УДК 004.056.5:005.8 DOI: 10.31673/2786-8362.2024.028264

Корченко О.Г., д.т.н.; **Лозова І.Л.**

СТРУКТУРНА МОДЕЛЬ СИСТЕМИ ОЦІНКИ НЕГАТИВНИХ НАСЛІДКІВ ВТРАТИ ПЕРСОНАЛЬНИХ ДАНИХ

Korchenko O.G., Lozova I.L. Structural model of the system for assessing the negative consequences of personal data loss. The article presents a structural model of a system for assessing the negative consequences of personal data breaches, aimed at enhancing the level of information security within organizations. The primary goal of the proposed model is to ensure effective risk management related to data leaks or unauthorized access to personal data by automating the processes of incident identification, impact assessment, and developing recommendations for mitigating consequences. The developed system considers modern data protection requirements, particularly the provisions of the General Data Protection Regulation (GDPR). It comprises the following key functional blocks: data formation and storage, incident identification and breach severity determination, expert information generation, and expert data processing. The use of the proposed approach helps reduce financial losses caused by personal data leaks, increases the organization's trust level, and ensures compliance with regulatory requirements in the field of information protection.

Keywords: personal data protection, negative consequences assessment system, information security assessment, GDPR Regulation, damage assessment, personal data loss, personal data confidentiality.

Корченко О.Г., Лозова І.Л. Структурна модель системи оцінки негативних наслідків втрати персональних даних. У статті представлено структурну модель системи оцінки негативних наслідків втрати персональних даних, яка спрямована на підвищення рівня інформаційної безпеки організацій. Система дозволяє автоматизувати процес аналізу ризиків, прогнозувати можливі наслідки витоків даних та мінімізувати фінансові втрати, відповідаючи вимогам GDPR. Розглянуто структуру системи, що включає блоки формування та зберігання даних, ідентифікації та визначення рівня порушення, формування експертної інформації, обробки експертних даних. Запропонований підхід забезпечує адаптацію до специфіки організацій та створює основу для ефективного управління ризиками і захисту персональних даних.

Ключові слова: захист персональних даних, система оцінювання негативних наслідків, оцінювання у сфері інформаційної безпеки, Регламент GDPR, оцінювання збитків, втрата персональних даних, конфіденційність персональних даних.

Вступ

Актуальність розробки системи оцінки негативних наслідків втрати персональних даних обумовлена зростаючою важливістю інформаційної безпеки в умовах цифрової трансформації суспільства. Персональні дані стали одним із найцінніших активів, як для приватних осіб, так і для організацій. Однак зростання обсягів даних та їх використання супроводжується посиленням кіберзагроз, які можуть призвести до витоків даних, несанкціонованого доступу, маніпуляцій або втрати інформації. Сучасні кіберзагрози створюють серйозні економічні та соціальні виклики. Витоки персональних даних спричиняють значні фінансові втрати для організацій, включаючи штрафи за порушення нормативних вимог, судові витрати та компенсації постраждалим. Додатково, вони завдають шкоди репутації організацій, що негативно впливає на їхню конкурентоспроможність. Законодавчі вимоги, такі як Загальний регламент захисту даних (GDPR), накладають обов’язок на організації забезпечувати високий рівень захисту персональних даних і здійснювати оцінку ризиків, пов’язаних із їх втратою чи витоком. Недотримання цих норм тягне за собою суттєві юридичні та фінансові наслідки. Автоматизація процесів оцінки ризиків стає критично необхідною через збільшення обсягів оброблюваних даних та необхідність швидкого реагування на інциденти. Традиційні ручні методи аналізу вже не забезпечують достатньої ефективності та швидкості виявлення загроз і прогнозування їхніх наслідків.

У зв’язку із вищезазначеним актуальною задачею є розробка моделі системи оцінювання негативних наслідків втрати персональних даних, що спрямована на автоматизацію ключових процесів аналізу ризиків, прогнозування наслідків та розробку заходів для їх мінімізації.

Використання такої системи буде сприяти покращенню рівня захисту інформації, зниженню фінансових ризиків і забезпеченню відповідності організації сучасним нормативним вимогам у сфері інформаційної безпеки.

Аналіз останніх досліджень. Аналіз існуючих систем оцінки негативних наслідків втрати персональних даних виявляє декілька підходів, що використовуються організаціями для управління ризиками та забезпечення відповідності законодавчим вимогам, зокрема GDPR.

Data Protection Impact Assessment, DPIA: DPIA є процедурою, передбаченою статтею 35 GDPR, яка допомагає систематично аналізувати, виявляти та мінімізувати ризики для персональних даних під час їх обробки [1]. Цей процес включає оцінку потенційних загроз, визначення їх ймовірності та впливу, а також розробку заходів для зниження ризиків.

Information Security Management Systems, ISMS: Багато організацій впроваджують ISMS відповідно до стандарту ISO/IEC 27001, який включає процеси оцінки ризиків, пов'язаних із втратою персональних даних [2]. Ці системи забезпечують структурований підхід до управління інформаційною безпекою, включаючи ідентифікацію ризиків, оцінку їх впливу та впровадження відповідних заходів контролю.

Методики аналізу ризиків: Існують різні методики аналізу ризиків, такі як OCTAVE, NIST SP 800-30 та інші, які допомагають організаціям ідентифікувати, оцінювати та управляти ризиками, пов'язаними з обробкою персональних даних. Ці методики надають інструменти для кількісної та якісної оцінки ризиків, що дозволяє приймати обґрунтовані рішення щодо заходів безпеки [3, 4].

Compliance Assessment Tools: Це інструменти для автоматизованого моніторингу та оцінки відповідності організацій різним нормативно-правовим актам, таким як GDPR, CCPA, HIPAA тощо. OneTrust DataGuidance надає шаблони для оцінки ризиків, автоматизує процеси моніторингу змін у законодавстві та управління даними, допомагаючи організаціям забезпечити відповідність вимогам [5]. LogicGate спеціалізується на автоматизації процесів управління ризиками, пропонуючи індивідуальні робочі потоки для оцінки відповідності, а також інтеграцію з іншими системами для ефективного моніторингу та звітності [6]. Varonis забезпечує моніторинг і аналіз доступу до даних, виявлення аномалій та надійну звітність, допомагаючи організаціям підтримувати відповідність вимогам GDPR і забезпечувати високий рівень безпеки даних [7]. Всі ці інструменти знижують ризики порушень, підвищують рівень безпеки даних і спрощують дотримання нормативів.

Недоліки існуючих систем оцінки негативних наслідків втрати персональних даних у контексті вимог GDPR часто пов'язані з наступними аспектами:

– обмеженість автоматизації та інтеграції – багато систем не мають достатньої автоматизації, що ускладнює їх інтеграцію в бізнес-процеси та оперативне реагування на порушення;

– складність урахування специфіки організації – типові моделі оцінки часто не враховують індивідуальних особливостей обробки даних конкретної організації;

– відсутність ефективного моніторингу та звітності – системи можуть не забезпечувати постійного моніторингу стану даних або звітності про інциденти;

– нестача прозорості алгоритмів оцінки – алгоритми, що використовуються в системах, можуть бути недостатньо прозорими або складними для розуміння;

– складність впровадження у малих і середніх підприємствах – системи часто є дорогими та складними для впровадження у малих і середніх підприємствах, це створює бар’єри для відповідності регламенту, особливо для малих організацій.

Постановка завдання. Згідно з вимогами Загального регламенту захисту даних (GDPR), захист персональних даних та управління ризиками, пов'язаними з їх порушенням, є ключовими аспектами для будь-якої організації, що обробляє персональні дані. У цьому контексті постає необхідність створення системи, яка б оцінювала можливі негативні наслідки від порушення конфіденційності даних.

Задачі, які необхідно вирішити при розробці системи:

– визначення типів персональних даних, які піддаються обробці.

– оцінка ймовірності інцидентів, що призводять до витоку, втрати чи несанкціонованого доступу до персональних даних;

– розрахунок потенційних фінансових втрат через порушення вимог GDPR, включаючи штрафи;

– моделювання сценаріїв негативних наслідків із врахуванням специфіки організації;

– розробка програмного забезпечення для автоматизованого збору та аналізу даних про ризики.

– впровадження механізмів оцінки наслідків, що відповідають Регламенту GDPR.

– формування рекомендацій щодо мінімізації ризиків і запобігання майбутнім порушенням конфіденційності.

Мета постановки завдання – створити інтегровану систему, яка дозволяє організаціям відповідати високим стандартам захисту персональних даних, зменшувати ризики порушення конфіденційності та мінімізувати негативні наслідки для бізнесу та суб'єктів даних.

Метою роботи є розробка та обґрунтування структурної моделі системи оцінки негативних наслідків від втрати персональних даних, що дозволить виявляти, аналізувати та прогнозувати ризики, пов'язані з витоком конфіденційної інформації. Зокрема, система спрямована на мінімізацію фінансових втрат організацій, а також на забезпечення відповідності вимогам сучасного законодавства і стандартів інформаційної безпеки.

Запропоновані підходи покликані підвищити ефективність управління ризиками, автоматизувати процеси оцінки, та створити основу для розробки рекомендацій щодо запобігання втраті персональних даних у майбутньому.

Виклад основного матеріалу дослідження.

На основі розробленої кортежної GDPR-моделі параметрів персональних даних [8] та методу оцінювання негативних наслідків від порушення конфіденційності персональних даних [9] розроблено структурну модель системи оцінки негативних наслідків втрати персональних даних (рис. 1), яка містить:

– блок формування та зберігання даних (БФЗД);

– блок ідентифікації та визначення рівня порушення (БІВРП);

– блок формування експертної інформації (БФЕІ);

– блок обробки експертних даних (БОЕД).

БФЗД служить для підготовки даних, заснованих на судженнях експертів і складається з:

– бази даних групи питань (БДГП) – містить питання для аналізу ризиків;

– бази даних результатів опитувань (БДРО) – включає зібрані відповіді експертів;

– бази даних рекомендацій (БДР) – зберігає пропозиції щодо мінімізації ризиків.

БІВРП складається з:

– модуля визначення загального глобального річного обігу (ЗГРО) – формування компоненти $T^{\ominus}$ здійснюється шляхом визначення експертом річного обігу в €;

– модуля визначення показника рівня порушення (ПРП) – показник рівня порушення $P^{\varphi}_{РП}$ обчислюється на основі множини визначених рівнів порушення, відносно яких формується коефіцієнт максимально можливого збитку.

БФЕІ – складається з модулів оцінювання та вибору певних характеристик порушення (специфіка порушення (СП), характер порушення (ХП), зниження шкоди (ЗШ), ступінь відповідальності (СВ), рецидив порушення (РП), рівень співпраці (РС), категорії даних (КД), спосіб виявлення (СПВ), відповідність заходам (ВЗ), дотримання кодексів (ДК), визначаючий чинник (ВЧ)), що засновується на конкретних оцінках діяльності підприємства, які в результаті сформують значення показників $P^{\varphi}_{СП}$, $P^{\varphi}_{ХП}$, $P^{\varphi}_{ЗШ}$, $P^{\varphi}_{СВ}$, $P^{\varphi}_{РЦП}$, $P^{\varphi}_{РС}$, $P^{\varphi}_{КД}$, $P^{\varphi}_{СПВ}$, $P^{\varphi}_{ВЗ}$, $P^{\varphi}_{ДК}$ та $P^{\varphi}_{ВЧ}$, що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства.

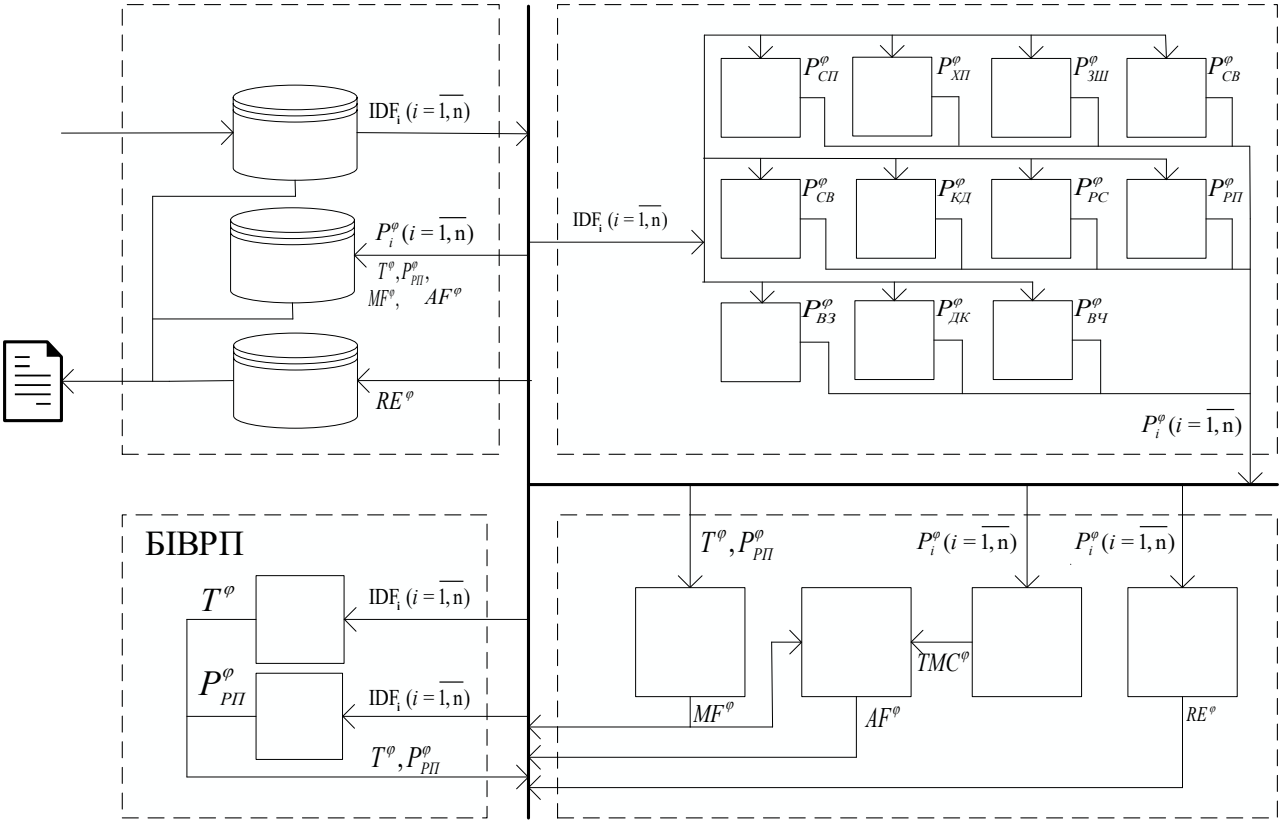

Рис. 1. Структурна модель системи оцінки негативних наслідків втрати персональних даних

БОЕД складається з:

– модуля вибору рекомендацій (ВР) – виставлення рекомендацій RE^{φ} для БФЕІ, відповідно до суджень експерта та своєї приналежності до певної категорії;

– модуля визначення коефіцієнта суми набраних балів (КСНБ) – визначення змінної TMC^{φ}, що буде містити коефіцієнт обчисленої кількості отриманих балів;

– модуля визначення максимального штрафу (МШ) – визначення змінної MF^{φ} для обрахунку максимального збитку для підприємства;

– модуля визначення максимально наближеного штрафу (МНШ), визначення змінної AF^{φ}, що відповідає за обчислення максимально наближеного штрафу з урахування КСНБ.

Система функціонує наступним чином.

В БДГП фахівці відповідної предметної галузі формують n-компонентний експертний запит $\mathrm{IDF_i}\ (i=\overline{1,n})$, що оцінює ризики витоку персональних даних, їхній вплив та частоту можливих порушень, який поступає на вхід модулів ЗГРО, ПРП, СП, ХП, ЗШ, СВ, РП, РС, КД, СПВ, ВЗ, ДК та ВЧ. В модулі ЗГРО формується компонента T^{φ} (див. (1) в [9]) шляхом визначення експертом річного обігу в євро (на основі фінансової звітності або оцінки). Модуль ПРП обчислює показник рівня порушення $P_{РП}^{\varphi}$ (див. (2) в [9]) на основі множини визначених рівнів порушення, відносно яких формується коефіцієнт максимально можливого збитку що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства. На цьому етапі аналізуються масштаби діяльності організації та рівень серйозності порушення.

В БФЕІ на основі n-компонентного експертного запиту $\mathrm{IDF_i}\ (i=\overline{1,n})$ фахівці відповідної предметної галузі присвоюють вагові коефіцієнти кожній категорії ризиків (наприклад, для конфіденційності, доступності, цілісності даних) з застосуванням експертного підходу та статистичних методів для визначення значущості кожного параметра. Формуються

інтегральні показники $P_{СП}^{\varphi}$, $P_{ХП}^{\varphi}$, $P_{ЗШ}^{\varphi}$, $P_{СВ}^{\varphi}$, $P_{РЦП}^{\varphi}$, $P_{РС}^{\varphi}$, $P_{КД}^{\varphi}$, $P_{СПВ}^{\varphi}$, $P_{ВЗ}^{\varphi}$, $P_{ДК}^{\varphi}$ та $P_{ВЧ}^{\varphi}$ (див. (4), (6), (8), (10), (12), (14), (16), (18), (20), (22), (24) в [9]), які дозволяють оцінити загальний рівень ризиків та порушень. Дані, отримані від фахівців відповідної предметної галузі P_i^{φ} $(i = \overline{1,11})$ зберігаються для подальшої обробки в БДРО. Формування експертної інформації (БФЕІ) об'єднує дані, аналізує їх із використанням вагових коефіцієнтів і прогнозує можливі наслідки витоків даних, що створює основу для ефективного управління ризиками.

Сформовані дані з БІВРП та з БФЕІ $T^{\Rightarrow}$, $P_{РП}^{\varphi}$, P_i^{φ} $(i = \overline{1,11})$ надходять у БОЕД, де формуються інтегральні показники, які дозволяють оцінити загальний рівень ризиків та порушень. На основі результатів n-компонентного експертного запиту P_i^{φ} $(i = \overline{1,11})$ і аналізу розробляються рекомендації RE^{φ} (див. (28) в [9]) для БФЕІ, відповідно до суджень фахівця відповідної предметної галузі та своєї приналежності до певної категорії, спрямовані на зменшення ризиків та формується БДР.

В модулі КСНБ відбувається підрахунок $S^{\varphi} = \sum_{i=1}^{11} P_i^{\varphi}$ (див. (30) в [9]), де P_i^{φ} $(i = \overline{1,11})$ – сума всіх набраних балів виходячи із суджень фахівців відповідної предметної галузі та формується TMC^{φ} (див. (31) в [9]), що буде містити коефіцієнт обчисленої кількості отриманих балів для всіх модулів БФЕІ.

Для визначення максимального збитку для підприємства використовується модуль МШ, дані до якого поступають з модулів ЗГРО та з ПРП, $T^{\Rightarrow}$ та $P_{РП}^{\varphi}$ відповідно, та обчислюється змінна MF^{φ} (див. (33) в [9]), що буде відповідати за максимальний штраф за правилами GDPR. На основі MF^{φ} в блоці МНШ обчислюється максимально наближений штраф AF^{φ} (див. (35) в [9]), що дозволяє визначити фактичний збиток для організації чи підприємства у разі порушення конфіденційності персональних даних.

Всі результати, які було отримано в блоках БІВРП, БФЕІ, БОЕД, записуються в файли для їх подальшої оцінки та обробки. На етапі формування звіту оцінки збитку, відбувається відкриття сформованих файлів та, відповідно до вибраних варіантів відповідей, вибираються рекомендації і обчислюється фактичний збиток для підприємства.

Висновки

Розроблена структурна модель системи оцінки негативних наслідків втрати персональних даних є важливим інструментом для підвищення рівня інформаційної безпеки організацій. Запропонована модель за рахунок впровадження блоків формування та зберігання даних, ідентифікації та визначення рівня порушення, формування експертної інформації, обробки експертних даних дозволяє побудувати автоматизовану систему підтримки прийняття рішень щодо оцінювання негативних наслідків витоку персональних даних та мінімізації відповідних фінансових втрат.

В подальшому необхідно розробити програмне забезпечення для реалізації цієї моделі, що стане важливим етапом у впровадженні відповідних теоретичних результатів, оскільки в перспективі це дозволить організаціям безперешкодно реалізовувати вимоги GDPR і створювати ефективну систему захисту персональних даних.

Впровадження цієї системи також сприятиме зміцненню довіри до організацій, покращить їх репутацію та забезпечить високий рівень захисту від фінансових і юридичних наслідків втрати персональних даних.

Список використаної літератури:

1. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільне переміщення таких даних. Переклад українською мовою. URL: https://zakon.rada.gov.ua/laws/show/984_008-16.

2. ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001.

3. Савельєва Т. В., Панаско О. М., Пригодюк О. М. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. Вісник Черкаського державного технологічного університету. Серія: Технічні науки. 2018. Т. 1, № 1. С. 81–89. URL: https://doi.org/10.24025/2306-4412.1.2018.153279.

4. Методика оцінки ризиків OCTAVE. Офіційний сайт CERT Carnegie Mellon University. URL: https://www.cert.org/octave/.

5. OneTrust DataGuidance. OneTrust DataGuidance. URL: https://www.onetrust.com/products/dataguidance/.

6. LogicGate. LogicGate. URL: https://www.logicgate.com/.

7. Varonis. Varonis. URL: https://www.varonis.com/.

8. Теоретико-множинна GDPR-модель параметрів персональних даних / О. Г. Корченко та ін. Ukrainian Information Security Research Journal. 2020. Т. 22, № 2. С. 120–141. URL: https://doi.org/10.18372/2410-7840.22.14871.

9. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних / В. Шульга та ін. Ukrainian Information Security Research Journal. 2023. Т. 25, № 4. С. 254–268. URL: https://doi.org/10.18372/2410-7840.25.18232.

Автори статті

Корченко Олександр – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0003-3376-0631

Лозова Ірина – старший викладач, Державний університет «Київський авіаційний інститут», Київ, Україна.

ORCID: 0000-0002-7224-4763

Authors of the article

Korchenko Oleksandr – Doctor of Science (technic), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0003-3376-0631

Lozova Iryna – senior lecturer, State University «Kyiv Aviation Institute», Kyiv, Ukraine.

ORCID: 0000-0002-7224-4763