян [5]. Вона вимагає, щоб приватність і захист даних були інтегровані в архітектуру IT-систем та бізнес-практики до початку обробки даних, а не додавалися пізніше як «заплатка». Сім фундаментальних принципів PbD в табл. 1.

Таблиця 1

Сім фундаментальних принципів PbD

№	Принцип (UA)	Практичний аспект у кібербезпеці
1.	Проактивний, а не реактивний захист	Обов'язкове проведення DPIA/PIA (Оцінки впливу на приватність) на етапі проектування
2.	Приватність як налаштування за замовчуванням	Всі налаштування системи мають бути максимально обмежувальними щодо збору та доступу до ПД
3.	Приватність інтегрована у дизайн	Використання гомоморфного шифрування (HE) або диференційної приватності для обробки
4.	Повна функціональність (Positive-Sum)	Забезпечення максимальної безпеки без шкоди для продуктивності та бізнес-логіки
5.	Наскрізний захист (End-to-End)	Шифрування ПД не лише під час передачі, а й у стані спокою (At Rest) та в обробці (In Use)
6.	Прозорість та відкритість	Документування та аудит усіх політик обробки та доступу, доступні для перевірки
7.	Повага до користувача	Забезпечення легкого доступу до власних даних, їхнього коригування та права на видалення (право бути забутим)

Техніки мінімізації та де-ідентифікації даних найбільш ефективний спосіб захисту ПД – це їхня мінімізація. Якщо дані не зберігаються або не ідентифікують особу, вони не можуть бути викрадені [6].

Ключові технології:

- токенізація: заміна чутливих ПД (наприклад, номерів кредитних карток, РНОКПП) на нечутливі, випадково згенеровані ідентифікатори (токени). Токени зберігаються в окремому, високозахищеному сховищі (Token Vault);
- анонімізація: процес безповоротного видалення ідентифікаторів, що дозволяють прямо чи опосередковано відновити особу. Вимагає високої уваги до ризиків ре-ідентифікації через комбінування анонімізованих наборів даних;
- псевдонімізація (GDPR Art. 4(5)): заміна ідентифікаторів на псевдоніми. Це оборотний процес, але для зв'язування псевдоніма з особою потрібен додатковий ключ, що значно ускладнює злом [7].

Модель комплексного ризик-орієнтованого захисту ПД (МКРОЗ) МКРОЗ пропонує інтегрований підхід, де кожен етап життєвого циклу ПД (збір, зберігання, обробка, видалення) має відповідний технічний та правовий контроль в табл. 2.

Таблиця 2

Життєвий цикл персональних даних та інтегровані контролі МКРОЗ

Етап життєвого циклу	Правовий контроль (Compliance)	Технічний контроль (Cybersecurity)
Збір	DPIA/PIA (оцінка впливу), згода суб'єкта	Мінімізація за замовчуванням (збір лише необхідних ПД)
Зберігання	Аудит доступу (Data Governance), право бути забутим	Шифрування At Rest (AES-256), архітектурна сегрегація (Token Vault)
Обробка	Правовий дозвіл, сегрегація обов'язків (SoD)	RBAC/ABAC (Контроль доступу), токенізація, гомоморфне шифрування
Передача	Транскордонні механізми (SCCs), прозорість	Шифрування In Transit (TLS/SSL), безпечні VPN-тунелі
Видалення	Політика ретенції, підтвердження видалення	Безпечне знищення даних (Wiping, Degaussing), Логування процесу

Реалізація МКРОЗ стикається з низкою викликів

По-перше, викликом продуктивності. Застосування передових методів, таких як гомоморфне шифрування, що дозволяє обробляти зашифровані дані без їхнього розшифрування, поки що є ресурсоємним і вимагає значних обчислювальних потужностей.

По-друге, викликом комплаєнсу в гібридних середовищах. Розподіл даних між локальними серверами та хмарними платформами ускладнює уніфіковане застосування політик доступу та шифрування, створюючи «сліпі зони» для DLP-систем.

По-третє, правовим викликом анонімізації. Європейське регулювання вимагає, щоб анонімізація була незворотною (тобто виключала можливість ре-ідентифікації).

Це створює постійний ризик для організацій, оскільки нові методи машинного навчання постійно підвищують ефективність ре-ідентифікації [8]. Модель МКРОЗ пропонує постійний перегляд технічних засобів захисту відповідно до еволюції загроз і правового поля.

Практичне значення моделі полягає у зміщенні уваги з формальної «галочки» комплаєнсу на інженерну стійкість системи, що гарантує захист ПД як першочерговий архітектурний пріоритет [9, 10].

Опис правових моделей інтеграції з ризик-менеджментом

Для ефективної інтеграції кібербезпеки та правового поля автор пропонує використовувати дві основні превентивні правові моделі, закріплені в міжнародному законодавстві (зокрема, GDPR), які перекладають юридичні вимоги на технічну архітектуру.

Модель «Приватність за дизайном» (Privacy by Design, PbD): ця модель є фундаментальною і вимагає вбудовування принципів захисту приватності та даних у технології, системи та бізнес-процеси на найперших етапах їх розробки та до їх фактичного запуску. Це означає, що замість накладання правових вимог на існуючу систему, архітектура системи одразу проєктується так, щоб забезпечувати максимальний захист ПД. На практиці це реалізується через оцінку впливу на приватність даних (Data Protection Impact Assessment, DPIA), яка є діагностичним та планувальним інструментом.

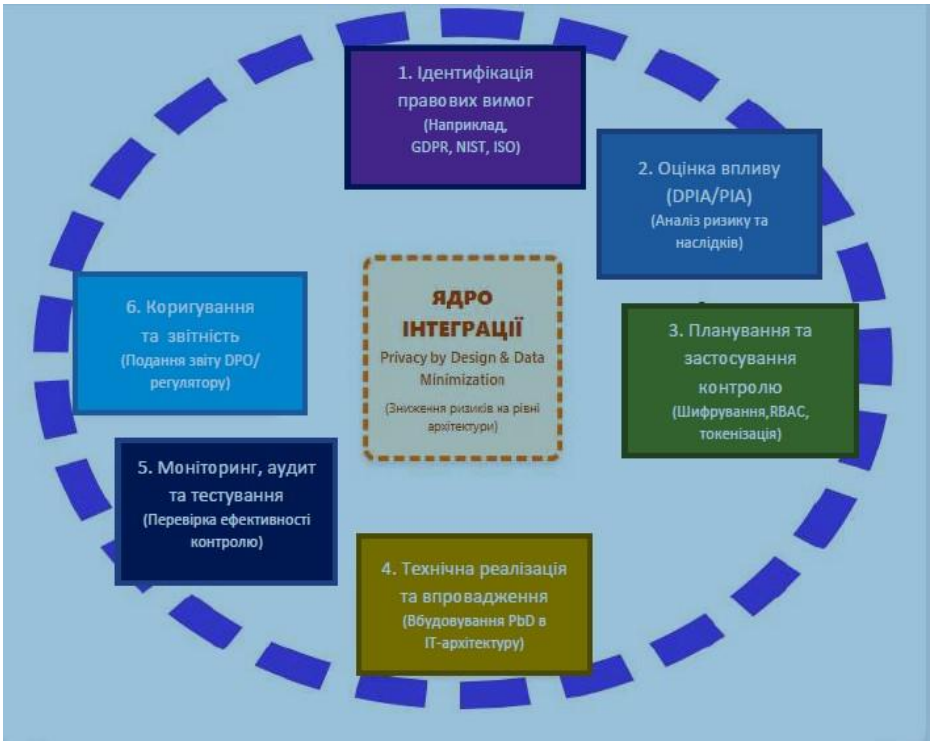

Рис. 1. Модель циклічної інтеграції правових моделей та ризик-менеджменту у сфері захисту ПД

Модель «Мінімізація даних» (Data Minimization): ця модель є практичним втіленням PbD і вимагає, щоб збір, обробка та зберігання персональних даних були обмежені лише тим обсягом, який є абсолютно необхідним для досягнення конкретної, законної мети. Технічно це реалізується через:

– псевдонімізацію/анонімізацію: заміна або видалення ідентифікаторів, що дозволяють прямо або опосередковано встановити особу;

– токенізацію: заміна чутливих даних нечутливими «токенами», які не несуть інформаційної цінності, але можуть бути використані для внутрішніх процесів;

– сегрегацію даних: фізичне чи логічне розділення чутливих ПД від загальних робочих даних, що ускладнює повний компроміс системи у разі інциденту.

Інтеграція правових моделей та ризик-менеджменту являє собою циклічний процес, де юридичні вимоги слугують відправною точкою для ідентифікації ризиків, а ризик-менеджмент забезпечує механізми їх технічного зниження.

Схема (рис. 1) ілюструє, що інтеграція починається з ідентифікації правових вимог (наприклад, GDPR, CCPA). Ці вимоги трансформуються в оцінку впливу на приватність (DPIA), яка є не просто юридичним, а ризик-орієнтованим процесом, що визначає ймовірність і наслідки порушення прав суб'єктів даних. На основі результатів DPIA застосовуються заходи контролю (технічні: шифрування, RBAC; організаційні: навчання, політики). Далі відбувається моніторинг і аудит, який перевіряє ефективність застосованих заходів і повертає інформацію для коригування правової відповідності, забезпечуючи безперервність циклу.

Проілюструвавши суть поєднання ризик-менеджменту та правових моделей, зазначимо позитивні сторони та недоліки такої інтеграції в табл. 3.

Таблиця 3

Поєднання ризик-менеджменту та правових моделей,
позитивні сторони та недоліки такої інтеграції

Аспект	Позитивні сторони	Недоліки
Проактивність	Гарантує, що ризики ПД усуваються на етапі проєктування (PbD), запобігаючи дорогим змінам після запуску та юридичним штрафам.	Вимагає значних початкових інвестицій у проєктування архітектури та потребує залучення висококваліфікованих спеціалістів (Data Privacy Officer, кіберюрист).
Ефективність	Створює єдину мову для юристів і технічних фахівців, де юридичні вимоги (наприклад, «мінімізація») мають чіткі технічні еквіваленти (токенизація).	Ризик-менеджмент може бути занадто гнучким, тоді як правові моделі є жорсткими. Це може призвести до «надмірної безпеки» (over-security) і зайвої бюрократизації процесів.
Відповідність	Забезпечує безперервну відповідність (Continuous Compliance), оскільки будь-яка зміна системи проходить через повторний цикл DPIA та оцінки ризиків.	Складність інтеграції з існуючими (legacy) системами, де правові моделі не були закладені спочатку.
Культура	Формує культуру, орієнтовану на приватність, підвищуючи довіру клієнтів і репутацію організації.	Вимагає постійного навчання персоналу, оскільки людський фактор залишається основним джерелом витоку даних.

Приклади успішної інтеграції ризик-менеджменту та правових моделей у світовій практиці кібербезпеки

Обґрунтування авторського підходу підтверджується світовими тенденціями у сфері Enterprise Risk Management (ERM) та регуляторними вимогами:

1. Рамка NIST (National Institute of Standards and Technology) США: рамка кібербезпеки NIST (особливо SP 800-37, RMF) є класичним прикладом інтеграції, де правові та регуляторні вимоги (наприклад, вимоги HIPAA для охорони здоров'я або FISMA для державних установ) є першим кроком у процесі управління ризиками. Це забезпечує, що технічні заходи контролю, які впроваджуються для зниження ризиків, одночасно є й юридично обов'язковими;

2. Банківський та фінансовий сектор: регулятори, як-от Basel Committee on Banking Supervision (BCBS) та європейський орган банківського нагляду (EBA), вимагають від

фінансових установ вбудовувати кіберризик у загальний фінансовий операційний ризик-менеджмент. Це означає, що потенційні штрафи за порушення GDPR або вимог PCI DSS (платіжні картки) розглядаються як фінансові ризики, що стимулює інтеграцію юридичного комплаєнсу та технічного захисту на рівні вищого керівництва;

3. Впровадження GDPR у ЄС: європейський загальний регламент про захист даних (GDPR) не лише наклав штрафи, але й зробив обов'язковим інструмент DPIA для високоризикових операцій. Це зобов'язало компанії, незалежно від їхньої технічної зрілості, переходити від «запобігання зламу» до «забезпечення прав суб'єктів даних», використовуючи ризик-менеджмент як методологічну основу.

Висновки

Інтеграція ризик-менеджменту та правових моделей у сфері захисту персональних даних є не просто рекомендованою практикою, а критичною необхідністю, що відображає сучасний рівень кіберзагроз та регуляторних вимог. Запропонована циклічна модель, заснована на принципах Privacy by Design та Data Minimization, дозволяє організаціям трансформувати абстрактні юридичні вимоги у конкретні, вимірювані технічні заходи контролю. Це усуває традиційний розрив між юристами та інженерами, створюючи єдину, прозору стратегію захисту. Ключовим досягненням такої інтеграції є перехід від реактивного комплаєнсу до проактивного управління ризиками. Застосування DPIA як мосту між правовим полем і технічною архітектурою дозволяє ідентифікувати, оцінити та мінімізувати юридичні та операційні ризики на ранніх етапах життєвого циклу даних. Світова практика, зокрема досвід застосування рамки NIST та вимог GDPR у фінансовому секторі, підтверджує, що саме такий комплексний підхід забезпечує найбільш стійку кібербезпеку.

Водночас, успішна реалізація вимагає подолання низки викликів, таких як значні початкові інвестиції, необхідність постійного навчання персоналу та інтеграція в застарілі IT-системи. Жорсткість правових моделей не повинна паралізувати гнучкість ризик-менеджменту; натомість, вони мають співіснувати, де право визначає цілі, а ризик-менеджмент – шляхи їх досягнення. Подальші дослідження мають бути зосереджені на розробці стандартизованих метрик для кількісної оцінки правового ризику (Legal Risk Quantification) у контексті кібербезпеки. Це дозволить організаціям не лише відповідати вимогам законодавства, але й економічно обґрунтовувати інвестиції у захист даних, підвищуючи таким чином загальну цифрову стійкість економіки.

Перелік посилань

1. Cavoukian, A. (2015). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.

2. The European Parliament and the Council of the European Union. (2016). General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

3. ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection Information security management systems Requirements. International Organization for Standardization.

4. Nissenbaum, H. (2016). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

5. National Institute of Standards and Technology (NIST). (2017). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). NIST SP 800-122.

6. Agrawal, R., & Srikant, R. (2000). Privacy-preserving data mining. ACM SIGMOD Record, 29(2), 1-12. (Про концепції анонімізації).

7. Gentry, C. (2019). Fully homomorphic encryption using ideal lattices. STOC '09: Proceedings of the forty-first annual ACM symposium on Theory of computing, 169–178. (Основи гомоморфного шифрування).

8. U.S. National Archives and Records Administration (NARA). (2020). Records Management: De-identification and Anonymization.

9. Vetlytska O. S. (2023). Захист конфіденційності у професійній діяльності: модель поведінкового контролю. Наукові записки: Серія «Технічні науки», 1(3), 20-25.

10. Ristenpart, T., & Kroll, J. A. (2020). Beyond the Boundary: A Framework for Secure and Ethical User Behavior Analysis. IEEE Security & Privacy, 18(1), 18-25.

Надійшла 12.09.2025