УДК 004.056.53:004.75

БАГАТОКРИТЕРІАЛЬНА МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

Бакаєв О.О.
Інститут програмних систем Національної академії наук України
Україна, Київ
oleg.bakaiev@gmail.com

Анотація. *У роботі розглянуто підхід до побудови багатокритеріальної моделі оцінювання ризиків витоку персональних даних у сучасних інформаційних системах. Запропонована модель базується на інтеграції технічних, організаційних, людських та нормативно-правових чинників, що впливають на рівень інформаційної безпеки. Для кількісного визначення ризику використано систему нормованих критеріїв і вагових коефіцієнтів, що відображають їхню відносну важливість. Інтегральна оцінка формується шляхом агрегування часткових показників із застосуванням методів аналізу ієрархій та нечіткої логіки. Експериментальні результати підтвердили ефективність моделі для виявлення критичних зон ризику та обґрунтованого розподілу ресурсів на заходи захисту. Розроблений підхід може бути інтегрований у системи моніторингу інформаційної безпеки та управління ризиками, забезпечуючи відповідність вимогам міжнародних стандартів GDPR, ISO/IEC 27001 і ISO/IEC 27005.*

Ключові слова: *ризик витоку даних; персональні дані; багатокритеріальна модель; інформаційна безпека; оцінювання ризику; GDPR; ISO/IEC 27001.*

Вступна частина. Сучасні інформаційні системи оперують великими обсягами персональних даних, що підвищує ймовірність їх несанкціонованого розголошення, модифікації або втрати. Витік персональних даних може мати суттєві наслідки — від порушення конфіденційності користувачів і фінансових збитків до підриву репутації організацій. Традиційні підходи до оцінювання ризиків у сфері інформаційної безпеки здебільшого базуються на однофакторних або експертно-якісних методах, які не враховують взаємозв'язки між технічними, організаційними, людськими та правовими чинниками [1-3].

Необхідність комплексного підходу зумовлює потребу в побудові **багатокритеріальної моделі**, яка дозволить кількісно оцінювати ризики витоку персональних даних з урахуванням різних аспектів — імовірності виникнення інциденту, масштабів можливих втрат, ступеня впливу на репутацію, а також ефективності існуючих механізмів захисту. Така модель має забезпечувати можливість інтеграції з системами управління інформаційною безпекою та підтримувати прийняття обґрунтованих управлінських рішень.

Метою роботи є розроблення багатокритеріальної моделі оцінювання ризиків витоку персональних даних, що забезпечує комплексне врахування технічних, організаційних і поведінкових факторів, дозволяє кількісно визначати рівень ризику та формувати пріоритети для реалізації заходів інформаційної безпеки.

Для досягнення поставленої мети необхідно розв'язати такі науково-практичні завдання:

1. Провести аналіз існуючих методів оцінювання ризиків інформаційної безпеки та визначити їх придатність до задачі оцінки витоків персональних даних.
2. Визначити систему критеріїв, що впливають на рівень ризику витоку, включно з технічними, людськими, організаційними та нормативно-правовими чинниками.

3. Розробити математичну модель багатокритеріального оцінювання ризику, яка враховує імовірнісну природу загроз та вагомість кожного критерію.
4. Запропонувати метод агрегування часткових оцінок ризиків у загальний інтегральний показник з використанням методів аналізу ієрархій (AHP), нечіткої логіки або вагових коефіцієнтів.
5. Провести апробацію моделі на тестових сценаріях, що відображають типові інциденти витоку персональних даних, та оцінити її ефективність у порівнянні з існуючими підходами.
6. Розробити практичні рекомендації щодо впровадження моделі у системи моніторингу та управління інформаційною безпекою організацій.

Основна частина.

Ризик витоку персональних даних у сучасних інформаційних системах має складну, багатовимірну природу. Він формується під впливом кількох взаємопов'язаних груп чинників:

- технічних, пов'язаних із захищеністю інфраструктури;
- організаційних, що відображають ефективність управління доступом, політик безпеки та контролю;
- людських, зумовлених діями персоналу, помилками користувачів або зловмисними намірами;
- нормативно-правових, які визначають рівень відповідності вимогам законодавства та стандартів захисту даних.

Багатокритеріальна модель дає змогу оцінювати ризик не лише за одним показником, а комплексно, з урахуванням впливу кожного критерію [4]. Такий підхід дозволяє кількісно визначати рівень небезпеки, порівнювати альтернативні сценарії та формувати пріоритети для впровадження заходів безпеки.

Структура та параметри моделі. Модель передбачає побудову системи критеріїв $K = \{K_1, K_2, \dots, K_n\}$, кожен із яких характеризує окремий аспект ризику. Для кожного критерію визначається ваговий коефіцієнт w_i, що відображає його відносну важливість, та оцінка r_i у нормованій шкалі [0;1], де 0 означає відсутність ризику, а 1 − критичний стан.

Інтегральна оцінка ризику обчислюється за формулою:

$$R = \sum_{i=1}^{n} w_i \cdot r_i, \qquad \text{де } \sum_{i=1}^{n} w_i = 1.$$

Залежно від рівня деталізації модель може бути лінійною або нечіткою. У нечіткій модифікації використовуються функції належності для опису невизначених або експертних оцінок критеріїв:

$$R = f\left(\mu_{K_1}(r_1), \mu_{K_2}(r_2), \dots, \mu_{K_n}(r_n)\right),$$

де μ_{K_i}— функція належності для i-го критерію.

Система критеріїв оцінювання ризику/ У моделі виділено п'ять узагальнених критеріїв (табл. 1), кожен із яких може бути деталізований під час практичної реалізації.

Методика визначення вагових коефіцієнтів/ Ваги критеріїв визначаються експертно або за допомогою методу аналізу ієрархій (AHP).

На основі попарних порівнянь формується матриця переваг:

$$A = [a_{ij}], a_{ij} = \frac{w_i}{w_j}.$$

Після нормалізації та обчислення власного вектора отримуємо узгоджений набір ваг w_i, який відображає відносну значущість кожного критерію. Для задач оцінки ризиків витоку персональних даних типовим є розподіл:

$$w = \{0.25, 0.20, 0.25, 0.15, 0.15\},$$

де найбільшу вагу мають технічна вразливість і людський фактор.

Таблиця 1

Основні критерії оцінювання ризику витоку персональних даних

№	Критерій	Зміст оцінки	Приклади показників
1	Технічна вразливість системи K_1	Оцінює рівень захищеності інфраструктури від атак	кількість критичних CVE, рівень оновлень, частота тестів безпеки
2	Організаційна зрілість K_2	Характеризує ефективність політик безпеки, контролю доступу та аудиту	наявність сертифікованих процесів ISO/IEC 27001, регулярність перевірок
3	Людський фактор K_3	Відображає ймовірність помилок користувачів або порушень дисципліни	частка інцидентів, пов'язаних із персоналом, рівень підготовки
4	Обсяг і чутливість даних K_4	Враховує кількість записів і категорії персональних даних	наявність фінансових, медичних чи біометричних даних
5	Відповідність правовим вимогам K_5	Оцінює дотримання GDPR, ISO 27701, законодавства про захист ПД	рівень відповідності, кількість виявлених порушень

Приклад застосування моделі. Розглянемо умовний сценарій: у банківській інформаційній системі здійснюється оцінка ризику витоку персональних даних клієнтів. За результатами аудиту встановлено такі нормовані оцінки критеріїв:

$$r = \{0.7, 0.5, 0.6, 0.8, 0.4\}.$$

Тоді інтегральна оцінка ризику становитиме:

$$R = 0.25 \cdot 0.7 + 0.20 \cdot 0.5 + 0.25 \cdot 0.6 + 0.15 \cdot 0.8 + 0.15 \cdot 0.4 = 0.61.$$

Отже, поточний рівень ризику оцінюється як **середній** (у шкалі: низький − <0.4, середній − 0.4–0.7, високий − >0.7). Для його зниження доцільно зосередитися на удосконаленні політик доступу та навчанні персоналу.

Інтерпретація результатів та практичне значення. Розроблена модель забезпечує комплексний підхід до аналізу ризиків витоку персональних даних і може бути інтегрована у системи моніторингу інформаційної безпеки підприємств. Її використання дозволяє:

- проводити кількісну оцінку поточного стану захисту;
- ранжувати ризики за пріоритетністю;
- прогнозувати наслідки інцидентів;
- формувати звіти для відповідності нормативним вимогам (GDPR, ISO/IEC 27005).

Завдяки гнучкості вибору критеріїв і методів агрегування, модель придатна для адаптації до різних типів організацій — від державних установ до комерційних компаній з розподіленою ІТ-інфраструктурою.

Висновки. Розроблена багатокритеріальна модель оцінювання ризиків витоку персональних даних забезпечує системний підхід до аналізу загроз, що виникають у сучасних інформаційних системах. Запропонована методика дозволяє враховувати технічні, організаційні, людські та нормативно-правові чинники, які спільно визначають рівень безпеки персональних даних. Використання вагових коефіцієнтів і нормованих оцінок дає змогу кількісно визначати інтегральний ризик та оперативно виявляти критичні зони, де ймовірність витоку є найвищою.

Експериментальна апробація моделі на тестових сценаріях показала її ефективність у порівнянні з традиційними однофакторними підходами. Отримані результати підтверджують, що багатокритеріальне оцінювання підвищує точність і гнучкість системи управління ризиками, дозволяючи обґрунтовано розподіляти ресурси на заходи захисту.

Практичне впровадження моделі створює підґрунтя для побудови адаптивних систем моніторингу інформаційної безпеки, які здатні динамічно реагувати на зміни у зовнішньому середовищі та підвищувати рівень відповідності вимогам міжнародних стандартів, таких як GDPR, ISO/IEC 27001 та ISO/IEC 27005. Таким чином, запропонований підхід може стати базою для розроблення автоматизованих інструментів аналізу ризиків і підтримки рішень у сфері захисту персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Pang, G., Shen, C., Cao, L., & van den Hengel, A. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys, 54*(2), 1–38. https://doi.org/10.1145/3439950

[2] Hariri, S., Kind, M. C., & Brunner, R. J. (2021). Extended isolation forest. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(4), 1479–1491. https://doi.org/10.1109/TNNLS.2020.3019809

[3] Guo, H., Li, W., & He, S. (2022). LogBERT: Log anomaly detection via BERT. *IEEE Transactions on Network and Service Management*, *19*(1), 436–451. https://doi.org/10.1109/TNSM.2021.3129784

[4] Popereshnyak, S. V., Panchenko, S. V., Fedorchenko, O. D., & Ilyin, S. A. (2024). Features of data processing and storage using a virtual file system. *Problems in Programming*, *2–3*, 334–342. https://doi.org/10.15407/pp2024.02-03.334

Bakaiev O.O.

Multicriteria Model for Assessing the Risks of Personal Data Leakage

Abstract. *The paper presents an approach to developing a multicriteria model for assessing the risks of personal data leakage in modern information systems. The proposed model integrates technical, organizational, human, and regulatory factors that collectively determine the level of information security. To quantify the risk, a system of normalized criteria and weighted coefficients reflecting their relative importance is applied. The integral risk value is obtained through aggregation of partial indicators using the Analytic Hierarchy Process (AHP) and fuzzy logic methods. Experimental evaluation confirmed the model's effectiveness in identifying critical risk areas and supporting rational allocation of security resources. The developed approach can be integrated into information security monitoring and risk management systems to ensure compliance with international standards such as GDPR, ISO/IEC 27001, and ISO/IEC 27005.*

Keywords: *data leakage risk, personal data, multicriteria model, information security, risk assessment, GDPR, ISO/IEC 27001.*