УДК 004.056.53:004.4
DOI: 10.31673/2409-7292.2025.031228

**Лозова І.Л., Різак М.В.,
Хохлачова Ю.Є., Котик О.В.**

АНАЛІЗ МОДЕЛЕЙ, МЕТОДІВ ТА СИСТЕМ ОЦІНЮВАННЯ ВТРАТ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

Стрімке поширення цифрових технологій, глобалізація інформаційних потоків та зростання кількості кіберзагроз призвели до значного підвищення ризику витоків персональних даних, що спричиняє як фінансові втрати, так і репутаційні та правові наслідки для організацій. Існуючі підходи до оцінювання критичності інцидентів витоку персональних даних мають фрагментарний характер: одні зосереджені на фінансових втратах, інші – на технічних чи соціально-психологічних аспектах, що ускладнює формування комплексної оцінки. З метою усунення виявлених прогалин у статті здійснено порівняльний аналіз сучасних моделей, методів та систем оцінювання негативних наслідків від витоку персональних даних, визначено їх сильні та слабкі сторони. Особливу увагу приділено відповідності розглянутих підходів положенням міжнародних стандартів, зокрема GDPR, а також можливостям їх практичного застосування в інформаційних системах. Наукова новизна отриманих результатів полягає у формуванні теоретичного підґрунтя для розробки вдосконалених моделей та методів комплексного оцінювання втрат від витоку персональних даних з урахуванням економічних, правових і репутаційних факторів.

Ключові слова: персональні дані, оцінювання втрат, критичність інцидентів, конфіденційність, GDPR, кібербезпека.

Вступ та постановка проблеми в загальному вигляді

Стрімкий розвиток цифрових технологій, глобалізація інформаційних потоків та масове використання персональних даних у бізнес-процесах і державному управлінні зумовлюють зростання кількості кіберзагроз і випадків порушення конфіденційності інформації. Витоки персональних даних стали однією з найбільш критичних проблем сучасної кібербезпеки, оскільки вони призводять не лише до фінансових втрат підприємств, але й до репутаційних ризиків, порушення прав суб'єктів даних, а також юридичної відповідальності організацій.

Згідно з вимогами міжнародних нормативних актів, зокрема Регламенту ЄС із захисту даних (GDPR), організації повинні своєчасно виявляти, аналізувати та оцінювати наслідки інцидентів, пов'язаних із витоками даних. Однак практика свідчить, що існуючі підходи до оцінювання втрат є фрагментарними: окремі моделі орієнтовані лише на фінансову складову, інші враховують технічні аспекти уразливостей або соціально-психологічні наслідки для користувачів, проте відсутня уніфікована методологія, яка б дозволяла всебічно оцінювати критичність інциденту.

Таким чином, постає науково-практична проблема розробки комплексних моделей і методів оцінювання негативних наслідків від витоку персональних даних, які б поєднували вимоги нормативно-правового регулювання, можливості сучасних систем моніторингу та аналізу кіберзагроз, а також інструменти прогнозування впливу на бізнес-процеси й суспільство.

Мета статті – здійснити комплексний аналіз існуючих методів, моделей та систем оцінювання оцінювання втрат від витоку персональних даних, провести їх порівняння за уніфікованими параметрами та визначити їх сильні й слабкі сторони з метою виявлення прогалин і формування наукового підґрунтя для подальшої розробки вдосконалених моделей та методів оцінювання втрат у сфері захисту персональних даних.

Основні матеріали дослідження

В умовах посилення регуляторних вимог, зокрема відповідно до положень Загального регламенту про захист даних (GDPR), питання комплексного оцінювання наслідків витоку персональних даних стає одним із ключових завдань у сфері кібербезпеки.

Незважаючи на значну кількість наукових досліджень та практичних рішень, на сьогодні не існує універсальної моделі, яка б дозволяла адекватно оцінити всі аспекти втрат, спричинених інцидентами порушення конфіденційності персональних даних. Кожен із наявних підходів має свої обмеження: економічно орієнтовані методи здебільшого не

враховують репутаційних ризиків, правові – не відображають фінансової складової, а технічні – часто обмежуються оцінкою уразливостей без урахування соціально-психологічних наслідків. Це зумовлює потребу у проведенні системного аналізу відомих моделей, методів та інструментів із метою виявлення їх переваг і недоліків. У роботі подано узагальнений аналіз понад п'ятнадцяти ключових моделей, методів і систем, які застосовуються для оцінки негативних наслідків витоку персональних даних. Кожен підхід розглядається в контексті його практичного застосування, визначаються основні параметри, що враховуються під час оцінювання, а також наводяться критерії вимірювання збитків. Окрему увагу приділено можливостям інтеграції цих методів у сучасні інформаційні системи та перспективам їх використання в умовах зростаючої складності кіберзагроз.

1. FAIR (Factor Analysis of Information Risk) [1-3]. Модель FAIR – кількісний підхід до аналізу інформаційних ризиків, який розбиває ризик на частоту події втрати (Loss Event Frequency) і величину втрат (Loss Magnitude). FAIR дозволяє оцінити фінансові наслідки ризику, використовуючи статистичні моделювання (наприклад, метод Монте-Карло) для отримання розподілу ймовірних збитків. Зокрема, FAIR враховує як прямі (наприклад, витрати на відновлення і штрафи), так і опосередковані втрати (наприклад, репутаційні збитки). Модель широко використовується в корпоративному секторі, є стандартизованою (через OCEG) і реалізована в таких інструментах, як RiskLens та AuditScripts. FAIR може враховувати імовірні штрафи за недотримання GDPR (до 4 % річного обороту або €20 млн), оскільки штрафні санкції розглядаються як частина компонента «Judgments and Fines» у категорії втрат.

2. NIST SP 800-30 (Risk Assessment) та NIST RMF [4-7]. NIST SP 800-30 – це керівництво для проведення оцінки ризиків у рамках Risk Management Framework (RMF) NIST. Цей метод описує процес ідентифікації активів, вразливостей і загроз, а також визначення рівня ризику за якісними чи кількісними критеріями. За замовчуванням NIST 800-30 використовує якісну шкалу (низький/середній/високий) для оцінки впливу, але також дозволяє застосовувати фінансові метрики, наприклад річне очікуване збитки (ALE). NIST RMF орієнтований на організаційний рівень та відповідає стандартам FISMA, ISO/IEC 27001 та іншим. Він не робить акцент безпосередньо на GDPR, але може бути використаний для проєктування відповідних контролів. Основні дані для оцінки – внутрішня інформація про активи, інциденти та експертні судження щодо ймовірності й наслідків. За стандартом NIST впливи (конфіденційність, цілісність, доступність) оцінюються окремо, репутаційні втрати прямо не враховуються (хоча організація може інтерпретувати їх через бізнес-контекст). NIST RMF широко поширений у публічному та приватному секторах у США.

3. NIST Privacy Framework (PF) та PRAM [8]. NIST Privacy Framework – добровільний інструмент для управління ризиками приватності, розроблений NIST спільно з зацікавленими сторонами. Він структурує процеси та практики побудови системи управління приватністю, узгоджених з вимогами GDPR. У рамках Фреймворку NIST також розроблена методологія PRAM (Privacy Risk Assessment Methodology), яка допомагає системним власникам крок за кроком оцінити потік персональних даних, визначити області приватності, пріоритезувати ризики і обрати заходи реагування. Згідно з MITRE, PRAM «проводить системного власника через опис середовища, оцінку потоків даних, ідентифікацію проблем приватності, їх пріоритизацію та пошук заходів для усунення». Цей підхід більше орієнтований на управління процесами та ризик-менеджмент, ніж на безпосередню кількісну оцінку збитків. NIST Privacy Framework та PRAM популярні серед організацій, що прагнуть відповідати вимогам GDPR і побудувати програму приватності.

4. ISO/IEC 27005 [6, 7, 9]. Міжнародний стандарт ISO 27005 описує процес управління інформаційною безпекою: ідентифікацію загроз, оцінку ризиків, вибір та моніторинг заходів безпеки. Стандарт дає структуровані рекомендації щодо оцінки ризиків для ISMS згідно з ISO 27001. Він передбачає виявлення активів, оцінку вразливостей і наслідків (часто в категоріях «низький/середній/високий») та допомагає планувати заходи захисту. Як і NIST, ISO 27005 не

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107. https://doi.org/10.31673/2409-7292.2025.031228

задає конкретних формул для обчислення фінансових збитків, але сприяє тому, щоб всі рішення базувалися на оцінці ризиків. Джерелом даних зазвичай є внутрішні реєстри інцидентів, результати тестів безпеки та оцінки експертів. ISO 27005 фокусується на технічних і організаційних аспектах безпеки, тож репутаційні та фінансові наслідки відображаються опосередковано, через бізнес-контекст організації. Стандарт широко використовують у всьому світі для побудови ISMS, його популярність велика (ISO 27000-серія загально-визнана).

5. ISO 31000 [10]. Міжнародний стандарт ISO 31000 – це загальні рекомендації з управління ризиками для будь-яких організацій і сфер діяльності. Він закладає фреймворк (керування, структура, PDCA-цикли) та загальні процеси (ідентифікація, аналіз, оцінка, обробка ризиків). ISO 31000 не містить специфічних методів вимірювання збитків чи метрик; він охоплює весь спектр ризиків (від фінансових до екологічних) у вигляді управлінської практики. Як і ISO 27005, цей стандарт більше про процес, ніж про підрахунок конкретних збитків. Користується широкою підтримкою в бізнесі та урядах, хоча не є сертифікованим (моральний стандарт).

6. OWASP Risk Rating Methodology [11]. Методологія OWASP Risk Rating – це адаптація класичної моделі оцінки ризику для веб-додатків. За її визначенням, оцінка ризику проводиться за шкалою «ймовірність × вплив», де ймовірність визначається факторами загрози та вразливості, а вплив – технічними й бізнес-факторами. Зокрема, оцінка впливу включає кількісні показники «Financial Damage» і «Reputation Damage» поряд з іншими факторами. Це означає, що OWASP враховує як прямі фінансові втрати (за відмову сервісу, витік даних тощо), так і репутаційну шкоду (втрата доходу через падіння довіри). Перевага – простота та «аплікаційний» характер (орієнтація на конкретні вразливості веб-систем), але методологія залишається частково суб'єктивною, бо оцінка залежить від експертних балів (1–10). OWASP Risk Rating часто реалізується в GRC-інструментах (наприклад, SimpleRisk) і популярний у розробників і тестувальників безпеки. З точки зору GDPR, OWASP сама по собі не покликана перевіряти відповідність, але може оцінювати ризики витоку даних у веб-контексті.

7. Data Protection Impact Assessment (DPIA) за GDPR [12]. DPIA – це обов'язкова за GDPR (стаття 35) процедура оцінки впливу планованої обробки персональних даних на права та свободи осіб. Хоча DPIA не є числовою «моделлю збитків», це офіційна методика, що змушує організації розглядати ризики витоку даних із погляду порушення приватності. У межах DPIA аналізують потенційні негативні наслідки (включно з фінансовими санкціями, зокрема штрафами GDPR) та планують заходи пом'якшення. Процедура включає збір даних про обробку, консультації з DPO і, за необхідності, узгодження з наглядовими органами. Вона сфокусована на захисті прав суб'єктів, а не на відшкодуванні збитків, але є важливою складовою GDPR-комплаєнсу.

8. CRAMM (CCTA Risk Analysis and Management Method) [6, 7, 13]. CRAMM – це якісний інструмент для аналізу й управління ризиками, розроблений у 1985 році урядовою агенцією Великобританії (CCTA). CRAMM пропонує збирання інформації про активи та потенційні загрози, класифікацію вразливостей і оцінку рівня ризику в кількісній шкалі (часто 0–100) на основі викликів та цінності активів. Згодом він був комерціалізований (програмне забезпечення «CRAMM Manager») і використовувався в 20 країнах. Хоча CRAMM не дає прямих формул для розрахунку фінансових збитків, він визначає пріоритети ризиків і рекомендовані заходи. Втрата репутації може бути опосередковано врахована як «бізнес-наслідок» високого ризику. Для CRAMM існують реалізації на базі ПО (Insight CRAMM); він був популярний в урядових структурах, менше – у приватному секторі.

9. OCTAVE [13, 14]. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – фреймворк для оцінки кіберризиків, розроблений SEI Карнегі-Меллонського університету. OCTAVE поєднує аналіз технічних вразливостей з пріоритетами бізнесу: спочатку ідентифікуються критичні активи (персональні дані, IT-інфраструктура тощо), потім

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107.
https://doi.org/10.31673/2409-7292.2025.031228

можливі загрози і вразливості, і формується план зменшення ризиків. Він складається з трьох фаз (Profile, Threat, Risk) з акцентом на контекст організації. OCTAVE описаний як «комплексна модель для керування ризиками», що поєднує технічні оцінки з пріоритетами організації. Оскільки це методологія, а не математична модель, вона не видає кількісні оцінки збитків; втрати описуються категоріями (фінансові, операційні, репутаційні). OCTAVE особливо популярний у критично важливих інфраструктурах і великих компаніях, які хочуть збалансувати інформаційні загрози з бізнес-цілями.

10. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) [13, 15]. EBIOS – метод аналізу ризиків IT-систем, створений у Франції (1995) SCSSI/ANSSI. Остання версія (EBIOS Risk Manager, з 2018) націлена на державні організації та критичні сервіси. EBIOS поєднує сценарний аналіз і матричну оцінку: спершу визначаються найстрашніші події та активи (MAST), потім оцінюють їх впливи і ймовірності. ANSSI описує EBIOS як метод, що «аналізує ризики, що загрожують інформаційним системам» і регулярно оновлюється для відображення сучасних загроз. EBIOS використовує як експертні оцінки, так і об'єктивні показники безпеки для кожного сценарію. У ньому є інструментарій (бібліотеки сценаріїв) та допоміжні таблиці. Хоча пряме число збитків не обчислюється, метод дає можливість оцінювати пріоритетність ризиків з точки зору ігор з імовірностями. Зазвичай втрата репутації розглядається в контексті «secondaire» наслідків. EBIOS підтримує сумісність з ISO 27005 і широко використовувався у Франції.

11. MEHARI [13, 16]. MEHARI – французька методологія (CLUSIF) для гармонізованого аналізу ризиків. MEHARI пропонує трифазний процес: підготовка, аналіз та прийняття ризиків. Він спирається на «knowledge base» (базу запитань і шаблонів), що охоплює типові загрози й активи. У MEHARI є пряма відповідність з ISO 27001/27005: процес повністю сумісний із їх циклами вдосконалення. Для вимірювання негативних наслідків MEHARI використовує бали й таблиці впливу (від низького до високого) для кожного ризикового сценарію, враховуючи технічні та бізнес-погляди. Втрати оцінюються через ймовірність реалізації сценарію і рівень його негативного впливу на діяльність (в тому числі можуть включати фінансові та репутаційні аспекти через бізнес-моделі). Існують програмні продукти на базі MEHARI (від CLUSIF та партнерів). Серед користувачів – організації, що дотримуються ISMS за ISO 27001.

12. Ponemon Institute – Емпірична модель вартості витоку даних [17]. Ponemon Institute (за підтримки IBM) щороку публікує дослідження «Cost of a Data Breach». Це не абстрактна методика, а емпірична рамка: на основі опитувань компаній, що зазнали витоків, розраховується середня собівартість. Ponemon використовує activity-based costing, включаючи сотні категорій прямих і непрямих затрат. Результати відображаються у доларах за інцидент або в розрахунку на одного вкраденого запису. Згідно з Ponemon, більшу частину сукупних витрат складають опосередковані затрати (втрата продажів, репутація, штрафи). Методологія Ponemon базується на реальних даних (для дослідження використано ~ 1600 компаній). Цей підхід підходить для аналізу історичних даних і розрахунку ROI заходів безпеки, але менш придатний для точного прогнозування індивідуальних кейсів. Він пов'язаний з GDPR через оцінку середніх штрафів та реакції на інциденти, хоча фокус – на глобальних статистиках. Інструментальну реалізацію у вигляді ПЗ немає – це деталізований звіт.

13. Cyber Value at Risk (CyberVaR, CVaR) [13, 18]. Cyber Value at Risk (CVaR) – фінансова методика, адаптована до кіберризиків, що оцінює потенційні максимальні втрати за певним імовірнісним рівнем (хвостовий ризик). Для обчислень CVaR застосовують сценарне моделювання (наприклад, Монте-Карло) з різними параметрами атаки (частота, наслідки, вартість активів). Метод надає статистично обґрунтовані верхні межі втрат (напр. 95%-й персентиль збитків). Це корисно для стратегічного планування та оцінки страхових премій (використовується страховиками). CVaR фокусується на найгірших сценаріях, забезпечуючи глибокі фінансові оцінки для управління ризиком. Реалізація зазвичай потребує

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107. https://doi.org/10.31673/2409-7292.2025.031228

спеціалізованого ПЗ (стохастичне моделювання). Для GDPR CVaR допомагає показати регуляторам готовність до найсерйозніших подій, але сам по собі не включає специфічних правових вимірів. Він є кількісним і вимагає даних про попередні інциденти, експертних оцінок ймовірностей і вартостей активів.

14. Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches [19]. Запропоновано кількісну модель оцінки вартості витоку даних та ймовірності такого інциденту. Модель побудована за принципом «multiplicative model» – кожен фактор множиться на відповідний коефіцієнт. Враховуються прямі фінансові витрати (розслідування, компенсації, штрафи) та непрямі витрати (втрата репутації, судові позови, упущений прибуток тощо). Регуляторні штрафи згадані як один із компонентів витрат; загалом акцент на мінімізації витрат загалом, а не конкретно на GDPR. У статті наведено формальні рівняння (для вартості на один запис, загальної вартості тощо) з опорою на дані IBM/Ponemon, програмної реалізації немає.

15. Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави [20]. Модель передбачає використання численних параметрів для визначення шкоди. Це включає множини ідентифікаторів, типових загроз, відомостей, ступенів секретності, показників економічної шкоди та інших наслідків. Модель дозволяє оцінити наслідки витоку державної таємниці на рівні окремих областей та для держави в цілому. Вона розрахована на аналіз різних аспектів, таких як загроза з боку іноземних спецслужб, порушення режиму доступу, втрати матеріальних носіїв та інші.

Загалом, модель передбачає інтеграцію числових значень для кожного компоненту, що дає змогу оцінити шкоду в різних формах: економічній, безпековій, а також у вигляді тяжких наслідків для національної безпеки. Розроблена модель є важливою для підвищення ефективності кіберзахисту та для визначення масштабів загрози в разі витоку державної таємниці через кібератаки.

16. Модель оцінювання параметрів безпеки персональних даних у степеневих соціальних мережах на основі їх топології [21]. Запропонована модель степеневої соціальної мережі дозволяє детальніше досліджувати динаміку взаємодії між окремими агентами в мережі, зокрема процеси поширення соціально значущої інформації. На відміну від класичних підходів, вона враховує зміни в топології, пов’язані з розширенням мережі та приєднанням нових вузлів, що призводить до зростання навантаження на інфраструктуру і, відповідно, посилює ризики порушення конфіденційності персональних даних користувачів.

Сформульовано підхід до оцінювання параметрів захисту персональних даних у соціальних мережах зі степеневим розподілом зв’язків між вузлами. Методика базується на топологічному аналізі таких мереж, зокрема тих, що моделюються за принципом Барабаші–Альберта із застосуванням механізму переважного приєднання. У цій моделі ймовірність формування нових зв’язків залежить від поточної кількості зв’язків вузла – чим вона більша, тим вищий шанс утворення нових контактів.

До ключових параметрів безпеки, які враховуються у дослідженні, відносяться: ступінь вузла, середня довжина шляху, ймовірність приєднання нових вузлів, коефіцієнт кластеризації та кореляція між степенями суміжних вузлів. Встановлено, що збільшення степеня вузлів та середньої довжини шляху у мережі сприяє підвищенню ризику витоку інформації, зокрема через вищу ймовірність її перехоплення.

Підвищення коефіцієнта кластеризації супроводжується інтенсифікацією інформаційних потоків, що збільшує навантаження на захисні механізми й ускладнює забезпечення конфіденційності. Кореляція між вузлами з різними степенями може мати як позитивний, так і негативний вплив на захист даних, залежно від конфігурації мережевих зв’язків. Проведено серію імітаційних експериментів для мереж різного масштабу, що дозволило підтвердити ефективність запропонованого підходу до оцінювання параметрів безпеки персональних даних у складних соціальних структурах.

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107. https://doi.org/10.31673/2409-7292.2025.031228

17. Модель підвищення захищеності персональних даних користувачів системи дистанційного навчання збройних сил України. В [22] розглянуто підходи до підвищення рівня безпеки персональних даних користувачів у системі дистанційного навчання, що функціонує у Збройних Силах України. Дослідження акцентує увагу на використанні сучасних інтелектуальних технологій, таких як гібридні нейронні мережі та інструменти нечіткої логіки, з метою підвищення ефективності захисту інформації.

Запропоновано методичну основу, що складається з кількох ключових етапів: аналіз і виявлення потенційних загроз, оцінювання поточного рівня інформаційної безпеки, визначення й реалізація заходів для його підвищення, а також формування прогнозу стану захисту з метою попередження майбутніх ризиків. Застосування апарату нечіткої логіки в моделюванні дає змогу враховувати множину зовнішніх та внутрішніх впливів – зокрема, рівень підготовки персоналу, тривалість часу після впровадження останніх заходів захисту тощо. Такий підхід забезпечує гнучке оцінювання поточного стану захищеності даних і сприяє своєчасному вдосконаленню політик кібербезпеки у військових освітніх системах.

18. Математична модель розрахунку цінності інформації установи [23]. Математична модель для оцінювання вартості інформації в межах діяльності установи. Сформульовано основні поняття, зокрема: «цінність інформації», «рівень її важливості», «період до повної втрати актуальності», а також «тип права власності». Ці поняття є базовими для аналізу об’єкта, що підлягає захисту.

Детально обґрунтовано набір показників, які доцільно враховувати при оцінюванні вартості інформації, і доведено, що ця вартість залежить від зазначених характеристик. Запропоновано метод обчислення цінності як середнього арифметичного від суми коефіцієнтів, що відповідають різним критеріям. Кожен коефіцієнт визначається шляхом ранжування з урахуванням значущості відповідного параметра – на основі нормативних актів або експертної оцінки.

До ключових коефіцієнтів, які впливають на розрахунок, належать: рівень доступу до інформації, тривалість збереження її актуальності, значущість інформації, а також форма права власності. За результатами моделювання встановлено, що найвищу вартість мають дані, що мають обмежений доступ, стратегічну важливість та перебувають у державній власності. Для ілюстрації підходу наведено приклад із формуванням переліку документів, що підлягають захисту, та обчислено їхню цінність. Запропонована модель дає змогу обґрунтувати потребу в додаткових захисних заходах у межах автоматизованих інформаційних систем установи, а також підтримує якісніше формування моделей загроз в ІКТ-середовищі.

Для забезпечення об’єктивності та повноти аналізу моделей, методів та систем оцінювання наслідків витоку персональних даних необхідним є визначення системи параметрів, що дозволить створити уніфіковану основу для структурованої оцінки відповідності, ефективності та придатності існуючих рішень у конкретному правовому та технологічному контексті [24, 25].

По-перше, встановлення чітких критеріїв уможливлює уніфікацію підходу до оцінювання. Оскільки кожен метод має власну структуру, принципи побудови, формати даних та сферу застосування, параметризований підхід дозволяє порівнювати ці рішення між собою незалежно від їх походження або первинного призначення.

По-друге, важливим є критерій відповідності правовим вимогам, зокрема Регламенту Європейського Союзу 2016/679 (GDPR), що визначає нормативні рамки обробки персональних даних. Параметр «GDPR-сумісність» дозволяє оцінити, наскільки модель чи метод враховують чинні правові стандарти в галузі захисту даних.

По-третє, практична доцільність впровадження аналізованих підходів оцінюється через параметри наявності програмного забезпечення та сферу застосування. Це дає змогу виявити, які з методів можуть бути безпосередньо використані в державному чи корпоративному середовищі, а які є виключно теоретичними або концептуальними.

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107. https://doi.org/10.31673/2409-7292.2025.031228

По-четверте, доцільно враховувати повноту охоплення категорій втрат, які можуть виникнути внаслідок витоку даних: фінансові, репутаційні, правові. Аналіз джерел даних (експертні, технічні, історичні) допомагає визначити, чи має метод базу для прийняття рішень на основі емпіричних доказів або сценарного моделювання.

Нарешті, формат оцінки та тип результату відіграють ключову роль у можливості інтеграції обраного підходу до систем управління ризиками та стратегічного планування. Наприклад, моделі, що надають кількісну оцінку у грошовому вираженні, є придатними для економічного обґрунтування витрат на захист даних.

Таким чином, формалізація параметрів оцінювання дозволяє здійснити комплексний, методично обґрунтований вибір найбільш ефективних рішень, ідентифікувати прогалини в існуючих підходах та визначити напрями для подальших досліджень і розробки нових моделей, що відповідають сучасним викликам у сфері захисту персональних даних (табл. 1).

Таблиця 1

Аналіз методів, моделей та систем оцінювання наслідків витоку персональних даних

Методи/Моделі/Системи	GDPR сумісність	ПЗ/реалізація	Сфера застосування			Джерело даних			Категорії втрат		Формат оцінки			Тип результату	
			Захист персональних даних	Інформаційна/ кібербезпека	Спеціалізовані/ галузеві	Експертні/опитувальні дані	Структурні/технічні дані	Історичні/фактичні інциденти	Репутаційні	Фінансові	Грошовий результат	Бальна/категорійна оцінка	Інтегральний показник	Кількісний	Якісний
1	–	+	–	+	+	+	–	–	+	+	+	–	+	+	–
2	–	+	–	+	–	+	+	+	-	+	+	+	–	+	+
3	+	–	+	+	–	+	+	–	+–	–	–	+	–	–	+
4	–	+	–	+	–	+	+	–	–	+	–	+	–	–	+
5	–	–	–	+	–	+	+	–	+–	+–	–	+	–	–	+
6	–	+	–	+	+	+	–	–	+	+	–	+	–	+	–
7	+	+	+	+	–	+	+	–	–	+	–	+	–	–	+
8	–	+	–	+	–	+	+	–	–	–	–	+	–	–	+
9	+–	–	–	+	+	+	+	–	+–	+–	–	+	–	–	+
10	+	+	+	+	+	+	+	–	–	–	–	+	–	–	+
11	–	+	–	+	–	+	+	–	+–	+–	–	+	–	–	+
12	–	–	–	+	+	+	–	+	+	+	+	–	–	+	–
13	–	+	–	+	+	–	–	+	+	+	+	–	–	+	–
14	+–	–	+	+	+	+	–	+	+	+	+	–	–	+	–
15	–	–	–	+	+	–	+	–	+	–	–	+	–	–	+
16	+–	–	+	–	+	–	+	–	+	–	–	–	+	+	–
17	+–	+	+	+	+	+	+	–	+	–	–	+	+	+	+
18	+–	–	–	+	+	+	+	–	+	+	–	–	+	+	–

Висновки та перспективи подальших досліджень

Проведений аналіз демонструє, що більшість систем, моделей та методів або не охоплюють усіх аспектів негативних наслідків витоку персональних даних, або не адаптовані до вимог GDPR. Лише частина безпосередньо сумісна з GDPR (DPIA, NIST Privacy Framework, EBIOS, частково OCTAVE тощо) прямо або повністю відповідають вимогам GDPR. Це свідчить про обмежену кількість інструментів, які спеціально адаптовані до європейського правового довкілля. Більшість підходів мають якісний або змішаний характер – ISO 31000, DPIA, MEHARI, EBIOS, OCTAVE, CRAMM, здебільшого оперують експертними оцінками,

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107. https://doi.org/10.31673/2409-7292.2025.031228

анкетами чи сценаріями без кількісної грошової оцінки, що ускладнює обґрунтування реальних фінансових наслідків для бізнесу. Тільки деякі моделі та методи оцінюють фінансові втрати безпосередньо – FAIR, Ponemon Cost Model, CyberVaR, Quantitative Assessment. Вони дозволяють здійснювати кількісну оцінку наслідків у грошовому вираженні, що є критично важливим для стратегічного планування та прийняття управлінських рішень. Переважна частина моделей вимагає суттєвих ресурсів на впровадження або дорогих інструментів (наприклад, FAIR через RiskLens або MEHARI через власні тулкити), що обмежує їхнє застосування для малих та середніх підприємств. Деякі моделі та методи (наприклад, NIST SP 800-30, ISO 27005, OWASP Risk Rating) орієнтовані виключно на технічну або IT-безпеку без правового контексту, що робить їх недостатніми для комплексної оцінки юридичних наслідків витоків персональних даних. Моделі та методи, побудовані виключно на опитуваннях чи інтерв'ю (Ponemon, MEHARI), можуть втрачати точність через залежність від суб'єктивної оцінки та зміни ринку. У цьому контексті методи, що базуються на структурованих експертних правилах або формалізованих коефіцієнтах, виглядають більш стабільними.

Українські моделі, представлені в аналізі, демонструють значний потенціал для адаптації до національних умов: вони враховують специфіку критичної інфраструктури, дистанційного навчання в ЗСУ, а також топології соціальних мереж. Ці підходи є перспективними, але потребують доопрацювання в частині стандартизації, відповідності GDPR і створення інструментів для практичного використання.

Отже, існує потреба у створенні інтегрованих теоретичних і прикладних засобів, які б дозволили: формалізовано оцінювати втрати від витоків персональних даних; підтримувати прийняття управлінських рішень у кризових ситуаціях; забезпечувати відповідність сучасним вимогам законодавства у сфері захисту даних.

Перелік посилань

1. Cost-Effective Risk Management | Resources. Quantitative Information Risk Management | The FAIR Institute. URL: https://www.fairinstitute.org/learn-fair

2. Fair Information Practice Principles (FIPPs). Home | FPC.gov. URL: https://www.fpc.gov/resources/fipps/

3. Introduction to FAIR. Medium. URL: https://medium.com/@enstructure/ introduction-to-fair-bc5e7da0e72c

4. NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/ legacy/sp/ nistspecialpublication-800-30r1.pdf.

5. NIST Risk Management Framework | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc. nist.gov/Projects/risk-management/about-rmf.

6. Луцький М.Г., Іванченко Є.В., Казмірчук С.В., Охрименко А.А. Сучасні засоби управління інформаційними ризиками. Захист інформації. 2011. Т.13. № 3 (52). С. 97-108.

7. Луцький М.Г., Корченко А.Г., Іванченко Є.В., Казмірчук С.В. Дослідження програмних засобів аналізу та оцінки ризиків інформаційної безпеки. Захист інформації. 2011. Т. 13. № 2 (51). С. 86-94.

8. NIST Privacy Framework: NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs /CSWP/ NIST.CSWP.01162020.pdf.

9. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT). БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: https: // online.budstandart.com / ua /catalog/doc-page.html?id_doc= 104400.

10. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT) URL: https://zakon.isu.net.ua/sites/default/files/normdocs /dstu_iso_31000_2018.pdf.

11. OWASP Risk Rating Methodology | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https: // owasp.org / www-community/OWASP_ Risk_Rating_Methodology

12. Data Protection Impact Assessment (DPIA) GDPR.eu. GDPR.eu. URL: https: // gdpr.eu / data-protection-impact-assessment-template/.

13. О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017, 435 с.

14. Applying OCTAVE: Practitioners Report. URL: https://kilthub.cmu.edu/ articles/report/Applying_OCTAVE_ Practiti oners_Report/6571985/1?file=12057020.

15. «Expression des Besoins et Identification des Objectifs de Sécurité EBIOS», Méthode de gestion des risques, ANSSI/ACE/BAC, Paris, Version du 25 janvier 2010, 95 p.

© Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. (2025) Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації, 3(63), 99–107. https://doi.org/10.31673/2409-7292.2025.031228

16. Потій О. В., Лєншин А. В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу. Збірник наукових праць Харківського університету Повітряних сил. 2010. Вип. 2. С. 85-91. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2010_2_21.

17. Security Studies | Ponemon Institute. Ponemon Institute. URL: https://www.ponemon.org/research/ponemon-library/security/?tag=5.

18. Cyber Value at Risk (CVaR): Measuring Worst-Case Scenarios - Horkan. URL: https://horkan.com/2025/04/21 / cyber-value-at-risk-cvar-measuring-worst-case-scenarios # :~: text = *% 20Focus % 20on % 20Worst,from%20 - ransomware%20 to%20insider%20attacks.

19. Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. Applied Sciences, 11(8), 3678. URL: https://doi.org/ 10.3390/ app11083678.

20. Korchenko A., Dreis Yu., Roshchuk M., Romanenko O. Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state. Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 29-35. https: // doi.org / 10.18372/2225-5036.24.12606.

21. Савченко В.А., Ахрамович В.М., Акулінічева М.В. Оцінювання параметрів безпеки персональних даних у степеневих соціальних мережах на основі їх топології. Сучасний захист інформації, №3(43), 2020. С. 6-13. URL: https://doi.org/10.31673/2409-7292.2020.030613.

22. Шапран О.О. Моделі підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України. Телекомунікаційні та інформаційні технології, 2022, № 2 (79). С. 33-45. URL: https://doi.org/10.31673/2412-4338.2022.023345.

23. Бойченко О. С., Костерев Д. С., Маковський І. Ю., Грищук О.М. Математична модель розрахунку цінності інформації установи. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем, 2022, №22, С.30–40. https://doi.org/10.46972/2076-1546.2022.22.03.

24. Толбатов А., Лозова І., Котик О., Толбатова О. Автоматизована система вибору засобів оцінювання збитків від втрати персональних даних. ІМА: 2024: Матеріали міжнародної наукової конференції молодих учених «Інформатика, математика, автоматика», Суми–Астана, 22–26 квітня 2024 р. Суми, 2024. С.256. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059494.pdf.

25. Лозова І., Біскупський А., Горожанова А. Засоби оцінювання шкоди від втрати інформації з обмеженим доступом. Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2021): збірник тез наукових доповідей, 23-26 червня 2021 р. Миколаїв, Коблево, 2021. С.58-62.

Надійшла 13.07.2025