МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кваліфікаційна наукова праця
на правах рукопису

ЛОЗОВА ІРИНА ЛЕОНІДІВНА

УДК 004.056.5:004.4(043)

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ОЦІНЮВАННЯ НЕГАТИВНИХ НАСЛІДКІВ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

Спеціальність 05.13.21 «Системи захисту інформації»

Подається на здобуття наукового ступеня
кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Ірина ЛОЗОВА

Науковий керівник:
КОРЧЕНКО Олександр Григорович,
доктор технічних наук, професор

Київ – 2025

АНОТАЦІЯ

Лозова І.Л. Моделі та методи оцінювання негативних наслідків від витоку персональних даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Державний університет інформаційно-комунікаційних технологій, Київ, 2025.

У дисертаційній роботі вирішується актуальна наукова задача розробки моделей та методів оцінювання негативних наслідків, спричинених витоком персональних даних для подальшої підтримки процесу прийняття рішень щодо мінімізації ризиків, оцінювання втрат та підвищення загального рівня інформаційної безпеки організацій.

У дисертаційній роботі нові наукові результати і висновки отримані на основі теоретико-множинного підходу, теоріях нечіткої логіки, прийняття рішень, алгоритмів, алгебри логіки, методах експертного оцінювання, моделювання інформаційних процесів і структур та операціях нечіткої арифметики. Вірогідність наукових результатів, висновків і рекомендацій, викладених у дисертаційній роботі, обґрунтовано використанням математичного апарату та моделювання на ЕОМ.

У процесі теоретичних досліджень і моделювання, у дисертаційній роботі отримані наступні наукові результати:

1) вперше розроблено теоретико-множинну та кортежну моделі параметрів персональних даних, в яких відповідно за рахунок формалізації множини показників річного обігу, рівня, специфіки та характеру порушення, зниження шкоди, ступеню відповідальності тощо та композиції коефіцієнтів важливості інформаційних ресурсів, ідентифікаторів середовища обробки та загроз, характеристик механізмів захисту, функціональних профілів безпеки і величини можливих збитків, дозволило відповідно формалізувати і моделювати вплив кожного із параметрів, що впливають на оцінювання збитку відповідно до Регламенту GDPR та визначити множини вхідних та вихідних параметрів для

формалізації процесу оцінювання шкоди від витоку персональних даних з урахуванням національного нормативно-правового забезпечення;

2) вперше розроблено метод оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR та метод оцінювання безпеки персональних даних, в яких відповідно за рахунок побудованої теоретико-множинної GDPR-моделі параметрів та реалізації аналітичного перетворення множин величин, що відображають судження експертів, розроблених нових правил оцінювання, розсіювання балів і визначеної множини рекомендацій та за рахунок побудованої кортежної моделі параметрів персональних даних та аналітичного перетворення множин вхідних даних (аналіз документів, середовища та мети обробки персональних даних, аналіз функціонуючих механізмів безпеки, ідентифікація можливих загроз захисту персональних даних тощо), дозволило відповідно визначати величину максимального та фактичного збитків для організації у разі витоку персональних даних і надавати рекомендації щодо вибору політики їх безпеки відповідно до положень Регламенту GDPR та дозволило надавати рекомендації щодо вибору політики безпеки персональних даних і послуг безпеки та визначати величину можливої шкоди у разі витоку таких персональних даних з урахуванням національного нормативно-правового забезпечення;

3) вперше запропоновано структурну модель системи оцінювання негативних наслідків від витоку персональних даних, що за рахунок використання методу оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR та 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.

Практичне значення одержаних результатів:

1) здійснено комплексний аналіз вітчизняних та міжнародних моделей, методів та систем у сфері захисту персональних даних, їх відповідність нормативно-правовій бази України та ЄС (зокрема, GDPR), що дозволило сформулювати вимоги до систем оцінювання наслідків витоку персональних даних. Отримані результати стали основою для постановки вимог до створення нових інтегрованих теоретичних і прикладних засобів, які б дозволили: формалізовано оцінювати втрати від витоків ПД; підтримувати прийняття управлінських рішень у кризових ситуаціях; забезпечувати відповідність сучасним вимогам законодавства у сфері захисту даних.

2) розроблено алгоритмічне забезпечення, яке реалізує структурну модель системи оцінювання негативних наслідків від витоку персональних даних відповідно до положень Регламенту GDPR. Це забезпечує формалізоване обчислення максимально наближеного розміру збитків на основі комплексного аналізу чинників інциденту, включаючи рівень порушення, тип персональних даних, контекст події та рівень відповідальності підприємства.

3) створено інтегровану базу даних параметрів інцидентів та оціночних характеристик, яка дозволяє здійснювати збір, обробку, збереження та повторне використання даних для оцінювання шкоди. База даних підтримує ієрархічну структуру оцінювання за напрямами відповідності GDPR, що дозволяє швидко і надійно формувати вхідні дані для експертного аналізу.

4) розроблено прикладне програмне забезпечення, що реалізує алгоритми системи оцінювання негативних наслідків від витоку персональних даних та автоматизує процес оцінювання і дозволяє підприємствам моделювати інциденти, отримувати оцінку ймовірних штрафних санкцій, генерувати звіти у форматах DOCX та PDF, а також формувати персоналізовані рекомендації щодо підвищення інформаційної безпеки та відповідності вимогам GDPR.

Практична цінність роботи підтверджена актами впровадження в ТОВ «СІТОН ДІДЖИТАЛ» (акт від 02.06.2025 р.), ТОВ «ФЛАЙ ТЕХНОЛОДЖИ УА» (акт від 12.05.2025 р.), ТОВ «ЕН-ЛАЙН» (акт від 19.05.2025 р.). а також

відображена у звітах про науково-дослідну роботу Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»: «Прогнозування інцидентів та потенційних кризових ситуацій в інформаційній сфері» (реєстраційний номер № 70/09.01.08), «Методологія оцінювання шкоди національній безпеці України від реалізації загроз в інформаційній сфері» (реєстраційний номер № 51/18.01.01) та «Система забезпечення кібербезпеки та стійкості об’єктів критичної інфраструктури» (реєстраційний номер № 5-2024/18.02).

У дисертаційній роботі здійснено комплексне дослідження проблеми оцінювання негативних наслідків від витоку персональних даних, запропоновано нові моделі, методи та інструменти, які дозволяють формалізовано визначати рівень шкоди, прогнозувати збитки та підтримувати прийняття управлінських рішень у сфері інформаційної безпеки. Результати роботи мають значну теоретичну й практичну цінність, підтверджену впровадженням у діяльність організацій, та сприяють підвищенню ефективності управління ризиками витоку персональних даних відповідно до національного та європейського законодавства.

Ключові слова: інформаційна безпека, кібербезпека, захист інформації, захист персональних даних, Регламент GDPR, оцінювання ризиків, кіберзагрози, методи, моделі, оцінювання витоків персональних даних, системи, алгоритми.

ABSTRACT

Lozova Iryna. Models and Methods for Assessing the Negative Consequences of Personal Data Breaches. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Candidate of Technical Science in the specialty 05.13.21 «Information security systems». – State University of Information and Communication Technologies, Kyiv, 2025.

The dissertation addresses the urgent scientific problem of developing models and methods for assessing the negative consequences caused by personal data breaches to support decision-making processes aimed at minimizing risks, estimating losses, and enhancing the overall level of information security in organizations.

The scientific results and conclusions presented in the dissertation are based on the use of set-theoretic approaches, fuzzy logic theory, decision-making theory, algorithms, logic algebra, expert assessment methods, modeling of information processes and structures, and fuzzy arithmetic operations. The reliability of the obtained scientific results, conclusions, and recommendations is substantiated by the application of mathematical framework або methods або techniques and computer modeling.

The following scientific results have been obtained in the dissertation:

1. For the first time, a set-theoretic and tuple-based model of personal data parameters was developed. These models formalize the influence of various factors — such as annual data turnover, type and nature of violation, mitigation efforts, liability level, and more — as well as the composition of coefficients of importance of information resources, environment identifiers, threats, protection mechanisms, and potential losses. These models allow formalizing and modeling the influence of parameters that affect damage assessment under the GDPR and define sets of input and output parameters for formalizing the assessment process in accordance with national legislation.

2. A method for assessing the negative consequences of personal data confidentiality violations under the GDPR and a method for evaluating the security of personal data were developed. These methods rely on the constructed set-theoretic

GDPR model and analytical transformation of expert judgment sets, as well as a tuple-based model of data parameters and analytical conversion of input sets (e.g., document analysis, environment and purpose of data processing, current security mechanisms, threat identification). This allows determining both the maximum and actual cost from a data breach and provides recommendations for choosing a security policy in compliance with the GDPR and national regulations.

3. A structural model of a system for assessing the negative consequences of personal data breaches is proposed for the first time. It integrates blocks for data generation and storage, violation identification, expert data processing, and supports the development of an automated decision support system for loss assessment and minimizing financial risks.

Practical significance of the obtained results:

1. A comprehensive analysis of national and international models, methods, and systems in the field of personal data protection was carried out, in the context of their compliance with the regulatory frameworks of Ukraine and the EU (including GDPR). This served as a foundation for defining the requirements for loss assessment systems and informed the development of theoretical and practical tools to: formally assess damage from data breaches, support crisis decision-making, and ensure legal compliance.

2. Algorithmic support was developed, implementing the structural model of the assessment system in accordance with the GDPR. This enables formalized computation of likely losses based on analysis of incident factors such as breach level, data types, context, and enterprise liability.

3. An integrated database of incident parameters and assessment characteristics was created to collect, process, store, and reuse data for damage assessment. The database supports a hierarchical structure aligned with GDPR compliance directions, enabling efficient preparation of expert input.

4. Application software was developed that implements algorithms of the damage assessment system and automates the evaluation process. The software allows

organizations to simulate incidents, estimate potential penalties, generate DOCX and PDF reports, and produce personalized recommendations for improving information security and GDPR compliance.

The practical value of the dissertation is confirmed by implementation acts in «SEETON DIGITAL LLC» (act dated 02.06.2025), «FLY TECHNOLOGY UA LLC» (act dated 12.05.2025), «N-LINE LLC» (act dated 19.05.2025), as well as by reports from research projects of the State Non-Commercial Enterprise «State University «Kyiv Aviation Institute»: «Forecasting incidents and potential crisis situations in the information sphere» (registration number № 70/09.01.08), «Methodology for assessing damage to the national security of Ukraine from threats in the information sphere» (registration number № 51/18.01.01), and «Cybersecurity and resilience system for critical infrastructure objects» (registration number № 5-2024/18.02).

The dissertation presents a comprehensive study of the problem of assessing the negative consequences of personal data breaches, proposes new models, methods, and tools for formalized loss estimation and decision-making support in the field of information security. The results have significant theoretical and practical value, confirmed by implementations in organizations, and contribute to improving the management of data breach risks in accordance with national and EU legislation.

Keywords: information security, cybersecurity, data protection, personal data, GDPR regulation, risk assessment, cyber threats, methods, models, data breach assessment, systems, algorithms.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Шаховал О., Лозова І., Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. *Захист інформації*. 2016. Т. 18, № 1. С. 57–65. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_1_9

2. Гізун А., Лозова І. Аналіз дефініцій поняття кризова ситуація та основних аспектів концепції управління безперервністю бізнесу. *Безпека інформації*. 2016. Т. 22, № 1. С. 99-108. URL: http://nbuv.gov.ua/UJRN/bezin_2016_22_1_17.

3. Корченко О., Дрейс Ю., Лозова І. Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. *Захист інформації*. 2016. Т. 18, № 1. С. 39-47. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_1_7

4. Гізун А., Лозова І., Трикуш О. Застосування механізму кореляції інцидентів/потенційних кризових ситуацій для оцінювання рівня критичності поточної ситуації в інформаційній сфері. *Безпека інформації*. 2017. Т. 23, № 3. С. 215-221. URL: http://nbuv.gov.ua/UJRN/bezin_2017_23_3_10

5. О. Корченко, Ю.Дрейс, І.Лозова, Є. Педченко. Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*. 2020. Т. 22, № 2. С. 120-141. URL: https://doi.org/10.18372/2410-7840.22.14871

6. Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л., Педченко Є.М. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Захист інформації.* 2023. Т. 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232.

7. Корченко О.Г., Лозова І.Л. Структурна модель системи оцінки негативних наслідків втрати персональних даних. *Наукові записки ДУІКТ*. 2024. №2 (6). С. 165-170. URL: https://doi.org/10.31673/2786-8362.2024.028264

8. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., Balagura, D. Development of the

sociocyberphysical systems` multi-contour security methodology. *Eastern-European Journal of Enterprise Technologies*. 2024. Vol. 1, no. 9 (127). P. 34–51. (*Scopus*) URL: https://doi.org/10.15587/1729-4061.2024.298844

9. Pedchenko Y., Karpinski M., Lozova I., Kotyk O., Petrovska M. Damage assessment from the personal data loss. Problems of scientific, technical and legal support for cybersecurity in the modern world : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 34-46. DOI: 10.24917/9788668020861 URL: https://bazawiedzy.uken.krakow.pl/info/article/UKENca47634692fd430697964f5fa8af695f/

10. V. Hrebenuik , Y. Dreis, A. Hrebenuik, I. Lozova. Definitions in the field of personal data protection: a comparative analysis of the legislation of Ukraine and European Union. Technologie, procesy i systemy produkcyjne: Monografia. Tom3. Akademia Techniczno Humanistyczna w Bielsku-Bialej, 2020. pp. 141 - 146. URL: https://engineerxxi.ubb.edu.pl/fcp/eHFNIBD8dJBYXMwoXQH5hbEpmfHIGFBcNBi4oGgh0VWFeUxRUPBYvEkFWQQMOZm96Dzc1IikcFEpjZXQLC3QZ/_users/code_0DQNBBTkZMh4KLBYRAGomPA9qIDw/publikacje/2020/engineerxxi_2020_vol3_13.pdf

11. Y. Dreis, I. Lozova, A. Biskupskyi, Y. Pedchenko, Y. Ivanchenko. GDPR-model of parameters for estimating losses from loss of personal data. Przetwarzanie, transmisja i bezpieczeństwo informacji: Monografia. Tom 2. Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2019. pp. 127 - 138. URL: https://www.researchgate.net/profile/Yurii-Dreis-2/publication/387069634_GDPR-MODEL_OF_PARAMETERS_FOR_ESTIMATING_LOSSES_FROM_LOSS_OF_PERSONAL_DATA_MODEL_PARAMETROW_GDPR_DO_SZACOWANIA_STRAT_Z_UTRATY_DANYCH_OSOBOWYCH/links/675edfb7da24c8537c76497f/GDPR-MODEL-OF-PARAMETERS-FOR-ESTIMATING-LOSSES-FROM-LOSS-OF-PERSONAL-DATA-MODEL-PARAMETROW-GDPR-DO-SZACOWANIA-STRAT-Z-UTRATY-DANYCH-OSOBOWYCH.pdf

12. Комп'ютерна програма «Програмний модуль оцінки негативних наслідків від витоку персональних даних»: а. с. 96927 Україна/ Ю. Дрейс., І. Лозова, Є. Педченко. Заявл. 27.03.2020 ; опубл. 29.05.2020, Бюл. № 58. URL: https://sis.nipo.gov.ua/uk/search/detail/1625864/

13. Лозова І., Корченко О. Розробка моделі системи оцінки негативних наслідків втрати персональних даних. *ITSec: Безпека інформаційних технологій*: Матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С.124-125. URL: https://drive.google.com/file/d/1Nt2w9E-N97TAIdAGqWKbaXsqASyP-4tt/view

14. Лозова І.Л., Корченко О.Г., Котик О.В. Оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали X Міжнарод. наук.-практ. конф., Київ, 25 квітня 2024 р. / Редкол.: О. І. Тимошенко та ін. Київ: Вид-во Європейського університету, 2024. С. 74-78. URL: https://e-u.edu.ua/userfiles/files/135/2024-zbirnik_h_mizhnarodna-_konf_aktualni_pitannya_zabezpechennya_kiberbezpeki_ta_zahistu_informacii.pdf

15. Толбатов А., Лозова І., Котик О., Толбатова О. Автоматизована система вибору засобів оцінювання збитків від втрати персональних даних. IMA: 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

16. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. Analysis of modern cloud services to ensure cybersecurity. *6th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES* 2022, Vol. 207, pp. 110 - 117. (*Scopus*). URL: https://doi.org/10.1016/j.procs.2022.09.043

17. Gnatyuk, S., Berdibayev, R., Azarov, I., Baisholan, N., Lozova I. Modern Types of Databases for SIEM System Development. *CEUR Workshop*

Proceedings, 2021, 3187, pp. 127-138. (*Scopus*). URL: https://ceur-ws.org/Vol-3187/paper12.pdf

18. Корченко О.Г., Лозова І.Л., Дрейс Ю.О., Хохлачова Ю.Є. Алгоритмічне забезпечення системи оцінки негативних наслідків від втрати персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали VII міжнарод. наук.-практ. конф., 24-27 лютого 2021 р. Київ: Вид-во Європейського університету, 2021. С.40-42. URL: https://www.researchgate.net/publication/389848654_ALGORITMICNE_ZABEZPECENNA_SISTEMI_OCINKI_NEGATIVNIH_NASLIDKIV_VID_VTRATI_PERSONALNIH_DANIH

19. 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.

20. Лозова І., Педченко Є., Баланда А. Теоретико-множинне представлення параметру «Рівень порушення» для кортежної GDPR-моделі, *ITSec-2020: Безпека інформаційних технологій*: Матеріали X міжнар. наук.-техніч. конф., м. Київ, 19-24 березня 2020 року. Київ, 2020. С. 47-49.

21. Дрейс Ю., Скворцов С., Лозова І., Біскупський А. Множинна інтерпретація параметрів «Зниження шкоди» та «Ступінь відповідальності» для кортежної GDPR-моделі. *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2020)*: Матеріали 12-ої Всеукр. науково-практ. конф., м. Миколаїв, 24-26 черв. 2020 р. Миколаїв, 2020. С. 21-24. URL: https://www.researchgate.net/publication/389848384_MNOZINNA_INTERPRETACIA_PARAMETRIV_ZNIZENNA_SKODI_TA_STUPIN_VIDPOVIDALNOSTI_DLA_KORTEZNOI_GDPR-MODELI

22. Лозова І. Теоретико-множинне представлення окремих параметрів для кортежної GDPR-моделі. *Безпека ресурсів інформаційних систем*: збірник тез І Міжнародної науково-практичної конференції, м. Чернігів, 16-17 квітня 2020 р.,

Чернігів: НУЧП, 2020. С. 110-116. URL: https://stu.cn.ua/wp-content/uploads /2021/04/bris-t.pdf

23. Дрейс Ю.О., Лозова І.Л., Ковальов Д.А. Структурно-параметрична GDPR-модель оцінки негативних наслідків від витоку персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали VI міжнарод. наук.-практ. конф., 19 – 22 лютого 2020 р. Київ: Вид-во Європейського університету, 2020. – С. 39-41. URL: https://www.researchgate.net/publication/389811894_STRUKTURNO-PARAMETRICNA_GDPR-MODEL_OCINKI_NEGATIVNIH_NASLIDKIV_VID_VITOKU_PERSONALNIH_DANIH

24. Дрейс Ю.О., Лозова І.Л. Розробка GDPR-моделі параметрів оцінювання наслідків витоку персональних даних. *Комп'ютерні технології: інновації, проблеми, рішення*: Матеріали II Всеукраїнської науково-технічної конференції, м. Житомир, 14-15 листопада 2019 р. Житомир, Житомирська політехніка, 2019. С. 78-79. URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/tezy-dopovidej-kt2019_os.pdf

25. Дрейс Ю.О., Лозова І.Л., Педченко Є.М. Оцінювання негативних наслідків від витоку персональних даних. *ITSec: Безпека інформаційних технологій*: Матеріали IX міжнародної науково-технічної конференції, м. Київ, 22-27 березня 2019 р. Київ, 2019. С.41-42.

26. Дрейс Ю.О., Лозова І.Л. Формування параметрів оцінювання негативних наслідків витоку персональних даних в автоматизованих системах. *ITSec: Безпека інформаційних технологій*: Матеріали VIII міжнародної науково-технічної конференції, м.Київ,16-18 травня 2018 р. Київ, 2018. С.14-15.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІТ	–	Інформаційні технології
АС	–	Автоматизована система
GDPR	–	Загальний регламент захисту даних
ПД	–	Персональні дані
БПД	–	База персональних даних
ПЗ	–	Програмне забезпечення
ЗІ	–	Захист інформації
СЗІ	–	Система захисту інформації
ТЗІ	–	Технічний захист інформації
КСЗІ	–	Комплексна система захисту інформації
СМІБ	–	Система менеджменту інформаційної безпеки
ІПКС	–	Інцидент / Потенційна кризова ситуація
СКФС	–	Соціокіберфізичні системи
SaaS	–	Програмне забезпечення як послуга
PaaS	–	Платформа як послуга
IaaS	–	Інфраструктура як послуга
IDS/IPS	–	Система виявлення / запобігання вторгнень
CERT	–	Команда реагування на комп’ютерні інциденти
PDCA	–	Цикл планування, виконання, перевірки, дій
DPIA	–	Оцінка впливу на захист даних
DPO	–	Уповноважений із захисту даних
DPA	–	Орган із захисту даних
EDPB	–	Європейська рада із захисту даних
NIST	–	Національний інститут стандартів і технологій США
ISO	–	Міжнародна організація зі стандартизації
SSL/TLS	–	Протоколи захищеного передавання даних

ВСТУП

Актуальність. У сучасних умовах стрімкого розвитку цифрових технологій, зростання кількості онлайн-сервісів та обсягу оброблюваних персональних даних, проблема забезпечення конфіденційності та безпеки персональної інформації набуває особливої актуальності. Витоки персональних даних спричиняють не лише порушення прав і свобод людини, а й значні фінансові та репутаційні втрати для організацій, а в окремих випадках – загрозу національній безпеці.

Згідно з міжнародними стандартами, зокрема Регламентом ЄС GDPR, а також законодавством України (Закони «Про захист персональних даних», «Про інформацію» тощо), власники і розпорядники персональних даних зобов’язані впроваджувати ефективні механізми виявлення інцидентів, оцінки шкоди та інформування постраждалих сторін. Однак на практиці залишається недостатньо формалізованих, адаптивних, масштабованих моделей та методів оцінки збитків, що виникають унаслідок витоку персональних даних. Особливо гостро ця проблема стоїть для державних інформаційних систем, об'єктів критичної інфраструктури, банківського, медичного та освітнього секторів, де витік даних може мати системні наслідки. Сучасні підходи часто не враховують множинність інцидентів, їх взаємозалежність, динамічний характер ризиків і необхідність оперативної реакції.

Водночас, зростає потреба в автоматизованих інструментах підтримки прийняття рішень, які здатні не лише фіксувати факт витоку, а й обчислювати рівень завданої шкоди – як у кількісному (фінансовому), так і в якісному (репутаційному, юридичному) вимірах. Це вимагає побудови науково обґрунтованих моделей, які враховують правові, технічні, організаційні та соціальні аспекти функціонування інформаційних систем.

Таким чином, розробка та вдосконалення моделей і методів оцінювання негативних наслідків від витоку персональних даних є актуальним науковим і

практичним завданням, вирішення якого сприятиме підвищенню стійкості організацій до кіберзагроз, зниженню економічних втрат та зміцненню інформаційної безпеки в державі загалом.

Серед вітчизняних науковців, які розглядали проблематику захисту персональних даних, можна відзначити роботи Брижка В.М., Різака М.В., Дрейса Ю.О., Дяковського О.С., Чернобая А.М. та інших. Проте, незважаючи на значні досягнення в цій галузі, переважна більшість наукових досліджень присвячена переважно правовим аспектам забезпечення конфіденційності персональних даних, тоді як технічні механізми захисту, а також методи оцінювання наслідків інцидентів, пов’язаних із витоком інформації, залишаються недостатньо опрацьованими та потребують подальшого наукового опрацювання.

Аналіз наукових досліджень показав, що для оцінювання негативних наслідків втрати персональних даних застосовуються різноманітні методи, моделі та системи. Але ці методи, мають певні недоліки, а саме вони або не охоплюють усіх аспектів негативних наслідків витоку персональних даних, або не адаптовані до вимог GDPR. Більшість підходів мають якісний або змішаний характер, здебільшого оперують експертними оцінками, анкетами чи сценаріями без кількісної грошової оцінки, що ускладнює обґрунтування реальних фінансових наслідків для бізнесу. Тільки деякі моделі та методи оцінюють фінансові втрати безпосередньо та дозволяють здійснювати кількісну оцінку наслідків у грошовому вираженні, що є критично важливим для стратегічного планування та прийняття управлінських рішень. Переважна частина систем вимагає суттєвих ресурсів на впровадження або дорогих інструментів, що обмежує їхнє застосування для малих та середніх підприємств. Деякі моделі та методи орієнтовані виключно на технічну або IT-безпеку без правового контексту, що робить їх недостатніми для комплексної оцінки юридичних наслідків витоків персональних даних.

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.

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи впроваджено в науково-дослідну роботу Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»: «Прогнозування інцидентів та потенційних кризових ситуацій в інформаційній сфері» (реєстраційний номер № 70/09.01.08), «Методологія оцінювання шкоди національній безпеці України від реалізації загроз в інформаційній сфері» (реєстраційний номер № 51/18.01.01) та «Система забезпечення кібербезпеки та стійкості об’єктів критичної інфраструктури» (реєстраційний номер № 5-2024/18.02).

Метою дисертаційної роботи є розробка моделей та методів оцінювання негативних наслідків, спричинених витоком персональних даних для подальшої підтримки процесу прийняття рішень щодо мінімізації ризиків, оцінювання втрат та підвищення загального рівня інформаційної безпеки організацій.

Відповідно до мети необхідно вирішити наступні **задачі:**

– проаналізувати сучасне вітчизняне та міжнародне нормативно-правове забезпечення у сфері захисту персональних даних, а також існуючі методи, моделі та системи оцінювання можливих негативних наслідків їх витоку чи втрати.

– розробити моделі інтегрованого представлення параметрів збитків, спричинених витоком персональних даних, відповідно до вимог чинного українського законодавства та положень Регламенту ЄС GDPR.

– розробити методи оцінювання безпеки персональних даних на основі кортежної моделі відповідно до вимог українського законодавства та механізмів розрахунку негативних наслідків на основі теоретико-множинної GDPR-моделі параметрів персональних даних.

– розробити структурну модель системи оцінювання негативних наслідків від витоку персональних даних, що відповідає принципам і положенням

Регламенту GDPR, та забезпечує врахування юридичних, технічних і організаційних чинників.

– розробити алгоритмічне та програмне забезпечення реалізації структурної моделі системи оцінювання негативних наслідків від витоку персональних даних для автоматизації відповідного процесу оцінювання, а також провести експериментальне дослідження з метою підтвердження достовірності теоретичних розробок і практичної ефективності запропонованих рішень.

Об’єкт дослідження – процес оцінювання негативних наслідків від витоку персональних даних.

Предмет дослідження – методи, моделі та системи оцінювання негативних наслідків (збитків) від витоку персональних даних.

Методи досліджень базуються на теоретико-множинному підході, теоріях нечіткої логіки, прийняття рішень, алгоритмів, алгебри логіки, методах експертного оцінювання, моделювання інформаційних процесів і структур та операціях нечіткої арифметики.

Наукова новизна отриманих результатів. У процесі теоретичних досліджень і моделювання, у дисертаційній роботі отримані наступні наукові результати:

– вперше розроблено теоретико-множинну та кортежну моделі параметрів персональних даних, в яких відповідно за рахунок формалізації множини показників річного обігу, рівня, специфіки та характеру порушення, зниження шкоди, ступеню відповідальності тощо та композиції коефіцієнтів важливості інформаційних ресурсів, ідентифікаторів середовища обробки та загроз, характеристик механізмів захисту, функціональних профілів безпеки і величини можливих збитків, дозволило відповідно формалізувати і моделювати вплив кожного із параметрів, що впливають на оцінювання збитку відповідно до Регламенту GDPR та визначити множини вхідних та вихідних параметрів для формалізації процесу оцінювання шкоди від витоку персональних даних з урахуванням національного нормативно-правового забезпечення;

– вперше розроблено метод оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR та метод оцінювання безпеки персональних даних, в яких відповідно за рахунок побудованої теоретико-множинної GDPR-моделі параметрів та реалізації аналітичного перетворення множин величин, що відображають судження експертів, розроблених нових правил оцінювання, розсіювання балів і визначеної множини рекомендацій та за рахунок побудованої кортежної моделі параметрів персональних даних та аналітичного перетворення множин вхідних даних (аналіз документів, середовища та мети обробки персональних даних, аналіз функціонуючих механізмів безпеки, ідентифікація можливих загроз захисту персональних даних тощо), дозволило відповідно визначати величину максимального та фактичного збитків для організації у разі витоку персональних даних і надавати рекомендації щодо вибору політики їх безпеки відповідно до положень Регламенту GDPR та дозволило надавати рекомендації щодо вибору політики безпеки персональних даних і послуг безпеки та визначати величину можливої шкоди у разі витоку таких персональних даних з урахуванням національного нормативно-правового забезпечення;

– вперше запропоновано структурну модель системи оцінювання негативних наслідків від витоку персональних даних, що за рахунок використання методу оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR та 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.

Практичне значення одержаних результатів.

– здійснено комплексний аналіз вітчизняних та міжнародних моделей, методів та систем у сфері захисту персональних даних, їх відповідність

нормативно-правовій бази України та ЄС (зокрема, GDPR), що дозволило сформулювати вимоги до систем оцінювання наслідків витоку персональних даних. Отримані результати стали основою для постановки вимог до створення нових інтегрованих теоретичних і прикладних засобів, які б дозволили: формалізовано оцінювати втрати від витоків ПД; підтримувати прийняття управлінських рішень у кризових ситуаціях; забезпечувати відповідність сучасним вимогам законодавства у сфері захисту даних.

– розроблено алгоритмічне забезпечення, яке реалізує структурну модель системи оцінювання негативних наслідків від витоку персональних даних відповідно до положень Регламенту GDPR. Це забезпечує формалізоване обчислення максимально наближеного розміру збитків на основі комплексного аналізу чинників інциденту, включаючи рівень порушення, тип персональних даних, контекст події та рівень відповідальності підприємства.

– створено інтегровану базу даних параметрів інцидентів та оціночних характеристик, яка дозволяє здійснювати збір, обробку, збереження та повторне використання даних для оцінювання шкоди. База даних підтримує ієрархічну структуру оцінювання за напрямами відповідності GDPR, що дозволяє швидко і надійно формувати вхідні дані для експертного аналізу.

– розроблено прикладне програмне забезпечення, що реалізує алгоритми системи оцінювання негативних наслідків від витоку персональних даних та автоматизує процес оцінювання і дозволяє підприємствам моделювати інциденти, отримувати оцінку ймовірних штрафних санкцій, генерувати звіти у форматах DOCX та PDF, а також формувати персоналізовані рекомендації щодо підвищення інформаційної безпеки та відповідності вимогам GDPR.

Практична цінність роботи підтверджена актами впровадження в ТОВ «СІТОН ДІДЖИТАЛ» (акт від 02.06.2025 р.), ТОВ «ФЛАЙ ТЕХНОЛОДЖИ УА» (акт від 12.05.2025 р.), ТОВ «ЕН-ЛАЙН» (акт від 19.05.2025 р.).

Особистий внесок здобувача. Усі наукові результати дисертації одержано автором самостійно. У друкованих працях, опублікованих у співавторстві, йому

належить наступне: [1] – дослідження та порівняльний аналіз стратегій кібербезпеки, розробка рекомендацій щодо удосконалення нормативно-правової бази; в [2] – аналіз поняття «кризова ситуація», формування підходів до класифікації кризових ситуацій; в [3] – розробка етапів моделі та обрахунок методу; в [4] – формалізація механізму кореляції інцидентів, розробка підходу до визначення рівня критичності кризової ситуації; в [5, 11, 23, 24] – розробка теоретико-множинної GDPR-моделі, опис структури параметрів персональних даних; [6, 9, 14] – розробка основних етапів методу оцінювання негативних наслідків від порушення конфіденційності персональних даних; [7, 13] – розробка структури моделі системи оцінки негативних наслідків втрати персональних даних, визначення її основних компонентів; [8] – розробка етапу 5, модифікація механізмів послуг безпеки в багатоконтурній системі захисту інформації (інтеграція постквантових алгоритмів); [10] – аналіз та узагальнення чинних нормативно-правових документів України та ЄС у сфері захисту персональних даних; [12, 18] – розробка алгоритмічного забезпечення системи оцінки негативних наслідків втрати персональних даних; [15] – визначення множини ознак для оцінки засобів оцінювання збитків від втрати персональних даних; [16] – дослідження та порівняльний аналіз архітектур хмарних сервісів; [17] – дослідження та аналіз існуючих типів сучасних баз даних і систем їх управління; [19] – аналіз засобів оцінювання шкоди від втрати інформації з обмеженим доступом; [20] – формулювання параметру «Рівень порушення», опис його множинного представлення; [21] – обґрунтування логічного підходу до представлення параметрів; [22] – представлення параметрів «Специфіка порушення» та «Характер порушення» з використанням теоретико-множинних підходів; [25] – розробка програмної моделі оцінки негативних наслідків від витоку персональних даних; [26] – визначення вхідних та вихідних параметрів моделі оцінювання негативних наслідків витоку персональних даних..

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на XIV Міжнародній науково-технічній конференції ITSec: Безпека інформаційних технологій, м. Тернопіль, 22-24 травня

2025 р.; X Міжнародній науково-практичній конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», м.Київ, 25 квітня 2024 р.; 6th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES 2022, м.Краків, Польща; VII Міжнародній науково-практичній конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації» 24–27 лютого 2021 р.; X міжнародній науково-технічній конференції «ITSec-2020: Безпека інформаційних технологій» м. Київ, 19-24 березня 2020 р.; I Міжнародній науково-практичній конференції «Безпека ресурсів інформаційних систем» м. Чернігів 16-17 квітня 2020 р.; II Всеукраїнській науково-технічній конференції «Комп'ютерні технології: інновації, проблеми, рішення» м. Житомир 14-15 листопада 2019 р.; IX міжнародній науково-технічній конференції «ITSec: Безпека інформаційних технологій», м. Київ, 22-27 березня 2019 р.

Публікації. Результати дисертації опубліковано в 26 наукових працях. Опубліковано статей – 8 [1 – 8], з яких 7 статей [1 – 7] – у наукових фахових виданнях України з Переліку, затвердженого МОН України, 1 стаття у наукових виданнях Scopus [8], три колективні монографії [9 – 11], авторське свідоцтво на комп'ютерну програму [12]. За матеріалами виступів на науково-технічних та науково-практичних конференціях опубліковано 14 публікацій [13 – 26], серед яких дві публікації [16, 17] проіндексовано в наукометричній базі Scopus.

Структура дисертації та її обсяг. Дисертаційна робота складається зі вступу, 4 розділів, висновків, списку використаних джерел (113 найменувань на 15 сторінках), 4 додатків (на 19 сторінках). Основний текст роботи викладено на 171 сторінці, рисунків – 32, таблиць – 15. Загальний обсяг роботи становить 205 сторінок.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МОДЕЛЕЙ ТА МЕТОДІВ ОЦІНКИ НЕГАТИВНИХ НАСЛІДКІВ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Базові поняття та визначення

Захист персональних даних (ПД) у цифрову епоху набуває статусу критичного елементу не лише інформаційної безпеки, але й забезпечення прав людини. В умовах стрімкого розвитку інформаційних технологій персональні дані стали як цінним ресурсом, так і джерелом значних ризиків у разі витоку або неправомірної обробки. Саме тому нормативно-правове регулювання, термінологічна чіткість і наукове осмислення категоріального апарату цієї сфери є ключовими передумовами ефективного забезпечення конфіденційності ПД.

Сьогодні можна стверджувати, що інформація – це гроші. Особливу увагу варто звертати на інформацію, яка знаходиться в інформаційних системах, онлайн-базах даних, інформаційних ресурсах різних рівнів. Згідно [1-4] та розуміння необхідності створення умов для забезпечення кібербезпеки і кіберзахисту держави, приведемо ситуації в закордонних установах, які не були готові до хакерських атак, внаслідок чого понесли великі втрати даних, а, отже, і матеріальні: Scottrade – викрадено детальну інформацію про 4,6 млн клієнтів; Excellus BlueCross BlueShield – витік більш ніж 10 млн записів, які включали в себе імена, дати народження, номери соціального страхування і поштові адреси, а також деякі фінансові рахунки; Carphone Warehouse – викрадено особисті дані близько 2,4 млн клієнтів (4% населення), а також їх зашифровані дані кредитних карток; аптечна мережа CVS – втрата даних кредитних карток, адрес електронної пошти та поштових адрес, номерів телефонів і паролів невідомої кількості клієнтів; UCLA Health – втрата 4,5 млн записів, які включають номери соціального страхування, і навіть медичних даних клієнтів; U.S Office of Personnel Management – отримано доступ до конфіденційної інформації; Anthem – страхова компанія втратила більше 80 мільйонів записів про клієнтів від номерів соціального страхування до конфіденційної інформації; Donald Trump’s hotel – крадіжка даних

кредитних карт (в тому числі коди і номери карт) в готелях фірми по всій території США; компанія Adobe зазнала кібератаки, внаслідок якої були викрадені дані понад 38 мільйонів користувачів, а також частина вихідного коду програмного забезпечення; через програмне забезпечення M.E.Doc було поширено вірус Petya (також відомий як NotPetya), вражено понад 1 500 українських компаній, включаючи банки, енергетичні компанії та державні установи, вірус спричинив масові втрати даних, зокрема персональних, та значні фінансові збитки.

Також, у контексті цифрової трансформації, коли дедалі більше бізнес-процесів переноситься в хмарні середовища, забезпечення конфіденційності персональних даних стає критично важливим завданням. Сучасні хмарні сервіси не лише забезпечують масштабовану інфраструктуру та зниження витрат на IT, але й виступають ключовим інструментом у системі захисту персональних даних, особливо з урахуванням вимог GDPR.

В дослідженні [5] проведено аналіз найпопулярніших хмарних платформ – Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, IBM Cloud та Alibaba Cloud – з позиції функціональності та кіберзахисту. Однією з центральних функцій, яку було проаналізовано, є DLP (Data Loss/Leak Prevention) – технологія, що прямо відповідає за запобігання витоку персональних даних під час їх обробки та зберігання в хмарі.

Таким чином, хмарні сервіси виступають: платформами для автоматизованої обробки персональних даних (через моделі SaaS, PaaS, IaaS); засобами для шифрування, резервного копіювання, та сегментації доступу до ПД; середовищем, де впроваджуються політики відповідності до GDPR, у тому числі через інструменти IAM, логування, моніторинг та ізоляцію середовищ.

Як відзначено в дослідженні [6], системи управління кризами, інцидентами інформаційної безпеки та інші захисні системи (IDS/IPS, антивіруси, CERT) тісно пов’язані з системами захисту персональних даних. Кризові ситуації в кіберпросторі часто спричинені витоком ПД, тому необхідне чітке визначення понять, які регулюють дії в таких обставинах.

Крім того, управління ризиками витоку персональних даних повинне бути частиною системи менеджменту інформаційної безпеки, яка базується на циклі PDCA (планування, реалізація, контроль, удосконалення).

Персональні дані – це одна з ключових категорій у сфері інформаційного права, що визначає правила обробки, захисту та використання інформації про фізичних осіб [7]. Нижче наведено визначення поняття персональних даних із різних нормативно-правових актів.

Відповідно до Закону України «Про захист персональних даних» [8] персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Цей закон є основним нормативним актом, що регулює правові аспекти збору, обробки, зберігання та захисту персональних даних в Україні.

Ключові терміни законодавства: суб’єкт персональних даних – фізична особа, персональні дані якої обробляються; володілець персональних даних – фізична або юридична особа, яка визначає мету обробки ПД; розпорядник персональних даних – особа, що здійснює обробку від імені володільця; обробка персональних даних – будь-які дії з ПД: збирання, накопичення, зберігання, знищення, розкриття тощо. Ці терміни формують правову основу регулювання персональних даних в Україні та відповідають нормам GDPR, Регламенту ЄС 2016/679.

В Конституції України (стаття 32) [9] не використовується термін «персональні дані», але закріплюються основоположні права людини на недоторканність особистого життя, зокрема заборону збору, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом.

В Законі України «Про інформацію» [10] (стаття 11) поняття персональних даних розглядається в контексті інформації про фізичну особу: персональні дані — це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. До конфіденційної інформації про

фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Українське законодавство поступово адаптується до норм ЄС, включаючи GDPR. Хоча це не є український нормативний акт, регламент має вплив на правове регулювання персональних даних в Україні. Відповідно до Регламенту GDPR [11]: «персональні дані» означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

Усі нормативно-правові акти підкреслюють, що персональні дані повинні дозволяти ідентифікацію особи (пряму чи опосередковану). Різні країни мають розширені категорії персональних даних, наприклад, США та ЄС додають до цього інтернет-ідентифікатори, дані про місцезнаходження, біометрію. Українське законодавство має гармонізовану базу з нормами ЄС через регуляції GDPR.

1.2. Нормативно-правове забезпечення захисту персональних даних

Гармонізація українського законодавства з європейськими стандартами стає одним із ключових завдань реформування галузі. Синхронізація правил дозволить підвищити довіру до обігу даних та зменшити правову фрагментацію (як очікується після повної адаптації GDPR). Разом з тим масштабування цифрових даних вимагає від фахівців розробити єдину методологічну основу для оцінювання реальної ефективності норм захисту інформації [12]. У зв’язку з цим актуальність дослідження обумовлена необхідністю всебічного аналізу й

порівняння правових моделей різних країн задля створення узагальненої методики оцінки дієвості заходів із захисту персональних даних.

Законодавча база України. Конституція України (ст.32) [9] закріплює право на таємницю особистого життя: збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди заборонено. Вона гарантує кожному судовий захист права на спростування недостовірної інформації про себе і відшкодування збитків. Ця стаття є основою всього подальшого законодавства про захист персональних даних, вимагаючи згоди на обробку і забезпечення гідності людини. Поряд з нею варто також зазначити ст.31 Конституції про таємницю кореспонденції і ст.34 про свободу слова, які уможливлюють обмін інформацією, але з дотриманням норм конфіденційності. У цілому Конституція встановлює принципи приватності та балансу між правом на інформацію й захистом особистих даних [13].

Закон України «Про захист персональних даних» [8] є ключовим актом, що безпосередньо регулює захист персональних даних під час їх обробки. Суб'єкти даних мають права на доступ до своїх даних, їх оновлення чи видалення, заперечення проти обробки, відкликання згоди. Контролери (володільці баз даних) зобов'язані отримувати згоду на обробку, вчасно реєструватися в Державному реєстрі баз персональних даних, забезпечувати технічний та організаційний захист даних і повідомляти Уповноваженого ВР про порушення безпеки. За порушення передбачено адміністративні штрафи (ст. 188-39 КУпАП), у разі тяжких злочинів – кримінальну відповідальність (ст. 182 КК України) [14].

Закон України «Про доступ до публічної інформації» [15] декларує загальне право на доступ громадян до публічної інформації, включно з відомостями про себе. Він встановлює процедуру отримання інформації від органів влади, але при цьому обмежує доступ до персональних даних третіх осіб без їх згоди. Цей закон передбачає відповідальність посадовців за несвоєчасне або неправомірне надання інформації (штрафи до декількох тисяч гривень за ст. 212-3 КУпАП). Згоди суб'єкта даних як такої цей закон не вимагає, окрім загальних випадків,

передбачених Законом «Про захист персональних даних» або іншими актами [16].

Закон України «Про інформацію» [10] закріплює право кожного на доступ до інформації про себе та свободу отримувати інформацію. Стаття 11 прямо забороняє збір і використання конфіденційної інформації (включаючи національність, освіту, здоров'я, адресу тощо) без згоди особи. Санкції за порушення Закону – адміністративна відповідальність за незахищені витоки інформації (ст. 182-39 КпАП), а за окремі випадки – ще й кримінальна (як «Порушення недоторканності приватного життя» ст. 182 КК).

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [17] регулює відносини у сфері електронних ідентифікаційних даних та довірчих послуг (електронні підписи, печатки, електронні часи та ін.). Він створює правові механізми захисту електронних ідентифікаційних даних (зокрема збереження ПІБ, паспортних даних у системі єдиного демографічного реєстру) та вимоги до провайдерів довірчих послуг. Закон зобов'язує організації впроваджувати безпечні технологічні рішення, проводити сертифікацію довірчих постачальників і призначати відповідальних осіб. За порушення вимог (наприклад, ненадання звітів, відсутність захисту даних) передбачені санкції: штрафи або анулювання атестата довірчого постачальника. Цей Закон підсилює захист ПД у цифровому обігу (обов'язок автентифікації через Єдиний державний реєстр – ЄВІД, шифрування тощо).

Законодавча база Європейського Союзу. Регламент (ЄС) 2016/679. «Загальний регламент захисту даних» [11] – основний закон ЄС з ПД. Він встановлює єдині правила обробки персональних даних у всіх країнах ЄС. GDPR поширюється на будь-яку організацію, що обробляє персональні дані громадян ЄС (навіть за кордоном). Права суб'єкта даних по GDPR дуже широкі: доступ до своїх даних, їх виправлення, видалення («право бути забутим»), обмеження обробки, перенесення даних у інший формат, заперечення проти обробки (або проти прямих маркетингових контактів). Регламент також гарантує право особи на відшкодування збитків. Зобов'язання контролерів: вони мають чітко

повідомляти про мету обробки, законні підстави (зокрема – згоди), зберігати мінімум даних, забезпечувати їхню безпеку (шифрування, регулярний аудит). При потребі – проводити DPIA (оцінку впливу на приватність) і призначати DPO. У разі порушення безпеки – обов'язок повідомити національний орган (Data Protection Authority) не пізніше ніж за 72 години. Наглядовий орган – національний DPA (у т.ч. єдиний Європейський департамент захисту даних), який може перевіряти та накладати санкції. Санкції: регламент задає суворий штраф – до 20 млн € або 4% світового обороту підприємства (вищу суму). GDPR стосується обох секторів (приватний, публічний), включає екстериторіальну дію (для компаній за межами ЄС, якщо вони обробляють дані громадян ЄС) [18-19].

Директива 2002/58/ЕС «Конфіденційність у сфері електронних комунікацій» (ePrivacy) [20]. Цей акт доповнює GDPR у сфері онлайн- і телекомунікацій. Він охоплює телекомунікаційні мережі та інтернет-послуги, регулюючи захист конфіденційності мережевого трафіку і використання "cookies" та подібних технологій. Права суб'єктів – це насамперед право на недоторканність комунікацій (заборона перехоплення, прослуховування без згоди) та захист «трафік-даних» (оператор не повинен зберігати їх довше, ніж потрібно). Обов'язки контролерів (провайдерів): забезпечувати технічну безпеку мережевих послуг, інформувати користувачів про значні ризики (віруси тощо), отримувати згоду користувача на встановлення cookie (яка виходить за рамки GDPR згоди). Санкції: встановлюються національними законами (часто передбачають великі штрафи для порушників privacy-практик провайдерів). Директива охоплює сектор зв'язку (телефони, інтернет) і поширює правило «конфіденційність за замовчуванням».

Директива 2016/680 (Law Enforcement Directive, ЄС) [21] регулює обробку персональних даних органами правопорядку (поліція, прокуратура, суди) з метою запобігання і розслідування злочинів. На відміну від GDPR, вона поширюється виключно на дані, пов'язані зі злочинною діяльністю (потенційні підозрювані, засуджені, жертви тощо). Права суб'єктів за LED включають право бути

поінформованими (ім’я контролера, мета обробки, право на скаргу), право доступу до своїх даних, виправлення, видалення або обмеження обробки. Санкції: директива вимагає, щоб країни-члени ввели адміністративну чи кримінальну відповідальність за порушення (в ЄС зазвичай це штрафи або дисциплінарні стягнення за національним законодавством) [22].

Законодавча база США. Privacy Act of 1974 (U.S.) [23] – федеральний закон, що регулює збір та обіг персональних даних у державних інформаційних системах США. Він вимагає від урядових відомств вести системи записів про осіб (systems of records) і публікувати їх опис у «Federal Register». Права суб’єкта: будь-який громадянин або постійний мешканець США має право отримати копії своїх записів, вимагати виправлення неточностей. Зобов’язання контролерів (урядові установи): збирати дані лише за законною метою, повідомляти особу про мету збору, не розголошувати записи без згоди (з 12 виключеннями, наприклад, правоохоронні запити). Санкції: за неправомірне розголошення – дисциплінарні санкції, адміністративні штрафи, а за вчинення злочину (порушення закону) – кримінальна відповідальність. Витоки даних регулюються загальними положеннями закону – наприклад, розголошення без згоди суворо заборонене.

Health Insurance Portability and Accountability Act (HIPAA, 1996) [24] – федеральний закон про захист медичної інформації. Його Privacy Rule передбачає захист всіх «індивідуально ідентифікованих медичних даних» (Protected Health Information – PHI), які належать до пацієнтів. Обов’язки контролерів: впроваджувати технічні та адміністративні заходи захисту PHI (шифрування, контроль доступу), а також інформувати пацієнтів про свої практики приватності (публікуючи «Notice of Privacy Practices»). Передбачено суворі обмеження на розкриття даних про пацієнта без його згоди (окрім випадків лікування, виставлення рахунків тощо). Санкції: штрафи до $50 000 за інцидент (максимум $1,5 млн на рік для одного типу порушення), можливе кримінальне переслідування за злісне порушення. Діє на приватні й державні медичні установи.

Children’s Online Privacy Protection Act (COPPA, 1998) [25] – закон про захист персональних даних дітей. Права: дає батькам контроль над тим, які дані про дітей до 13 років збирають онлайн-сервіси. Обов’язки контролерів (операторів сайтів/додатків для дітей): перед збором будь-якої «особисто ідентифікованої інформації» від дитини необхідно отримати перевірену згоду батьків (verifiable parental consent). Оператори мають публікувати чіткі політики приватності та лише збирати мінімум даних для роботи сервісу. Нагляд: Федеральна комісія зі зв’язку (FTC). Санкції: за порушення закону – штрафи до $50 000 за інцидент.

Законодавча база Канади. PIPEDA (Personal Information Protection and Electronic Documents Act, 2000) [26] – федеральний закон Канади. Він поширюється на всі приватні компанії і неурядові організації, що здійснюють комерційну діяльність у Канаді. Права суб’єктів: доступ до власних записів, право виправити неточні дані, право знати, як використовується інформація. Обов’язки контролерів (бізнесів): забезпечити конфіденційність даних, повідомляти клієнтів про ціль збору та використання інформації, обмежувати збір мінімально необхідним обсягом, а також отримувати згоду (зазвичай неявну або явну) перед обробкою. Працівники, що керують персональною інформацією, мають проводити політики безпеки, шифрувати дані, інформувати про обробку. Санкції: бізнеси можуть бути притягнені до адміністративних штрафів (до C$100 000 при внесенні злочину) або до договору виплати відшкодування.

Privacy Act (Канада, 1983) [27] – федеральний закон про захист особистих даних громадян, якими оперує уряд Канади. Він подібний до Privacy Act США: встановлює правила, за якими державні установи збирають, використовують, розкривають і зберігають ПД громадян. Права: громадянин або постійний житель має право отримати копію своїх даних в державних реєстрах і вимагати виправлення помилок. Санкції: за зловживання інформацією – дисциплінарні заходи проти держслужбовців, адміністративні штрафи, кримінальна відповідальність за незаконне розголошення.

Отже, для забезпечення ефективного захисту персональних даних у глобальному масштабі, різні країни розробили нормативно-правові акти, які визначають права суб'єктів даних, зобов'язання контролерів, компетенції наглядових органів, а також санкції за порушення та умови повідомлення про витік. На основі проведеного аналізу [28-32] сформуємо порівняльну таблицю міжнародного та національного законодавства щодо захисту персональних даних (табл.1.1).

Таблиця 1.1

Порівняльний аналіз міжнародного та національного законодавства щодо захисту персональних даних

Аспект	Україна (Закон про захист персональних даних)	ЄС (GDPR)	США (CPRA, HIPAA, інші)	Канада (PIPEDA)
1	2	3	4	5
1. Визначення персональних даних	Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована	Детально визначено: будь-яка інформація про ідентифіковану особу (включаючи онлайн-ідентифікатори, IP, біометрію)	Різниться в залежності від акту: імена, адреси, SSN, біометрія, але немає єдиного дефінітивного визначення	Особиста інформація: будь-які дані, які дозволяють ідентифікувати особу
2. Категорії чутливих даних	Чутливі персональні дані (расова належність, політичні погляди, релігія, здоров'я, статеве життя)	Розширений перелік special categories: етнічне походження, біометрія, генетичні, політичні, релігійні дані тощо	Чутливі дані регулюються галузевими актами (HIPAA – здоров'я, GLBA – фінанси), в єдиному законі – неповно	Чутлива інформація визначена, але перелік обмежений (здоров'я, фінанси, расова належність)
3. Правові підстави для обробки	Згода суб'єкта, виконання договору, законодавча вимога, захист інтересів	Чіткі правові підстави (згода, контракт, правові зобов'язання, життєво важливі інтереси, суспільний інтерес, законні інтереси)	В основному – згода або спеціальні галузеві винятки	Згода основна, можливі винятки для договірних зобов'язань або законних цілей

Продовження таблиці 1.1

1	2	3	4	5
4. Права суб'єкта даних	Право доступу, виправлення, блокування, видалення	Повний набір прав: доступ, виправлення, стирання, обмеження обробки, заперечення	Обмежені права, залежно від галузі (HIPAA – медичні дані, CCPA – обмежене право на стирання)	Доступ, виправлення, обмежене право видалення, відгук згоди
5. Повідомлення про порушення	Вимога повідомляти регулятора та суб'єктів даних у випадку значної шкоди	Обов'язкове повідомлення протягом 72 годин регулятору, якщо є ризик прав суб'єктів	Залежить від штату (наприклад, Каліфорнія – обов'язково), для HIPAA – 60 днів	Вимога повідомляти про серйозні інциденти в залежності від масштабу
6. Оцінка впливу (DPIA)	Вимоги відсутні (немає терміну DPIA)	DPIA обов'язкова для ризикованих обробок	Відсутня єдина вимога DPIA, інколи вимагається галузевими актами	Вимога формального DPIA відсутня
7. Принципи обробки даних	Законність, справедливість, пропорційність, відповідальність	Законність, справедливість, прозорість, мінімізація даних, обмеження зберігання, цілісність, конфіденційність	Варіюються, здебільшого в рамках "розумних заходів безпеки" та "мінімізації збору"	Схожі до GDPR: ідентифіковані цілі, мінімізація збору, безпека
8. Відповідальність (Accountability)	Визначення володільця та розпорядника, реєстрація баз даних	Високий рівень відповідальності: ведення реєстрів обробки, DPO, демонстрація відповідності	Прямий обов'язок відповідальності рідко зафіксований, здебільшого регулюється через штрафи	Обов'язок демонструвати дотримання принципів захисту даних
9. Передача даних за кордон	Можлива за умови забезпечення адекватного рівня захисту	Чіткі механізми: адекватність, стандартні договірні положення, BCR	Відсутня єдина система, кожен акт (наприклад, Privacy Shield для ЄС-США, що скасований)	Передача дозволена, якщо забезпечується адекватний рівень захисту
10. Штрафи та санкції	Штрафи визначені, але менші за європейські, не перевищують 17 тис. грн.	До 20 млн євро або 4% глобального обороту	Різняться: CCPA – до 7.5 тис. дол., HIPAA – до 1.5 млн дол.	До 100 тис. канадських дол. за серйозні порушення

Аналіз таких актів, як GDPR (ЄС), HIPAA та Privacy Act (США), PIPEDA (Канада), а також національних законів України (наприклад, ЗУ «Про захист персональних даних») свідчить про суттєві відмінності у сфері екстериторіальності, механізмах отримання згоди, вимогах до обробки, інформування про інциденти та масштабі санкцій. Європейський підхід (GDPR) характеризується високим рівнем деталізації, екстериторіальним ефектом і жорсткими фінансовими штрафами, тоді як, наприклад, закони США є більш фрагментованими за галузевим принципом (медицина, діти, урядові дані). Канадське законодавство, натомість, надає значну автономію провінціям, хоча й забезпечує федеральний нагляд за дотриманням конфіденційності в приватному секторі. Українська нормативна база наближається до європейських стандартів, однак потребує подальшої гармонізації – зокрема, впровадження обов'язкової DPIA, призначення DPO та забезпечення належної екстериторіальної дії. Порівняння дозволяє ідентифікувати сильні та слабкі сторони національного регулювання, що є основою для створення ефективної моделі захисту ПД з урахуванням міжнародного досвіду.

1.3. Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних

Попри наявність численних підходів до оцінювання ризиків у сфері інформаційної безпеки, методи, які дозволяють комплексно оцінювати сукупні втрати від витоку персональних даних, залишаються фрагментарними. Більшість існуючих моделей не враховує важливі аспекти – зокрема, довгострокові репутаційні втрати, вплив на права суб'єктів персональних даних, штрафні санкції регуляторів та соціальні наслідки для організацій.

Актуальність аналізу предмета дослідження зумовлена потребою у створенні інтегрованих теоретичних і прикладних засобів, які б дозволили: формалізовано оцінювати економічні, юридичні та репутаційні втрати від витоків ПД; підтримувати прийняття управлінських рішень у кризових ситуаціях;

забезпечувати відповідність сучасним вимогам законодавства у сфері захисту даних. Така багаторівнева оцінка є необхідною для побудови ефективних систем управління інформаційною безпекою, мінімізації наслідків інцидентів витоку персональних даних та підвищення рівня кіберстійкості організацій.

Існує безліч підходів до оцінки негативних наслідків витоку персональних даних. Нижче наведено аналіз понад 15 ключових моделей, методів та систем, що використовуються в інформаційній безпеці, а також беруть до уваги економічні, правові та репутаційні втрати. Кожен підхід коротко описано з контекстом застосування та основними підходами до вимірювання збитків.

1. FAIR (Factor Analysis of Information Risk) [33-35]. Модель FAIR – кількісний підхід до аналізу інформаційних ризиків, який розбиває ризик на частоту події втрати і величину втрат. 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: упущені доходи внаслідок ослаблення бренду). 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 [36-39]. 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 річні очікувані 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.

3. NIST Privacy Framework (PF) та PRAM [40]. NIST Privacy Framework – інструмент для управління ризиками приватності. 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 оцінити потік персональних даних, визначити області приватності, пріоритезувати ризики і обрати заходи реагування. Цей підхід більше орієнтований на управління процесами та ризик-менеджмент, ніж на безпосередню кількісну оцінку збитків.

4. ISO/IEC 27005 [38, 39, 41]. 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. 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.

5. ISO 31000 [42]. Міжнародний стандарт ISO 31000 (2018) 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.

6. OWASP Risk Rating Methodology [43]. 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), але залишається частково суб'єктивним, бо оцінка залежить від експертних балів (1–10).

7. Data Protection Impact Assessment (DPIA) за GDPR [44]. DPIA – це обов'язкова за GDPR (стаття 35) процедура оцінки впливу планованої обробки персональних даних на права та свободи осіб. Хоча DPIA не є числовим «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.

8. CRAMM (CCTA Risk Analysis and Management Method) [38, 39, 45]. CRAMM – це якісний інструмент для аналізу й управління ризиками), 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. 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 ПЗ (Insight CRAMM).

9. OCTAVE [45, 46]. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – фреймворк для оцінки кіберризиків. OCTAVE поєднує аналіз технічних вразливостей з пріоритетами бізнесу: спочатку ідентифікуються

критичні активи (персональні дані, IT-інфраструктура тощо), потім 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).

10. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) [45, 47]. EBIOS – метод аналізу ризиків IT-систем, поєднує сценарний аналіз і матричну оцінку: спершу визначаються події та активи (MAST), потім оцінюють їх впливи і ймовірності. 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.

11. MEHARI [45, 48]. MEHARI – французька методологія 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).

12. Ponemon Institute – емпірична модель вартості витоку даних [49]. 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. Методологія Ponemon базується на реальних даних, 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. Інструментальну реалізацію у вигляді ПЗ немає – це деталізований звіт.

13. Cyber Value at Risk (CyberVaR, CVaR) [45, 50]. Cyber Value at Risk (CVaR) – фінансова методика, адаптована до кіберризиків, що оцінює потенційні максимальні втрати за певним імовірнісним рівнем. Для обчислень CVaR застосовують сценарне моделювання (наприклад, Монте-Карло) з різними параметрами атаки (частота, наслідки, вартість активів). Метод надає статистично обґрунтовані верхні межі втрат. 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 [51]. Кількісна 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.

15. Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави [52]. 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 ДТ 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. 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.

16. Модель оцінювання параметрів безпеки персональних даних у степеневих соціальних мережах на основі їх топології [53]. 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.

17. Модель підвищення захищеності персональних даних користувачів системи дистанційного навчання збройних сил України. В [54] 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 [55]. Математична модель для оцінювання вартості інформації в межах діяльності установи. 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 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 [56-57].

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.

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. 1.2).

Таблиця 1.2.

Аналізу 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/кіберзбезпека	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
1	–	+	–	+	+	+	–	–	+	+	+	–	+	+	–
2	–	+	–	+	–	+	+	+	-	+	+	+	–	+	+
3	+	–	+	+	–	+	+	–	+–	–	–	+	–	–	+

Продовження таблиці 1.2.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	–	+	–	+	–	+	+	–	–	+	–	+	–	–	+
5	–	–	–	+	–	+	+	–	+–	+–	–	+	–	–	+
6	–	+	–	+	+	+	–	–	+	+	–	+	–	+	–
7	+	+	+	+	–	+	+	–	–	+	–	+	–	–	+
8	–	+	–	+	–	+	+	–	–	–	–	+	–	–	+
9	+–	–	–	+	+	+	+	–	+–	+–	–	+	–	–	+
10	+	+	+	+	+	+	+	–	–	–	–	+	–	–	+
11	–	+	–	+	–	+	+	–	+–	+–	–	+	–	–	+
12	–	–	–	+	+	+	–	+	+	+	+	–	–	+	–
13	–	+	–	+	+	–	–	+	+	+	+	–	–	+	–
14	+–	–	+	+	+	+	–	+	+	+	+	–	–	+	–
15	–	–	–	+	+	–	+	–	+	–	–	+	–	–	+
16	+–	–	+	–	+	–	+	–	+	–	–	–	+	+	–
17	+–	+	+	+	+	+	+	–	+	–	–	+	+	+	+
18	+–	–	–	+	+	+	+	–	+	+	–	–	+	+	–

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, 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.

1.4. Висновки до розділу 1

Узагальнено термінологічний апарат у сфері захисту персональних даних відповідно до чинного законодавства України та міжнародних нормативів, зокрема GDPR. Законодавчі дефініції понять «персональні дані», «обробка», «володілець», «розпорядник» сформували чітке підґрунтя для юридичного

врегулювання та оцінки інформаційних інцидентів. Дослідження показало, що узгодженість термінів між українським законодавством та GDPR є запорукою подальшої інтеграції національної системи захисту ПД до європейських стандартів.

Проведений аналіз нормативно-правового забезпечення захисту персональних даних продемонстрував розвиток нормативної бази у сфері захисту персональних даних як на національному, так і на міжнародному рівнях. Законодавство України має значний потенціал, проте потребує удосконалення – зокрема, запровадження інститутів DPIA, DPO, вдосконалення санкційного механізму та забезпечення екстериторіальної дії. Порівняльний аналіз законодавств ЄС, США, Канади дозволив ідентифікувати відмінності у підходах до регулювання приватності, прав суб'єктів даних та відповідальності за порушення. Зроблено висновок про доцільність подальшої гармонізації національного законодавства із GDPR для посилення правового захисту громадян України.

Аналіз існуючих методів, моделей та систем оцінювання втрат від витоку персональних даних показав, що більшість із них не забезпечують комплексного покриття всіх аспектів ризиків і не адаптовані до вимог сучасного законодавства, зокрема GDPR. Переважна частина підходів зосереджена на якісній або частково кількісній оцінці ризиків і потребує суб'єктивних експертних оцінок. Лише обмежене коло моделей (FAIR, CyberVaR, Ponemon) дає змогу проводити фінансову оцінку наслідків, що є вкрай важливим для ухвалення стратегічних управлінських рішень. Значна кількість методів також не має реалізованого програмного забезпечення або потребує дорогих інструментів, що обмежує їх доступність для малого і середнього бізнесу.

Зіставлення моделей, методів та систем за єдиним набором параметрів дозволило не лише визначити рівень відповідності кожного з них вимогам безпеки та практичного впровадження, а й виявити прогалини, які слід усунути під час розробки нових підходів. Перспективними виглядають українські моделі, що

враховують специфіку місцевих умов, зокрема в освітніх і військових структурах, але вони потребують доопрацювання в частині стандартизації та відповідності європейським нормам. Таким чином, існує реальна потреба у створенні нових інтегрованих моделях, методах та системах, яка б враховували як кількісні, так і якісні характеристики втрат, підтримували б аналітичні рішення у кризових ситуаціях і були б адаптовані до правового поля ЄС.

РОЗДІЛ 2. РОЗРОБКА МОДЕЛЕЙ ОЦІНЮВАННЯ ВТРАТ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Теоретико-множинна GDPR-модель параметрів персональних даних

Для мінімізації втрат від порушення організацією Регламенту GDPR та зменшення негативного рейтингу на рівні держави актуальною задачею є розробка методів та моделей, що реалізують відповідні оцінювання. Саме тому, теоретико-множинне представлення параметрів Регламенту GDPR у кортежній моделі дозволяє вирішити актуальну науково-практичну задачу формалізації процесу оцінювання негативних наслідків витоку ПД, заподіяних їх обробкою.

В ході проведеного аналізу було досліджено роботи у сфері захисту ПД [33-57]. Можливості зазначених розробок, щодо застосування їх для оцінювання шкоди відносно Регламенту GDPR [11] мають суттєві недоліки, оскільки: не враховано, що при аналізі Регламенту GDPR, організація не має змоги чітко встановити факт порушення, через відсутність чіткої прив'язки статей Регламенту GDPR до його одинадцяти принципів; відсутнє чітке визначення можливих масштабів фінансових та репутаційних збитків, у разі будь-якої дії, що суперечить Регламенту GDPR; не закладені можливості створення будь-якого GDPR-інструментарію, що дозволить автоматизувати в організації процес виявлення наслідків використання та будь-якої дії з ПД суб'єктів.

Введемо множину всіх можливих ідентифікаторів, що відображають організацію, яка реалізує процес виявлення та оцінювання наслідків від втрати ПД [58].

$$\mathbf{IDF} = \{\bigcup_{\varphi=1}^{z} \mathbf{IDF}^{\varphi}\} = \{\mathbf{IDF}^{\varphi_1}, \mathbf{IDF}^{\varphi_2}, ..., \mathbf{IDF}^{\varphi_z}\}, \quad (2.1)$$

де $\mathbf{IDF}^{\varphi} \subseteq \mathbf{IDF}\ (\varphi = \overline{1,z})$ – ідентифікатор кортежу параметрів φ-ї організації. Наприклад, (2.1) при z=3, матиме вигляд $\mathbf{IDF} = \{\bigcup_{\varphi=1}^{3} \mathbf{IDF}^{\varphi}\} = \{\mathbf{IDF}^{1}, \mathbf{IDF}^{2}, \mathbf{IDF}^{3}\} =$

$= \{\mathbf{IDF}^{КАІ}, \mathbf{IDF}^{СІТОН}, \mathbf{IDF}^{ФТЕХ}\}$, де $\mathbf{IDF}^{1} = \mathbf{IDF}^{КАІ}$, $\mathbf{IDF}^{2} = \mathbf{IDF}^{СІТОН}$, $\mathbf{IDF}^{3} = \mathbf{IDF}^{ФТЕХ}$ відповідно ідентифікатори кортежів параметрів організацій **«Київський**

авіаційний інститут», «СІТОН» та **«ФЛАЙ ТЕХНОЛОДЖИ»**.

Для φ-ї організації кортеж параметрів має вигляд:

$$\mathbf{IDF}^{\varphi} =< \mathbf{IDF}_1^{\varphi}, \mathbf{IDF}_2^{\varphi}, ..., \mathbf{IDF}_i^{\varphi}, ..., \mathbf{IDF}_n^{\varphi} >, \quad (2.2)$$

де: $\mathbf{IDF}_i^{\varphi} \subseteq \mathbf{IDF}^{\varphi}$ $(i = \overline{1,n})$ – компонент кортежу, що відображає i-й ідентифікатор параметрів φ-ї організації, а n – максимальне число таких параметрів. Зазначимо, що для всіх членів $\mathbf{IDF}^{\varphi}$ характерна властивість порядку. Наприклад, відповідно до Регламенту GDPR, при $n = 13$ кортеж (2.2) визначимо як [39, 40] (див. табл. 2.1):

$$\begin{gathered}\mathbf{IDF}^{\varphi} = < \mathbf{IDF}_1^{\varphi}, \mathbf{IDF}_2^{\varphi}, ..., \mathbf{IDF}_7^{\varphi}, ..., \mathbf{IDF}_{13}^{\varphi} >= \\ < \mathbf{T}^{\varphi}, \mathbf{L}^{\varphi}, \mathbf{N}^{\varphi}, \mathbf{CH}^{\varphi}, \mathbf{A}^{\varphi}, \mathbf{R}^{\varphi}, \mathbf{I}^{\varphi}, \mathbf{C}^{\varphi}, \mathbf{CA}^{\varphi}, \mathbf{M}^{\varphi}, \mathbf{ME}^{\varphi}, \mathbf{AD}^{\varphi}, \mathbf{F}^{\varphi}, \mathbf{RE}^{\varphi} >,\end{gathered} \quad (2.3)$$

де: $\mathbf{IDF}_1^{\varphi} = \mathbf{T}^{\varphi}$ (Річний обіг); $\mathbf{IDF}_2^{\varphi} = \mathbf{L}^{\varphi}$ (Рівень порушення); $\mathbf{IDF}_3^{\varphi} = \mathbf{N}^{\varphi}$ (Специфіка порушення); $\mathbf{IDF}_4^{\varphi} = \mathbf{CH}^{\varphi}$ (Характер порушення); $\mathbf{IDF}_5^{\varphi} = \mathbf{A}^{\varphi}$ (Зниження шкоди); $\mathbf{IDF}_6^{\varphi} = \mathbf{R}^{\varphi}$ (Ступінь відповідальності); $\mathbf{IDF}_7^{\varphi} = \mathbf{I}^{\varphi}$ (Рецидив порушення); $\mathbf{IDF}_8^{\varphi} = \mathbf{C}^{\varphi}$ (Рівень співпраці); $\mathbf{IDF}_9^{\varphi} = \mathbf{CA}^{\varphi}$ (Категорії даних); $\mathbf{IDF}_{10}^{\varphi} = \mathbf{M}^{\varphi}$ (Спосіб виявлення); $\mathbf{IDF}_{11}^{\varphi} = \mathbf{ME}^{\varphi}$ (Відповідність заходам); $\mathbf{IDF}_{12}^{\varphi} = \mathbf{AD}^{\varphi}$ (Дотримання кодексів); $\mathbf{IDF}_{13}^{\varphi} = \mathbf{F}^{\varphi}$ (Визначаючий чинник); $\mathbf{IDF}_{14}^{\varphi} = \mathbf{RE}^{\varphi}$ (Превентивні рекомендації) [60, 61].

Таблиця 2.1.

Приклад опису елементів кортежу відповідно до Регламенту GDPR

$\mathbf{IDF}^{\varphi}$	Назва $\mathbf{IDF}^{\varphi}$	Опис $\mathbf{IDF}^{\varphi}$
1	2	3
$\mathbf{T}^{\varphi}$	Річний обіг	Загальний глобальний річний обіг (turnover) підприємства за попередній фінансовий рік
$\mathbf{L}^{\varphi}$	Рівень порушення	Рівень (level) порушення
$\mathbf{N}^{\varphi}$	Специфіка порушення	Специфіка (nature), ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм
$\mathbf{CH}^{\varphi}$	Характер порушення	Навмисний або недбалий характер (character) порушення
$\mathbf{A}^{\varphi}$	Зниження шкоди	Будь-які дії (action), вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних
$\mathbf{R}^{\varphi}$	Ступінь відповідальності	Ступінь відповідальності (responsibility) контролера або оператора, зважаючи на технічні та організаційні інструменти, які вони застосовують відповідно до статей 25 і 32

Продовження таблиці 2.1.

1	2	3
$\mathbf{I^{\varphi}}$	Рецидив порушення	Будь-які належні попередні порушення (infringements) з боку контролера або оператора
$\mathbf{C^{\varphi}}$	Рівень співпраці	Рівень співпраці (cooperation) з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків порушення
$\mathbf{CA^{\varphi}}$	Категорії даних	Категорії (categories) ПД, на які вплинуло порушення
$\mathbf{M^{\varphi}}$	Спосіб виявлення	Спосіб (manner), у який наглядовому органу стало відомо про порушення, зокрема, або, і якщо так, то якою мірою, контролер або оператор повідомив про порушення
$\mathbf{ME^{\varphi}}$	Відповідність заходам	Якщо заходи (measures), вказані в статті 58(2), було раніше призначено проти відповідного контролера або оператора щодо того самого питання, – відповідність цим заходам
$\mathbf{AD^{\varphi}}$	Дотримання кодексів	Дотримання (adherence) затверджених кодексів поведінки відповідно до статті 40 або затверджених кодексів поведінки відповідно до статті 42
$\mathbf{F^{\varphi}}$	Визначаючий чинник	Будь-який інший обтяжувальний або пом'якшувальний фактор (factor), застосовний до обставин справи, такий як отримана фінансова вигода або витрати, яких вдалося уникнути, прямо чи опосередковано, від порушення
$\mathbf{RE^{\varphi}}$	Превентивні рекомендації	Превентивні рекомендації (recommendations). Вказуються для всіх компонент від 3 до 13.

Перший компонент кортежу $\mathbf{T^{\varphi}}$ – **«Річний обіг»**. Визначення глобального річного обігу підприємства за минулий рік. Формування компонента $\mathbf{T^{\varphi}}$ здійснюється шляхом визначення експертом річного обігу в €. Даний компонент методу немає розгалужень та має лише 1 елемент. Наприклад, якщо φ-та компанія за минулий фінансовий рік мала глобальний річний обіг 3 млрд. €, то даний компонент матиме наступний вигляд: $\mathbf{IDF_1^{\varphi} = T^{\varphi}} = 3\,000\,000\,000$ € [58].

Другий компонент $\mathbf{L^{\varphi}}$ – **«Рівень порушення»**, визначається виразом [62]:

$$\mathbf{L^{\varphi}} = \{\bigcup_{i=1}^{n_1} \mathbf{L_i^{\varphi}}\} = \{\mathbf{L_1^{\varphi}}, \mathbf{L_2^{\varphi}}, ..., \mathbf{L_{n_1}^{\varphi}}\}, \tag{2.4}$$

де: $\mathbf{L^{\varphi}}$ – множина усіх можливих рівнів порушень, $\mathbf{L_i^{\varphi}} \subseteq \mathbf{L^{\varphi}}$ $(i = \overline{1,n_1})$ – i-та підмножина рівнів порушення, а n_1 – кількість таких підмножин. Наприклад, при $n_1 = 2$ $(i = \overline{1,2})$ формулу (2.4) можна представити як: $\mathbf{L^{\varphi}} = \{\bigcup_{i=1}^{2} \mathbf{L_i^{\varphi}}\} = \{\mathbf{L_1^{\varphi}}, \mathbf{L_2^{\varphi}}\} =$ $\{$**"Ст.83,п.4","Ст.83,п.5"**$\}$, де з урахуванням [11] підмножини $\mathbf{L_1^{\varphi}} \subseteq \mathbf{L^{\varphi}}$ та $\mathbf{L_2^{\varphi}} \subseteq \mathbf{L^{\varphi}}$

відповідно характеризують значення: $\mathbf{L_1^{\varphi}} = \{\mathbf{"Ст.83,п.4"}\}$ та $\mathbf{L_2^{\varphi}} = \{\mathbf{"Ст.83,п.5"}\}$, що відповідно трактується як: «На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 10 000 000 євро або, у випадку підприємства, до 2% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою» та «На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 20 000 000 євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою». Далі, підмножину $\mathbf{L_i^{\varphi}}$ визначимо як:

$$\mathbf{L_i^{\varphi}} = \{\bigcup_{j=1}^{n_{1i}} L_{ij}^{\varphi}\} = \{L_{i1}^{\varphi}, L_{i2}^{\varphi}, ..., L_{in_{1i}}^{\varphi}\}, \tag{2.5}$$

де $L_{ij}^{\varphi} \subseteq \mathbf{L_i^{\varphi}}$ ($j = \overline{1,n_{1i}}$) – j-те значення параметру $\mathbf{L_i^{\varphi}}$ у межах i-ї підмножини, а n_{1i} кількість альтернативних значень параметрів i-ї підмножини. Відповідно до статті 83 (п.4, п.5) та, з урахуванням (2.5) вираз (2.4) можна представити у такому вигляді:

$$\mathbf{L^{\varphi}} = \{\bigcup_{i=1}^{n_1} \mathbf{L_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_1} \{\bigcup_{j=1}^{n_{1i}} L_{ij}^{\varphi}\}\} = \{\{L_{11}^{\varphi}, L_{12}^{\varphi}, ..., L_{1n_{1i}}^{\varphi}\}, \{L_{21}^{\varphi}, L_{22}^{\varphi}, ..., L_{2n_{1i}}^{\varphi}\}, ..., \{L_{n_1 1}^{\varphi}, L_{n_1 2}^{\varphi}, ..., L_{n_1 n_{1i}}^{\varphi}\}\}. \tag{2.6}$$

Тоді, наприклад, для φ-ї організації при $n_1 = 2$ ($i = \overline{1,2}$), $n_{11} = 3$ ($j = \overline{1,3}$), $n_{12} = 5$ ($j = \overline{1,5}$), формула (2.6) матиме вигляд:

$$\mathbf{L^{\varphi}} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{1i}} L_{ij}^{\varphi}\}\} = \{\{L_{11}^{\varphi}, L_{12}^{\varphi}, L_{13}^{\varphi}\}, \{L_{21}^{\varphi}, L_{22}^{\varphi}, L_{23}^{\varphi}, L_{24}^{\varphi}, L_{25}^{\varphi}\}\} = \{\{"Cm.83,n.4,nn.a", "Cm.83,n.4,nn.b", "Cm.83,n.4,nn.c"\}, \{"Cm.83,n.5,nn.a", "Cm.83,n.5,nn.b", "Cm.83,n.5,nn.c", Cm.83,n.5,nn.d", "Cm.83,n.5,nn.e"\}\}. \tag{2.7}$$

Третій компонент $\mathbf{N^{\varphi}}$ – **«Специфіка порушення»**, визначається виразом [63]:

$$\mathbf{N^{\varphi}} = \{\bigcup_{i=1}^{n_2} \mathbf{N_i^{\varphi}}\} = \{\mathbf{N_1^{\varphi}}, \mathbf{N_2^{\varphi}}, ..., \mathbf{N_{n_2}^{\varphi}}\}, \tag{2.8}$$

де $\mathbf{N^{\varphi}}$ – множина критеріїв специфіки, ступеня тяжкості і тривалості порушення, $\mathbf{N_i^{\varphi}} \subseteq \mathbf{N^{\varphi}}$ ($i = \overline{1,n_2}$) i-та підмножина критеріїв визначення специфіки, ступеня тяжкості

та тривалості порушення, а n_2 – кількість таких підмножин. Наприклад, для φ-ї організації при $n_2 = 4$ $(i = \overline{1,4})$ формулу (2.8) можна представити як: $\mathbf{N^{\varphi}} = \{\bigcup_{i=1}^{4} \mathbf{N_i^{\varphi}}\} = \{\mathbf{N_1^{\varphi}}, \mathbf{N_2^{\varphi}}, \mathbf{N_3^{\varphi}}, \mathbf{N_4^{\varphi}}\}$, де підмножини $\mathbf{N_1^{\varphi}} \subseteq \mathbf{N^{\varphi}}$, $\mathbf{N_2^{\varphi}} \subseteq \mathbf{N^{\varphi}}$, $\mathbf{N_3^{\varphi}} \subseteq \mathbf{N^{\varphi}}$ та $\mathbf{N_4^{\varphi}} \subseteq \mathbf{N^{\varphi}}$ відповідно характеризують значення: $\mathbf{N_1^{\varphi}}$ = **«Класифікація втрачених даних»;** $\mathbf{N_2^{\varphi}}$ = **«Протяжність порушення»;** $\mathbf{N_3^{\varphi}}$ = **«Кількість постраждалих суб'єктів ПД»;** $\mathbf{N_4^{\varphi}}$ = **«Рівень впливу на суб'єкти ПД».** Далі, підмножину $\mathbf{N_i^{\varphi}}$ визначимо як:

$$\mathbf{N_i^{\varphi}} = \{\bigcup_{j=1}^{n_{2i}} N_{ij}^{\varphi}\} = \{N_{i1}^{\varphi}, N_{i2}^{\varphi}, ..., N_{in_{2i}}^{\varphi}\}, \tag{2.9}$$

де $N_{ij}^{\varphi} \subseteq \mathbf{N_i^{\varphi}}$ $(j = \overline{1,n_{2i}})$ – j-те значення параметру $\mathbf{N_i^{\varphi}}$ у межах i-ї підмножини, а n_{2i} кількість альтернативних значень параметрів i-ї підмножини. Відповідно до сформованих підмножин у формулі (2.9) вираз (2.8) можна представити як:

$$\mathbf{N^{\varphi}} = \{\bigcup_{i=1}^{n_2} \mathbf{N_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_2} \{\bigcup_{j=1}^{n_{2i}} N_{ij}^{\varphi}\}\} = \{\{N_{11}^{\varphi}, N_{12}^{\varphi}, ..., N_{1n_{2i}}^{\varphi}\}, \{N_{21}^{\varphi}, N_{22}^{\varphi}, ..., N_{2n_{2i}}^{\varphi}\}, ..., \{N_{n_2 1}^{\varphi}, N_{n_2 2}^{\varphi}, ..., N_{n_2 n_{2i}}^{\varphi}\}\}. \tag{2.10}$$

Наприклад, при $n_2 = 4$ $(i = \overline{1,4})$, $n_{21} = 5$ $(j = \overline{1,5})$, $n_{22} = 5$ $(j = \overline{1,5})$, $n_{23} = 5$ $(j = \overline{1,5})$ і $n_{24} = 5$ $(j = \overline{1,5})$ формула (2.10) матиме вигляд:

$$\mathbf{N^{\varphi}} = \{\bigcup_{i=1}^{4} \{\bigcup_{j=1}^{n_{2i}} N_{ij}^{\varphi}\}\} = \{\{N_{11}^{\varphi}, N_{12}^{\varphi}, N_{13}^{\varphi}, N_{14}^{\varphi}, N_{15}^{\varphi}\}, \{N_{21}^{\varphi}, N_{22}^{\varphi}, N_{23}^{\varphi}, N_{24}^{\varphi}, N_{25}^{\varphi}\}, \{N_{31}^{\varphi}, N_{32}^{\varphi}, N_{33}^{\varphi}, N_{34}^{\varphi}, N_{35}^{\varphi}\}, \{N_{41}^{\varphi}, N_{42}^{\varphi}, N_{43}^{\varphi}, N_{44}^{\varphi}, N_{45}^{\varphi}\}\}. \tag{2.11}$$

Четвертий компонент $\mathbf{CH^{\varphi}}$ – «**Характер порушення»**, визначається виразом:

$$\mathbf{CH^{\varphi}} = \{\bigcup_{i=1}^{n_3} \mathbf{CH_i^{\varphi}}\} = \{\mathbf{CH_1^{\varphi}}, \mathbf{CH_2^{\varphi}}, ..., \mathbf{CH_{n_3}^{\varphi}}\}, \tag{2.12}$$

де $\mathbf{CH^{\varphi}}$ – множина критеріїв характеру порушення, $\mathbf{CH_i^{\varphi}} \subseteq \mathbf{CH^{\varphi}}$ $(i = \overline{1,n_3})$ i-та підмножина критеріїв характеру порушення, а n_3 – кількість таких підмножин. Наприклад, для φ-ї організації при $n_3 = 3$ $(i = \overline{1,3})$ формулу (2.12) можна

представити як: $\mathbf{CH^{\varphi}} = \{\bigcup_{i=1}^{3} \mathbf{CH_i^{\varphi}}\} = \{\mathbf{CH_1^{\varphi}}, \mathbf{CH_2^{\varphi}}, \mathbf{CH_3^{\varphi}}\}$, де підмножини $\mathbf{CH_1^{\varphi}} \subseteq \mathbf{CH^{\varphi}}$, $\mathbf{CH_2^{\varphi}} \subseteq \mathbf{CH^{\varphi}}$ та $\mathbf{CH_3^{\varphi}} \subseteq \mathbf{CH^{\varphi}}$ відповідно характеризують значення: $\mathbf{CH_1^{\varphi}}$ **= «Рівень галузевої підтримки програмної безпеки організації відповідно до міжнародних стандартів»;** $\mathbf{CH_2^{\varphi}}$ **= «Наявність повідомлення контролерами керівництва про ризики, що були виявлені»;** $\mathbf{CH_3^{\varphi}}$ **= «Дії керівництва на рекомендації з безпеки наглядового органу».** Підмножину $\mathbf{CH_i^{\varphi}}$ визначимо як:

$$\mathbf{CH_i^{\varphi}} = \{\bigcup_{j=1}^{n_{3i}} CH_{ij}^{\varphi}\} = \{CH_{i1}^{\varphi}, CH_{i2}^{\varphi}, ..., CH_{in_{3i}}^{\varphi}\}, \quad (2.13)$$

де $CH_{ij}^{\varphi} \subseteq \mathbf{CH_i^{\varphi}}$ $(j = \overline{1,n_{3i}})$ – j-те значення параметру $\mathbf{CH_i^{\varphi}}$ у межах i-ї підмножини, а n_{3i} кількість альтернативних значень параметрів i-ї підмножини. З урахування (2.13) вираз (2.12) можна представити як [58]: $\mathbf{CH^{\varphi}} = \{\bigcup_{i=1}^{n_3} \mathbf{CH_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_3} \{\bigcup_{j=1}^{n_{3i}} CH_{ij}^{\varphi}\}\} =$

$$\{\{CH_{11}^{\varphi}, CH_{12}^{\varphi}, ..., CH_{1n_{3i}}^{\varphi}\}, \{CH_{21}^{\varphi}, CH_{22}^{\varphi}, ..., CH_{2n_{3i}}^{\varphi}\}, ..., \{CH_{n_3 1}^{\varphi}, CH_{n_3 2}^{\varphi}, ..., CH_{n_3 n_{3i}}^{\varphi}\}\}. \quad (2.14)$$

Наприклад, при $n_3 = 3\,(i = \overline{1,3})$, $n_{31} = 5\,(j = \overline{1,5})$, $n_{32} = 2\,(j = \overline{1,2})$, $n_{33} = 2$ $(j = \overline{1,2})$ формула (2.14) матиме вигляд: $\mathbf{CH^{\varphi}} = \{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{n_{3i}} CH_{ij}^{\varphi}\}\} =$

$$\{\{CH_{11}^{\varphi}, CH_{12}^{\varphi}, CH_{13}^{\varphi}, CH_{14}^{\varphi}, CH_{15}^{\varphi}\}, \{CH_{21}^{\varphi}, CH_{22}^{\varphi}\}, \{CH_{31}^{\varphi}, CH_{32}^{\varphi}\}\}. \quad (2.15)$$

П’ятий компонент $\mathbf{A^{\varphi}}$ – **«Зниження шкоди»**, визначається виразом [64]:

$$\mathbf{A^{\varphi}} = \{\bigcup_{i=1}^{n_4} \mathbf{A_i^{\varphi}}\} = \{\mathbf{A_1^{\varphi}}, \mathbf{A_2^{\varphi}}, ..., \mathbf{A_{n_4}^{\varphi}}\}, \quad (2.16)$$

де $\mathbf{A^{\varphi}}$ – множина критеріїв дій, що вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб’єктами даних, $\mathbf{A_i^{\varphi}} \subseteq \mathbf{A^{\varphi}}$ $(i = \overline{1,n_4})$ – i-та підмножина вжитих дій контролером або оператором для зниження рівня шкоди, а n_4 – кількість таких підмножин. Наприклад, для φ-ї організації при $n_4 = 3$ $(i = \overline{1,3})$ формулу (2.16) можна інтерпретувати як: $\mathbf{A^{\varphi}} = \{\bigcup_{i=1}^{3} \mathbf{A_i^{\varphi}}\} = \{\mathbf{A_1^{\varphi}}, \mathbf{A_2^{\varphi}}, \mathbf{A_3^{\varphi}}\}$, де з урахуванням [11]

підмножини $\mathbf{A}_1^{\varphi} \subseteq \mathbf{A}^{\varphi}$, $\mathbf{A}_2^{\varphi} \subseteq \mathbf{A}^{\varphi}$ та $\mathbf{A}_3^{\varphi} \subseteq \mathbf{A}^{\varphi}$ відповідно характеризують значення: $\mathbf{A}_1^{\varphi}$**= «Міра відшкодування збитків, яких зазнали суб'єкти ПД»;** $\mathbf{A}_2^{\varphi}$**= «Наявність в організації дієвого плану пом'якшення наслідків до втручання наглядового органу»** та $\mathbf{A}_3^{\varphi}$**= «Розмір розрахункових витрат, що пов'язані з пом'якшенням наслідків».** Далі, підмножину $\mathbf{A}_\mathbf{i}^{\varphi}$ визначимо як:

$$\mathbf{A}_\mathbf{i}^{\varphi} = \{\bigcup_{j=1}^{n_{4i}} A_{ij}^{\varphi}\} = \{A_{i1}^{\varphi}, A_{i2}^{\varphi}, ..., A_{in_{4i}}^{\varphi}\}, \tag{2.17}$$

де $A_{ij}^{\varphi} \subseteq \mathbf{A}_\mathbf{i}^{\varphi}$ $(j = \overline{1,n_{4i}})$ – j-те значення параметру $\mathbf{A}_\mathbf{i}^{\varphi}$ у межах i-ї підмножини, а n_{4i} кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.17) вираз (2.16) можна представити як: $\mathbf{A}^{\varphi} = \{\bigcup_{i=1}^{n_4} \mathbf{A}_\mathbf{i}^{\varphi}\} = \{\bigcup_{i=1}^{n_4} \{\bigcup_{j=1}^{n_{4i}} A_{ij}^{\varphi}\}\} =$

$$\{\{A_{11}^{\varphi}, A_{12}^{\varphi}, ..., A_{1n_{4i}}^{\varphi}\}, \{A_{21}^{\varphi}, A_{22}^{\varphi}, ..., A_{2n_{4i}}^{\varphi}\}, ..., \{A_{n_4 1}^{\varphi}, A_{n_4 2}^{\varphi}, ..., A_{n_4 n_{4i}}^{\varphi}\}\}. \tag{2.18}$$

Наприклад, при $n_4 = 3$ $(i = \overline{1,4})$, $n_{41} = 5$ $(j = \overline{1,5})$, $n_{42} = 2$ $(j = \overline{1,2})$, $n_{43} = 5$ $(j = \overline{1,5})$ формула (2.18) матиме вигляд:

$$\mathbf{A}^{\varphi} = \{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{n_{4i}} A_{ij}^{\varphi}\}\} = \{\{A_{11}^{\varphi}, A_{12}^{\varphi}, A_{13}^{\varphi}, A_{14}^{\varphi}, A_{15}^{\varphi}\}, \{A_{21}^{\varphi}, A_{22}^{\varphi}\}, \{A_{31}^{\varphi}, A_{32}^{\varphi}, A_{33}^{\varphi}, A_{34}^{\varphi}, A_{35}^{\varphi}\}\}. \tag{2.19}$$

Шостий компонент $\mathbf{R}^{\varphi}$ – **«Ступінь відповідальності»**, визначається виразом:

$$\mathbf{R}^{\varphi} = \{\bigcup_{i=1}^{n_5} \mathbf{R}_\mathbf{i}^{\varphi}\} = \{\mathbf{R}_\mathbf{1}^{\varphi}, \mathbf{R}_\mathbf{2}^{\varphi}, ..., \mathbf{R}_{\mathbf{n_5}}^{\varphi}\}, \tag{2.20}$$

де $\mathbf{R}^{\varphi}$**–** множина ступеня відповідальності контролера/оператора, $\mathbf{R}_\mathbf{i}^{\varphi} \subseteq \mathbf{R}^{\varphi}$ $(i = \overline{1,n_5})$ – i-та підмножина ступеня відповідальності контролера/оператора, а n_5 – кількість таких підмножин. За аналогією з попереднім викладом, наприклад, при $n_5 = 8$ $(i = \overline{1,8})$ формулу (2.20) можна представити як: $\mathbf{R}^{\varphi} = \{\bigcup_{i=1}^{8} \mathbf{R}_\mathbf{i}^{\varphi}\} =$ $\{\mathbf{R}_\mathbf{1}^{\varphi}, \mathbf{R}_\mathbf{2}^{\varphi}, \mathbf{R}_\mathbf{3}^{\varphi}, \mathbf{R}_\mathbf{4}^{\varphi}, \mathbf{R}_\mathbf{5}^{\varphi}, \mathbf{R}_\mathbf{6}^{\varphi}, \mathbf{R}_\mathbf{7}^{\varphi}, \mathbf{R}_\mathbf{8}^{\varphi}\}$, де підмножини $\mathbf{R}_\mathbf{1}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, $\mathbf{R}_\mathbf{2}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, $\mathbf{R}_\mathbf{3}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, $\mathbf{R}_\mathbf{4}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, $\mathbf{R}_\mathbf{5}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, $\mathbf{R}_\mathbf{6}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, $\mathbf{R}_\mathbf{7}^{\varphi} \subseteq \mathbf{R}^{\varphi}$ та $\mathbf{R}_\mathbf{8}^{\varphi} \subseteq \mathbf{R}^{\varphi}$, відповідно характеризують

значення: $\mathbf{R_1^{\varphi}}$ **= «Наявність в організації забезпечення захисту ПД»;** $\mathbf{R_2^{\varphi}}$ **= «Наявність в організації використання засобів шифрування та маркування ПД»;** $\mathbf{R_3^{\varphi}}$ **= «Використання організацією сучасних стандартів шифрування інформації»;** $\mathbf{R_4^{\varphi}}$ **= «При використанні шифрування, було втрачено ключі разом із даними»;** $\mathbf{R_5^{\varphi}}$ **= «Виконання організацією затверджених планів реагування на інциденти та відновлення після них»;** $\mathbf{R_6^{\varphi}}$ **= «Наявність в організації надійних процедур тестування»;** $\mathbf{R_7^{\varphi}}$ **= «Наявність в організації надійних процедур управління ризиками»;** $\mathbf{R_8^{\varphi}}$ **= «Наявність Кодексу поведінки працівників в організації» [64].** Підмножину $\mathbf{R_i^{\varphi}}$ визначимо як:

$$\mathbf{R_i^{\varphi}} = \{\bigcup_{j=1}^{n_{5i}} R_{ij}^{\varphi}\} = \{R_{i1}^{\varphi}, R_{i2}^{\varphi}, ..., R_{in_{5i}}^{\varphi}\}, \tag{2.21}$$

де: $R_{ij}^{\varphi} \subseteq \mathbf{R_i^{\varphi}}$ $(j = \overline{1,n_{5i}})$ – j-те значення параметру $\mathbf{R_i^{\varphi}}$ у межах i-ї підмножини, а n_{5i} – кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.21) вираз (2.20) можна представити як: $\mathbf{R^{\varphi}} = \{\bigcup_{i=1}^{n_5} \mathbf{R_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_5} \{\bigcup_{j=1}^{n_{5i}} R_{ij}^{\varphi}\}\} =$

$$\{\{R_{11}^{\varphi}, R_{12}^{\varphi}, ..., R_{1n_{5i}}^{\varphi}\}, \{R_{21}^{\varphi}, R_{22}^{\varphi}, ..., R_{2n_{5i}}^{\varphi}\}, ..., \{R_{n_5 1}^{\varphi}, R_{n_5 2}^{\varphi}, ..., R_{n_5 n_{5i}}^{\varphi}\}\}. \tag{2.22}$$

Наприклад, для φ-ї організації при $n_5 = 8$ $(i = \overline{1,8})$, $n_{51} = 2$ $(j = \overline{1,2})$, $n_{52} = 2$ $(j = \overline{1,2})$, $n_{53} = 3$ $(j = \overline{1,3})$, $n_{54} = 3$ $(j = \overline{1,3})$, $n_{55} = 2$ $(j = \overline{1,2})$, $n_{56} = 2$ $(j = \overline{1,2})$, $n_{57} = 2$ $(j = \overline{1,2})$, $n_{58} = 2$ $(j = \overline{1,2})$, формула (2.22) матиме вигляд:

$$\mathbf{R^{\varphi}} = \{\bigcup_{i=1}^{8} \{\bigcup_{j=1}^{n_{5i}} R_{ij}^{\varphi}\}\} = \{\{R_{11}^{\varphi}, R_{12}^{\varphi}\}, \{R_{21}^{\varphi}, R_{22}^{\varphi}\},$$
$$\{R_{31}^{\varphi}, R_{32}^{\varphi}, R_{33}^{\varphi}\}, \{R_{41}^{\varphi}, R_{42}^{\varphi}, R_{43}^{\varphi}\}, \{R_{51}^{\varphi}, R_{52}^{\varphi}\}, \{R_{61}^{\varphi}, R_{62}^{\varphi}\}, \{R_{71}^{\varphi}, R_{72}^{\varphi}\}, \{R_{81}^{\varphi}, R_{82}^{\varphi}\}\}. \tag{2.23}$$

Сьомий компонент $\mathbf{I^{\varphi}}$ – **«Рецидив порушення»** [58], визначається виразом:

$$\mathbf{I^{\varphi}} = \{\bigcup_{i=1}^{n_6} \mathbf{I_i^{\varphi}}\} = \{\mathbf{I_1^{\varphi}}, \mathbf{I_2^{\varphi}}, ..., \mathbf{I_{n_6}^{\varphi}}\}, \tag{2.24}$$

де $\mathbf{I^{\varphi}}$ **–** множина порушень з боку контролера/оператора, $\mathbf{I_i^{\varphi}} \subseteq \mathbf{I^{\varphi}}$ $(i = \overline{1,n_6})$ i-та

підмножина порушень з боку контролера/оператора, а n_6 кількість таких підмножин. Наприклад, $n_6 = 1$ $(i = 1)$ формулу (2.24) можна представити як: $\mathbf{I}^{\varphi} = \{\bigcup_{i=1}^{1} \mathbf{I}_i^{\varphi}\} = \{\mathbf{I}_1^{\varphi}\},$ де підмножина $\mathbf{I}_1^{\varphi} \subseteq \mathbf{I}^{\varphi}$ відповідно характеризує значення: $\mathbf{I}_1^{\varphi}$ = **«Перша втрата ПД в організації».** Підмножину $\mathbf{I}_i^{\varphi}$ визначимо як:

$$\mathbf{I}_i^{\varphi} = \{\bigcup_{j=1}^{n_{6i}} \mathbf{I}_{ij}^{\varphi}\} = \{\mathbf{I}_{i1}^{\varphi}, \mathbf{I}_{i2}^{\varphi}, ..., \mathbf{I}_{in_{6i}}^{\varphi}\}, \quad (2.25)$$

де $\mathbf{I}_{ij}^{\varphi} \subseteq \mathbf{I}_i^{\varphi}$ $(j = \overline{1, n_{6i}})$ – j-те значення параметру $\mathbf{I}_i^{\varphi}$ у межах i-ї підмножини, а n_{6i} – кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.25) вираз (2.24) можна представити як: $\mathbf{I}^{\varphi} = \{\bigcup_{i=1}^{n_6} \mathbf{I}_i^{\varphi}\} = \{\bigcup_{i=1}^{n_6} \{\bigcup_{j=1}^{n_{6i}} \mathbf{I}_{ij}^{\varphi}\}\} =$

$$\{\{\mathbf{I}_{11}^{\varphi}, \mathbf{I}_{12}^{\varphi}, ..., \mathbf{I}_{1n_{6i}}^{\varphi}\}, \{\mathbf{I}_{21}^{\varphi}, \mathbf{I}_{22}^{\varphi}, ..., \mathbf{I}_{2n_{6i}}^{\varphi}\}, ..., \{\mathbf{I}_{n_6 1}^{\varphi}, \mathbf{I}_{n_6 2}^{\varphi}, ..., \mathbf{I}_{n_6 n_{6i}}^{\varphi}\}\}. \quad (2.26)$$

Наприклад, при $n_6 = 1$ $(i = 1)$, $n_{61} = 2$ $(j = \overline{1,2})$, формулу (2.26) можна представити як:

$$\mathbf{I}_i^{\varphi} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{n_{6i}} \mathbf{I}_{ij}^{\varphi}\}\} = \{\{\mathbf{I}_{11}^{\varphi}, \mathbf{I}_{12}^{\varphi}\}\}, \quad (2.27)$$

де: $\mathbf{I}_{11}^{\varphi}$ = **«Так»**; $\mathbf{I}_{12}^{\varphi}$ = **«Ні»**. Зважаючи на вираз (2.27), а саме компоненту $\mathbf{I}_{12}^{\varphi}$, яка має відповідь **«Ні»**, отримуємо наступне розгалуження підмножини $\mathbf{I}_{ij}^{\varphi}$:

$$\mathbf{I}_{ij}^{\varphi} = \{\bigcup_{k=1}^{n_{6ij}} \mathbf{I}_{ijk}^{\varphi}\} = \{\mathbf{I}_{ij1}^{\varphi}, \mathbf{I}_{ij2}^{\varphi}, ..., \mathbf{I}_{ijn_{6ij}}^{\varphi}\}, \quad (2.28)$$

де $\mathbf{I}_{ijk}^{\varphi} \subseteq \mathbf{I}_{ij}^{\varphi}$ $(k = \overline{1, n_{6ij}})$ – k-те значення параметру $\mathbf{I}_{ij}$ у межах ij-ї підмножини, а n_{6ij} – кількість альтернативних значень параметрів ij-ї підмножини. З урахуванням (2.28) вираз (2.26) можна представити як: $\mathbf{I}^{\varphi} = \{\bigcup_{i=1}^{n_6} \mathbf{I}_i^{\varphi}\} = \{\bigcup_{i=1}^{n_6} \{\bigcup_{j=1}^{n_{6i}} \mathbf{I}_{ij}^{\varphi}\}\} =$

$$\{\bigcup_{i=1}^{n_6}\{\bigcup_{j=1}^{n_{6i}}\{\bigcup_{k=1}^{n_{6ij}}\mathbf{I}^{\varphi}_{\mathbf{ijk}}\}\}\} = \{\{\{\mathbf{I}^{\varphi}_{111},\mathbf{I}^{\varphi}_{112},...,\mathbf{I}^{\varphi}_{11\mathbf{n}_{6ij}}\},\{\mathbf{I}^{\varphi}_{121},\mathbf{I}^{\varphi}_{122},...,\mathbf{I}^{\varphi}_{12\mathbf{n}_{6ij}}\},...,$$
$$\{\mathbf{I}^{\varphi}_{1\mathbf{n}_{6i}1},\mathbf{I}^{\varphi}_{1\mathbf{n}_{6i}2},...,\mathbf{I}^{\varphi}_{1\mathbf{n}_{6i}\mathbf{n}_{6ij}}\}\},...,\{\{\mathbf{I}^{\varphi}_{\mathbf{n}_6 11},\mathbf{I}^{\varphi}_{\mathbf{n}_6 12},...,\mathbf{I}^{\varphi}_{\mathbf{n}_6 1\mathbf{n}_{6ij}}\},$$
$$\{\mathbf{I}^{\varphi}_{\mathbf{n}_6 21},\mathbf{I}^{\varphi}_{\mathbf{n}_6 22},...,\mathbf{I}^{\varphi}_{\mathbf{n}_6 2\mathbf{n}_{6ij}}\},...,\{\mathbf{I}^{\varphi}_{\mathbf{n}_6\mathbf{n}_{6i}1},\mathbf{I}^{\varphi}_{\mathbf{n}_6\mathbf{n}_{6i}2},...,\mathbf{I}^{\varphi}_{\mathbf{n}_6\mathbf{n}_{6i}\mathbf{n}_{6ij}}\}\}\}. \quad (2.29)$$

Наприклад, при $n_6 = 1$ $(i = 1)$, $n_{61} = 2$ $(i = \overline{1,2})$, та при $n_{61} = 1$ $n_{611} = 0$ $(j = 0)$, а при $n_{61} = 2$ $n_{612} = 3$ $(j = \overline{1,3})$, формулу (2.29) можна представити як:

$$\mathbf{I}^{\varphi} = \{\bigcup_{i=1}^{1}\mathbf{I}^{\varphi}_{\mathbf{i}}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\mathbf{I}^{\varphi}_{\mathbf{ij}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\{\bigcup_{k=1}^{n_{6ij}}\mathbf{I}^{\varphi}_{\mathbf{ijk}}\}\}\} = \{\{\mathbf{I}^{\varphi}_{11},\{\mathbf{I}^{\varphi}_{121},\mathbf{I}^{\varphi}_{122},\mathbf{I}^{\varphi}_{123}\}\}\}, \quad (2.30)$$

де: $\mathbf{I}^{\varphi}_{121}$ = **«Нове порушення (втрата даних, їх видалення, типи даних) аналогічно попередньому»**; $\mathbf{I}^{\varphi}_{122}$ = **«Організацією вжито заходів щодо усунення проблем, які було зафіксовано в попередньому порушенні»**; $\mathbf{I}^{\varphi}_{123}$ = **«Наявність стягнення штрафу за нове порушення»**. Виходячи з (2.30), підмножину $\mathbf{I}^{\varphi}_{\mathbf{ijk}}$ визначимо як:

$$\mathbf{I}^{\varphi}_{\mathbf{ijk}} = \{\bigcup_{e=1}^{n_{6ijk}} I^{\varphi}_{ijke}\} = \{I^{\varphi}_{ijk1}, I^{\varphi}_{ijk2},..., I^{\varphi}_{ijkn_{6ijk}}\}, \quad (2.31)$$

де $I^{\varphi}_{ijke} \subseteq \mathbf{I}^{\varphi}_{\mathbf{ijk}}$ $(e = \overline{1,n_{6ijk}})$ – e-те значення параметру $\mathbf{I}^{\varphi}_{\mathbf{ijk}}$ у межах ijk-ї підмножини, а n_{6ijk} кількість альтернативних значень параметрів ijk-ї підмножини.

З урахуванням (2.31) вираз (2.29) можна представити як: $\mathbf{I}^{\varphi} = \{\bigcup_{i=1}^{n_6}\mathbf{I}^{\varphi}_{\mathbf{i}}\} =$

$$\{\bigcup_{i=1}^{n_6}\{\bigcup_{j=1}^{n_{6i}}\mathbf{I}^{\varphi}_{\mathbf{ij}}\}\} = \{\bigcup_{i=1}^{n_6}\{\bigcup_{j=1}^{n_{6i}}\{\bigcup_{k=1}^{n_{6ij}}\mathbf{I}^{\varphi}_{\mathbf{ijk}}\}\}\} = \{\bigcup_{i=1}^{n_6}\{\bigcup_{j=1}^{n_{6i}}\{\bigcup_{k=1}^{n_{6ij}}\{\bigcup_{e=1}^{n_{6ijk}} I^{\varphi}_{ijke}\}\}\}\} = \{\{\{\{I^{\varphi}_{1111}, I^{\varphi}_{1112},...,$$
$$I^{\varphi}_{111n_{6ijk}}\},\{I^{\varphi}_{1121}, I^{\varphi}_{1122},..., I^{\varphi}_{112n_{6ijk}}\},...,\{I^{\varphi}_{11n_{6ij}1}, I^{\varphi}_{11n_{6ij}2},..., I^{\varphi}_{11n_{6ij}n_{6ijk}}\}\},...,\{\{I^{\varphi}_{n_6n_{6i}11}, \quad (2.32)$$
$$I^{\varphi}_{n_6n_{6i}12},..., I^{\varphi}_{n_6n_{6i}1n_{6ijk}}\},\{I^{\varphi}_{n_6n_{6i}21}, I^{\varphi}_{n_6n_{6i}22},..., I^{\varphi}_{n_6n_{6i}2n_{6ijk}}\},...,\{I^{\varphi}_{n_6n_{6i}n_{6ij}1}, I^{\varphi}_{n_6n_{6i}n_{6ij}2},..., I^{\varphi}_{n_6n_{6i}n_{6ij}n_{6ijk}}\}\}\}\}.$$

Наприклад, для φ-ї організації при $n_6 = 1$ $(i = 1)$, $n_{61} = 2$ $(j = \overline{1,2})$, та при $n_{61} = 1$ $n_{611} = 0$ $(k = 0)$, а при $n_{61} = 2$ $n_{612} = 3$ $(k = \overline{1,3})$, $n_{6121} = 3$ $(e = \overline{1,3})$, $n_{6122} = 3$ $(e = \overline{1,3})$, $n_{6123} = 3$ $(e = \overline{1,3})$ формулу (2.32) можна представити як:

$$\mathbf{I}^{\varphi} = \{\bigcup_{i=1}^{1}\mathbf{I}_{\mathbf{i}}^{\varphi}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\mathbf{I}_{\mathbf{ij}}^{\varphi}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\{\bigcup_{k=1}^{n_{6ij}}\mathbf{I}_{\mathbf{ijk}}^{\varphi}\}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\{\bigcup_{k=1}^{n_{6ij}}\{\bigcup_{e=1}^{n_{6ijk}}I_{ijke}^{\varphi}\}\}\}\} =$$
$$\{\{I_{11}^{\varphi},\{\{I_{1211}^{\varphi},I_{1212}^{\varphi},I_{1213}^{\varphi}\},\{I_{1221}^{\varphi},I_{1222}^{\varphi},I_{1223}^{\varphi}\},\{I_{1231}^{\varphi},I_{1232}^{\varphi},I_{1233}^{\varphi}\}\}\}\}. \quad (2.33)$$

Восьмий компонент $\mathbf{C}^{\varphi}$ – **«Рівень співпраці»** [58, 59] визначається виразом:

$$\mathbf{C}^{\varphi} = \{\bigcup_{i=1}^{n_7}\mathbf{C}_{\mathbf{i}}^{\varphi}\} = \{\mathbf{C}_{\mathbf{1}}^{\varphi},\mathbf{C}_{\mathbf{2}}^{\varphi},...,\mathbf{C}_{\mathbf{n_7}}^{\varphi}\}, \quad (2.34)$$

де $\mathbf{C}^{\varphi}$ – множина критеріїв рівня співпраці з наглядовим органом, $\mathbf{C}_{\mathbf{i}}^{\varphi} \subseteq \mathbf{C}^{\varphi}$ $(i = \overline{1,n_7})$ i-та підмножина рівня співпраці з наглядовим органом, а n_7 – кількість таких підмножин. Наприклад, $n_7 = 3\,(i = \overline{1,3})$ формулу (2.34) можна представити як: $\mathbf{C}^{\varphi} = \{\bigcup_{i=1}^{3}\mathbf{C}_{\mathbf{i}}^{\varphi}\} = \{\mathbf{C}_{\mathbf{1}}^{\varphi},\mathbf{C}_{\mathbf{2}}^{\varphi},\mathbf{C}_{\mathbf{3}}^{\varphi}\}$, де підмножини $\mathbf{C}_{\mathbf{1}}^{\varphi} \subseteq \mathbf{C}^{\varphi}$, $\mathbf{C}_{\mathbf{2}}^{\varphi} \subseteq \mathbf{C}^{\varphi}$ та $\mathbf{C}_{\mathbf{3}}^{\varphi} \subseteq \mathbf{C}^{\varphi}$, відповідно характеризують значення: $\mathbf{C}_{\mathbf{1}}^{\varphi}$ = «**Міра безпосереднього залучення керівництва до розслідування наглядовим органом»**, $\mathbf{C}_{\mathbf{2}}^{\varphi}$ = **«Працівники з власної ініціативи дали свідчення наглядовому органу»** та $\mathbf{C}_{\mathbf{3}}^{\varphi}$ = **«Організація розробила і подала План по відновленню / Отримано Наказ від наглядового органу»**. Підмножину $\mathbf{C}_{\mathbf{i}}^{\varphi}$ можна представити як:

$$\mathbf{C}_{\mathbf{i}}^{\varphi} = \{\bigcup_{j=1}^{n_{7i}}C_{ij}^{\varphi}\} = \{C_{i1}^{\varphi},C_{i2}^{\varphi},...,C_{in_{7i}}^{\varphi}\}, \quad (2.35)$$

де $C_{ij}^{\varphi} \subseteq \mathbf{C}_{\mathbf{i}}^{\varphi}$ $(j = \overline{1,n_{7i}})$ – j-те значення параметру $\mathbf{C}_{\mathbf{i}}^{\varphi}$ у межах i-ї підмножини, а n_{7i} кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.35) вираз (2.34) можна представити як: $\mathbf{C}^{\varphi} = \{\bigcup_{i=1}^{n_7}\mathbf{C}_{\mathbf{i}}^{\varphi}\} = \{\bigcup_{i=1}^{n_7}\{\bigcup_{j=1}^{n_{7i}}C_{ij}^{\varphi}\}\} =$

$$\{\{C_{11}^{\varphi},C_{12}^{\varphi},...,C_{1n_{7i}}^{\varphi}\},\{C_{21}^{\varphi},C_{22}^{\varphi},...,C_{2n_{7i}}^{\varphi}\},...,\{C_{n_7 1}^{\varphi},C_{n_7 2}^{\varphi},...,C_{n_7 n_{7i}}^{\varphi}\}\}. \quad (2.36)$$

Наприклад, при $n_7 = 3\,(i = \overline{1,3})$, $n_{71} = 5\,(j = \overline{1,5})$, $n_{72} = 2\,(j = \overline{1,2})$, $n_{73} = 2$ $(j = \overline{1,2})$ формула (2.36) матиме вигляд:

$$\mathbf{C^{\varphi}} = \{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{n_{7i}} C_{ij}^{\varphi}\}\} = \{\{C_{11}^{\varphi}, C_{12}^{\varphi}, C_{13}^{\varphi}, C_{14}^{\varphi}, C_{15}^{\varphi}\}, \{C_{21}^{\varphi}, C_{22}^{\varphi}\}, \{C_{31}^{\varphi}, C_{32}^{\varphi}\}\}. \quad (2.37)$$

Дев'ятий компонент $\mathbf{CA^{\varphi}}$ – **«Категорії даних»**, визначається виразом:

$$\mathbf{CA^{\varphi}} = \{\bigcup_{i=1}^{n_8} \mathbf{CA_i^{\varphi}}\} = \{\mathbf{CA_1^{\varphi}}, \mathbf{CA_2^{\varphi}}, ..., \mathbf{CA_{n_8}^{\varphi}}\}, \quad (2.38)$$

де $\mathbf{CA^{\varphi}}$ – множина критеріїв категорій ПД, $\mathbf{CA_i^{\varphi}} \subseteq \mathbf{CA^{\varphi}}$ $(i = \overline{1,n_8})$ i-та підмножина категорій ПД, на які вплинуло порушення, а n_8 – кількість таких підмножин. Наприклад, $n_8 = 3$ $(i = \overline{1,3})$ формулу (2.38) можна представити як: $\mathbf{CA^{\varphi}} = \{\bigcup_{i=1}^{3} \mathbf{CA_i^{\varphi}}\} =$ $\{\mathbf{CA_1^{\varphi}}, \mathbf{CA_2^{\varphi}}, \mathbf{CA_3^{\varphi}}\}$, де підмножини $\mathbf{CA_1^{\varphi}} \subseteq \mathbf{CA^{\varphi}}$, $\mathbf{CA_2^{\varphi}} \subseteq \mathbf{CA^{\varphi}}$ та $\mathbf{CA_3^{\varphi}} \subseteq \mathbf{CA^{\varphi}}$, відповідно характеризують значення: $\mathbf{CA_1^{\varphi}}$ = **«Втрачені дані про персонал організації були незашифровані»**, $\mathbf{CA_2^{\varphi}}$ = **«Втрачені дані містили чутливі ПД організації»** та $\mathbf{CA_3^{\varphi}}$ = «**Втрачені дані містили інформацію про кримінальні правопорушення організації».** Підмножину $\mathbf{CA_i^{\varphi}}$ можна представити як:

$$\mathbf{CA_i^{\varphi}} = \{\bigcup_{j=1}^{n_{8i}} CA_{ij}^{\varphi}\} = \{CA_{i1}^{\varphi}, CA_{i2}^{\varphi}, ..., CA_{in_{8i}}^{\varphi}\}, \quad (2.39)$$

де $CA_{ij}^{\varphi} \subseteq \mathbf{CA_i^{\varphi}}$ $(j = \overline{1,n_{8i}})$ – j-те значення параметру $\mathbf{CA_i^{\varphi}}$ у межах i-ї підмножини, а n_{8i} кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.39) вираз (2.38) можна представити як: $\mathbf{CA^{\varphi}} = \{\bigcup_{i=1}^{n_8} \mathbf{CA_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_8}\{\bigcup_{j=1}^{n_{8i}} CA_{ij}^{\varphi}\}\} =$

$$\{\{CA_{11}^{\varphi}, CA_{12}^{\varphi}, ..., CA_{1n_{8i}}^{\varphi}\}, \{CA_{21}^{\varphi}, CA_{22}^{\varphi}, ..., CA_{2n_{8i}}^{\varphi}\}, ..., \{CA_{n_8 1}^{\varphi}, CA_{n_8 2}^{\varphi}, ..., CA_{n_8 n_{8i}}^{\varphi}\}\}. \quad (2.40)$$

Наприклад, при $n_8 = 3$ $(i = \overline{1,3})$, $n_{81} = 2$ $(j = \overline{1,5})$, $n_{82} = 2$ $(j = \overline{1,2})$ і $n_{83} = 2$ $(j = \overline{1,2})$ формула (2.40) матиме вигляд:

$$\mathbf{CA^{\varphi}} = \{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{n_{8i}} CA_{ij}^{\varphi}\}\} = \{\{CA_{11}^{\varphi}, CA_{12}^{\varphi}\}, \{CA_{21}^{\varphi}, CA_{22}^{\varphi}\}, \{CA_{31}^{\varphi}, CA_{32}^{\varphi}\}\}. \quad (2.41)$$

Десятий компонент $\mathbf{M^{\varphi}}$ – **«Спосіб виявлення»** [59], визначається виразом:

$$\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{n_9} \mathbf{M_i^{\varphi}}\} = \{\mathbf{M_1^{\varphi}}, \mathbf{M_2^{\varphi}}, ..., \mathbf{M_{n_9}^{\varphi}}\}, \quad (2.42)$$

де $\mathbf{M^{\varphi}}$ – множина критеріїв способу повідомлення про порушення, $\mathbf{M_i^{\varphi}} \subseteq \mathbf{M^{\varphi}}$ $(i = \overline{1,n_9})$ *i*-та підмножина способу, у який наглядовому органу стало відомо про порушення, а n_9 – кількість таких підмножин. Наприклад, $n_9 = 1$ $(i = 1)$ формулу (2.42) можна представити як: $\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{1} \mathbf{M_i^{\varphi}}\} = \{\mathbf{M_1^{\varphi}}\}$, де підмножина $\mathbf{M_1^{\varphi}} \subseteq \mathbf{M^{\varphi}}$ відповідно характеризує значення: $\mathbf{M_1^{\varphi}}$ = **«Наглядовий орган отримав повідомлення про порушення від:»**. Підмножину $\mathbf{M_i^{\varphi}}$ визначимо як:

$$\mathbf{M_i^{\varphi}} = \{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}^{\varphi}}\} = \{\mathbf{M_{i1}^{\varphi}}, \mathbf{M_{i2}^{\varphi}}, ..., \mathbf{M_{in_{9i}}^{\varphi}}\}, \quad (2.43)$$

де: $\mathbf{M_{ij}^{\varphi}} \subseteq \mathbf{M_i^{\varphi}}$ $(j = \overline{1,n_{9i}})$ – *j*-те значення параметру $\mathbf{M_i^{\varphi}}$ у межах *i*-ї підмножини, а n_{9i} кількість альтернативних значень параметрів *i*-ї підмножини. З урахуванням (2.43) вираз (2.42) можна представити як: $\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{n_9} \mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}^{\varphi}}\}\} =$

$$\{\{\mathbf{M_{11}^{\varphi}}, \mathbf{M_{12}^{\varphi}}, ..., \mathbf{M_{1n_{9i}}^{\varphi}}\}, \{\mathbf{M_{21}^{\varphi}}, \mathbf{M_{22}^{\varphi}}, ..., \mathbf{M_{2n_{9i}}^{\varphi}}\}, ..., \{\mathbf{M_{n_9 1}^{\varphi}}, \mathbf{M_{n_9 2}^{\varphi}}, ..., \mathbf{M_{n_9 n_{9i}}^{\varphi}}\}\}. \quad (2.44)$$

Наприклад, при $n_9 = 1$ $(i = 1)$, $n_{91} = 4$ $(j = \overline{1,4})$ формулу (2.44) можна представити як: $\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}^{\varphi}}\}\} = \{\{\mathbf{M_{11}^{\varphi}}, \mathbf{M_{12}^{\varphi}}, \mathbf{M_{13}^{\varphi}}, \mathbf{M_{14}^{\varphi}}\}\}$, де: $\mathbf{M_{11}^{\varphi}}$ = **«Суб'єкт порушник»**; $\mathbf{M_{12}^{\varphi}}$ = **«Інформатор»**; $\mathbf{M_{13}^{\varphi}}$ = **«Заголовки ЗМІ»**; $\mathbf{M_{14}^{\varphi}}$ = **«Інше»**. Підмножину $\mathbf{M_{ij}^{\varphi}}$ визначимо як:

$$\mathbf{M_{ij}^{\varphi}} = \{\bigcup_{k=1}^{n_{9ij}} \mathbf{M_{ijk}^{\varphi}}\} = \{\mathbf{M_{ij1}^{\varphi}}, \mathbf{M_{ij2}^{\varphi}}, ..., \mathbf{M_{ijn_{9ij}}^{\varphi}}\}, \quad (2.45)$$

де $\mathbf{M_{ijk}^{\varphi}} \subseteq \mathbf{M_{ij}^{\varphi}}$ $(k = \overline{1,n_{9ij}})$ – *k*-те значення параметру $\mathbf{M_{ij}^{\varphi}}$ у межах *ij*-ї підмножини, а n_{9ij} кількість альтернативних значень параметрів *ij*-ї підмножини. З урахуванням (2.45) вираз (2.44) можна представити як:

$$\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{n_9}\mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\mathbf{M_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\mathbf{M_{ijk}^{\varphi}}\}\}\} = \{\{\{\mathbf{M_{111}^{\varphi}},\mathbf{M_{112}^{\varphi}},...,\mathbf{M_{11n_{9ij}}^{\varphi}}\},$$
$$\{\mathbf{M_{121}^{\varphi}},\mathbf{M_{122}^{\varphi}},...,\mathbf{M_{12n_{9ij}}^{\varphi}}\},...,\{\mathbf{M_{1n_{9i}1}^{\varphi}},\mathbf{M_{1n_{9i}2}^{\varphi}},...,\mathbf{M_{1n_{9i}n_{9ij}}^{\varphi}}\}\},...,\{\{\mathbf{M_{n_9 11}^{\varphi}},\mathbf{M_{n_9 12}^{\varphi}},...,$$
$$\mathbf{M_{n_9 1n_{9ij}}^{\varphi}}\},\{\mathbf{M_{n_9 21}^{\varphi}},\mathbf{M_{n_9 22}^{\varphi}},...,\mathbf{M_{n_9 2n_{9ij}}^{\varphi}}\},...,\{\mathbf{M_{n_9n_{9i}1}^{\varphi}},\mathbf{M_{n_9n_{9i}2}^{\varphi}},...,\mathbf{M_{n_9n_{9i}n_{9ij}}^{\varphi}}\}\}\}. \quad (2.46)$$

Наприклад, при $n_9 = 1$ $(i = 1)$, $n_{91} = 4$ $(j = \overline{1,4})$ та $n_{91} = 1$ $n_{911} = 1$ $(k = \overline{1,1})$, а при $n_{91} = 2$, $n_{91} = 3$, $n_{91} = 4$ і $n_{912} = 0$ $(k = 0)$ формулу (2.46) можна представити як: $\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{1}\mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\mathbf{M_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\{\bigcup_{k=1}^{n_{9ij}}\mathbf{M_{ijk}^{\varphi}}\}\}\} = \{\{\{\mathbf{M_{111}^{\varphi}}\},\mathbf{M_{12}^{\varphi}},\mathbf{M_{13}^{\varphi}},\mathbf{M_{14}^{\varphi}}\}\}$, де: $\mathbf{M_{111}^{\varphi}} =$ **«"Суб'єкт порушник" повідомив наглядовий орган протягом 72 годин після виникнення інциденту» відповідно до статті 33(1)».** Підмножину $\mathbf{M_{ijk}^{\varphi}}$ визначимо як:

$$\mathbf{M_{ijk}^{\varphi}} = \{\bigcup_{e=1}^{n_{9ijk}}\mathbf{M_{ijke}^{\varphi}}\} = \{\mathbf{M_{ijk1}^{\varphi}},\mathbf{M_{ijk2}^{\varphi}},...,\mathbf{M_{ijkn_{9ijk}}^{\varphi}}\}, \quad (2.47)$$

де $\mathbf{M_{ijke}^{\varphi}} \subseteq \mathbf{M_{ijk}^{\varphi}}$ $(e = \overline{1,n_{9ijk}})$ – e-те значення параметру $\mathbf{M_{ijk}^{\varphi}}$ у межах ijk-ї підмножини, а n_{9ijk} кількість альтернативних значень параметрів ijk-ї підмножини. З урахуванням (2.47) вираз (2.46) можна представити як:

$$\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{n_9}\mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\mathbf{M_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\mathbf{M_{ijk}^{\varphi}}\}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}}\mathbf{M_{ijke}^{\varphi}}\}\}\}\} =$$
$$\{\{\{\{\mathbf{M_{1111}^{\varphi}},\mathbf{M_{1112}^{\varphi}},...,\mathbf{M_{111n_{9ijk}}^{\varphi}}\},\{\mathbf{M_{1121}^{\varphi}},\mathbf{M_{1122}^{\varphi}},...,\mathbf{M_{112n_{9ijk}}^{\varphi}}\},...,$$
$$\{\mathbf{M_{11n_{9ij}1}^{\varphi}},\mathbf{M_{11n_{9ij}2}^{\varphi}},...,\mathbf{M_{11n_{9ij}n_{9ijk}}^{\varphi}}\}\},...,\{\{\mathbf{M_{n_9n_{9i}11}^{\varphi}},\mathbf{M_{n_9n_{9i}12}^{\varphi}},...,\mathbf{M_{n_9n_{9i}1n_{9ijk}}^{\varphi}}\},$$
$$\{\mathbf{M_{n_9n_{9i}21}^{\varphi}},\mathbf{M_{n_9n_{9i}22}^{\varphi}},...,\mathbf{M_{n_9n_{9i}2n_{9ijk}}^{\varphi}}\},...,\{\mathbf{M_{n_9n_{9i}n_{9ij}1}^{\varphi}},\mathbf{M_{n_9n_{9i}n_{9ij}2}^{\varphi}},...,\mathbf{M_{n_9n_{9i}n_{9ij}n_{9ijk}}^{\varphi}}\}\}\}\}. \quad (2.48)$$

Наприклад, при $n_9 = 1$ $(i = 1)$, $n_{91} = 4$ $(j = \overline{1,4})$ та при $n_{91} = 1$ $n_{911} = 1$ $(k = \overline{1,1})$, $n_{9111} = 3$ $(e = \overline{1,3})$, а при $n_{91} = 2$, $n_{91} = 3$, $n_{91} = 4$ та $n_{912} = 0$ $(k = 0)$ формулу (2.48) можна представити як: $\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{1}\mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\mathbf{M_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\{\bigcup_{k=1}^{n_{9ij}}\mathbf{M_{ijk}^{\varphi}}\}\}\} =$

$= \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}}\mathbf{M_{ijke}^{\varphi}}\}\}\}\} = \{\{\{\{\mathbf{M_{1111}^{\varphi}},\mathbf{M_{1112}^{\varphi}},\mathbf{M_{1113}^{\varphi}}\}\},\mathbf{M_{12}^{\varphi}},\mathbf{M_{13}^{\varphi}},\mathbf{M_{14}^{\varphi}}\}\}$, де: $\mathbf{M_{1111}^{\varphi}} =$

«Так»; $\mathbf{M}^{\varphi}_{1112}$ = **«Ні»**; $\mathbf{M}^{\varphi}_{1113}$ = **«Невідомо»**. Підмножину $\mathbf{M}^{\varphi}_{\mathbf{ijke}}$ визначимо як:

$$\mathbf{M}^{\varphi}_{\mathbf{ijke}} = \{\bigcup_{p=1}^{n_{9ijke}} \mathbf{M}^{\varphi}_{\mathbf{ijkep}}\} = \{\mathbf{M}^{\varphi}_{\mathbf{ijke1}}, \mathbf{M}^{\varphi}_{\mathbf{ijke2}}, ..., \mathbf{M}^{\varphi}_{\mathbf{ijken_{9ijke}}}\}, \quad (2.49)$$

де $\mathbf{M}^{\varphi}_{\mathbf{ijkep}} \subseteq \mathbf{M}^{\varphi}_{\mathbf{ijke}}$ $(p = \overline{1,n_{9ijke}})$ – p-те значення параметру $\mathbf{M}^{\varphi}_{\mathbf{ijke}}$ у межах *ijke*-ї підмножини, а n_{9ijke} кількість альтернативних значень параметрів *ijke*-ї підмножини. З урахуванням (2.49) вираз (2.48) можна представити як:

$$\mathbf{M}^{\varphi} = \{\bigcup_{i=1}^{n_9} \mathbf{M}^{\varphi}_{\mathbf{i}}\} = \{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \mathbf{M}^{\varphi}_{\mathbf{ij}}\}\} = \{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \{\bigcup_{k=1}^{n_{9ij}} \mathbf{M}^{\varphi}_{\mathbf{ijk}}\}\}\} = \{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \{\bigcup_{k=1}^{n_{9ij}} \{\bigcup_{e=1}^{n_{9ijk}} \mathbf{M}^{\varphi}_{\mathbf{ijke}}\}\}\}\} =$$

$$\{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \{\bigcup_{k=1}^{n_{9ij}} \{\bigcup_{e=1}^{n_{9ijk}} \{\bigcup_{p=1}^{n_{9ijke}} \mathbf{M}^{\varphi}_{\mathbf{ijkep}}\}\}\}\}\} = \{\{\{\{\{\mathbf{M}^{\varphi}_{\mathbf{11111}}, \mathbf{M}^{\varphi}_{\mathbf{11112}}, ..., \mathbf{M}^{\varphi}_{\mathbf{1111n_{9ijke}}}\},$$

$$\{\mathbf{M}^{\varphi}_{\mathbf{11121}}, \mathbf{M}^{\varphi}_{\mathbf{11122}}, ..., \mathbf{M}^{\varphi}_{\mathbf{1112n_{9ijke}}}\}, ..., \{\mathbf{M}^{\varphi}_{\mathbf{111n_{9ijk}1}}, \mathbf{M}^{\varphi}_{\mathbf{111n_{9ijk}2}}, ..., \mathbf{M}^{\varphi}_{\mathbf{111n_{9ijk}n_{9ijke}}}\}\}, \quad (2.50)$$

$$\{\{\mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}11}}, \mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}12}}, ..., \mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}1n_{9ijke}}}\}, \{\mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}21}}, \mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}22}}, ..., \mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}2n_{9ijke}}}\}, ...,$$

$$\{\mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}n_{9ijk}1}}, \mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}n_{9ijk}2}}, ..., \mathbf{M}^{\varphi}_{\mathbf{n_9n_{9i}n_{9ij}n_{9ijk}n_{9ijke}}}\}\}\}\}.$$

Наприклад, при $n_9 = 1$ $(i = \overline{1})$, $n_{91} = 4$ $(j = \overline{1,4})$ та при $n_{91} = 1$ $n_{911} = 1$ $(k = \overline{1,1})$, $n_{9111} = 3$ $(e = \overline{1,3})$, $n_{91112} = 1$ $(p = \overline{1,1})$, а при $n_{91} = 2$, $n_{91} = 3$, $n_{91} = 4$ та $n_{912} = 0$ $(k = 0)$ формулу (2.50) можна представити як: $\mathbf{M}^{\varphi} = \{\bigcup_{i=1}^{1} \mathbf{M}^{\varphi}_{\mathbf{i}}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{4} \mathbf{M}^{\varphi}_{\mathbf{ij}}\}\} =$

$$\{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{4} \{\bigcup_{k=1}^{n_{9ij}} \mathbf{M}^{\varphi}_{\mathbf{ijk}}\}\}\} == \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{4} \{\bigcup_{k=1}^{n_{9ij}} \{\bigcup_{e=1}^{n_{9ijk}} \mathbf{M}^{\varphi}_{\mathbf{ijke}}\}\}\}\} = \{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \{\bigcup_{k=1}^{n_{9ij}} \{\bigcup_{e=1}^{n_{9ijk}} \{\bigcup_{p=1}^{n_{9ijkp}} \mathbf{M}^{\varphi}_{\mathbf{ijkep}}\}\}\}\}\} = \{\{\{\{\mathbf{M}^{\varphi}_{\mathbf{1111}},$$

$\{\mathbf{M}^{\varphi}_{\mathbf{11121}}\}, \mathbf{M}^{\varphi}_{\mathbf{1113}}\}\}, \mathbf{M}^{\varphi}_{\mathbf{12}}, \mathbf{M}^{\varphi}_{\mathbf{13}}, \mathbf{M}^{\varphi}_{\mathbf{14}}\}\}$, де: $\mathbf{M}^{\varphi}_{\mathbf{11121}}$ = **«Повідомлення наглядового органу не відбулося протягом 72 годин і організація має задокументовану причину».** Підмножину $\mathbf{M}^{\varphi}_{\mathbf{ijkep}}$ визначимо як:

$$\mathbf{M}^{\varphi}_{\mathbf{ijkep}} = \{\bigcup_{x=1}^{n_{9ijkep}} M^{\varphi}_{ijkepx}\} = \{M^{\varphi}_{ijkep1}, M^{\varphi}_{ijkep2}, ..., M^{\varphi}_{ijkepn_{9ijkep}}\}, \quad (2.51)$$

де $M^{\varphi}_{ijkepx} \subseteq \mathbf{M}^{\varphi}_{\mathbf{ijkep}}$ $(x = \overline{1,n_{9ijkep}})$ – x-те значення параметру $\mathbf{M}^{\varphi}_{\mathbf{ijkep}}$ у межах *ijkep*-ї підмножини, а n_{9ijkep} кількість альтернативних значень параметрів *ijkep*-ї підмножини. З урахуванням (2.51) вираз (2.50) можна представити як:

$$\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{n_9} \mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}} \mathbf{M_{ijk}^{\varphi}}\}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}} \mathbf{M_{ijke}^{\varphi}}\}\}\}\} =$$

$$\{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}}\{\bigcup_{p=1}^{n_{9ijke}} \mathbf{M_{ijkep}^{\varphi}}\}\}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}}\{\bigcup_{p=1}^{n_{9ijke}}\{\bigcup_{x=1}^{n_{9ijkep}} M_{ijkepx}^{\varphi}\}\}\}\}\} =$$

$$\{\{\{\{\{\{M_{111111}^{\varphi}, M_{111112}^{\varphi}, ..., M_{11111n_{9ijkep}}^{\varphi}\}, \{M_{111121}^{\varphi}, M_{111122}^{\varphi}, ..., M_{11112n_{9ijkep}}^{\varphi}\}, ...,$$

$$\{M_{1111n_{9ijke}1}^{\varphi}, M_{1111n_{9ijke}2}^{\varphi}, ..., M_{1111n_{9ijke}n_{9ijkep}}^{\varphi}\}\}, ..., \{\{M_{n_9 n_{9i} n_{9ij} n_{9ijk} 11}^{\varphi}, M_{n_9 n_{9i} n_{9ij} n_{9ijk} 12}^{\varphi}, ...,$$

$$M_{n_9 n_{9i} n_{9ij} n_{9ijk} 1n_{9ijkep}}^{\varphi}\}, \{M_{n_9 n_{9i} n_{9ij} n_{9ijk} 21}^{\varphi}, M_{n_9 n_{9i} n_{9ij} n_{9ijk} 22}^{\varphi}, ..., M_{n_9 n_{9i} n_{9ij} n_{9ijk} 2n_{9ijkep}}^{\varphi}\}, ...,$$

$$\{M_{n_9 n_{9i} n_{9ij} n_{9ijk} n_{9ijke} 1}^{\varphi}, M_{n_9 n_{9i} n_{9ij} n_{9ijk} n_{9ijke} 2}^{\varphi}, ..., M_{n_9 n_{9i} n_{9ij} n_{9ijk} n_{9ijke} n_{9ijkep}}^{\varphi}\}\}\}\}\}. \quad (2.52)$$

Наприклад, при $n_9 = 1$ $(i = 1)$, $n_{91} = 4$ $(j = \overline{1,4})$ та при $n_{91} = 1$ $n_{911} = 1$ $(k = \overline{1,1})$, $n_{9111} = 3$ $(e = \overline{1,3})$, $n_{91112} = 1$ $(p = \overline{1,1})$, $n_{911121} = 3$ $(x = \overline{1,3})$, а при $n_{91} = 2$, $n_{91} = 3$, $n_{91} = 4$ та $n_{912} = 0$ $(k = 0)$ формулу (2.52) можна представити як:

$$\mathbf{M^{\varphi}} = \{\bigcup_{i=1}^{1} \mathbf{M_i^{\varphi}}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4} \mathbf{M_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\{\bigcup_{k=1}^{n_{9ij}} \mathbf{M_{ijk}^{\varphi}}\}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{4}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}} \mathbf{M_{ijke}^{\varphi}}\}\}\}\} =$$

$$\{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}}\{\bigcup_{p=1}^{n_{9ijkp}} \mathbf{M_{ijkep}^{\varphi}}\}\}\}\} = \{\bigcup_{i=1}^{n_9}\{\bigcup_{j=1}^{n_{9i}}\{\bigcup_{k=1}^{n_{9ij}}\{\bigcup_{e=1}^{n_{9ijk}}\{\bigcup_{p=1}^{n_{9ijke}}\{\bigcup_{x=1}^{n_{9ijkep}} M_{ijkepx}^{\varphi}\}\}\}\}\} = \quad (2.53)$$

$$\{\{\{\{M_{1111}^{\varphi}, \{\{M_{111211}^{\varphi}, M_{11122}^{\varphi}, M_{11123}^{\varphi}\}\}, M_{1113}^{\varphi}\}\}, M_{12}^{\varphi}, M_{13}^{\varphi}, M_{14}^{\varphi}\}\}.$$

Одинадцятий компонент $\mathbf{ME^{\varphi}}$ – **«Відповідність заходам»**, визначається:

$$\mathbf{ME^{\varphi}} = \{\bigcup_{i=1}^{n_{10}} \mathbf{ME_i^{\varphi}}\} = \{\mathbf{ME_1^{\varphi}}, \mathbf{ME_2^{\varphi}}, ..., \mathbf{ME_{n_{10}}^{\varphi}}\}, \quad (2.54)$$

де $\mathbf{ME^{\varphi}}$ – множина критеріїв відповідності заходам, $\mathbf{ME_i^{\varphi}} \subseteq \mathbf{ME^{\varphi}}$ $(i = \overline{1,n_{10}})$ і-та підмножина заходів раніше призначених проти контролера/оператора, а n_{10} – кількість таких підмножин. Наприклад, при $n_{10} = 1$ $(i = 1)$ формулу (2.54) можна представити як: $\mathbf{ME^{\varphi}} = \{\bigcup_{i=1}^{1} \mathbf{ME_i^{\varphi}}\} = \{\mathbf{ME_1^{\varphi}}\}$, де підмножина $\mathbf{ME_1^{\varphi}} \subseteq \mathbf{ME^{\varphi}}$ відповідно характеризує значення: $\mathbf{ME_1^{\varphi}}$ **= «Застосовано коригувальні заходи відповідно до Статті 58 (a-h та j)»**. Підмножину $\mathbf{ME_i^{\varphi}}$ визначимо як [58, 59]:

$$\mathbf{ME_i^{\varphi}} = \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}^{\varphi}}\} = \{\mathbf{ME_{i1}^{\varphi}}, \mathbf{ME_{i2}^{\varphi}}, ..., \mathbf{ME_{in_{10i}}^{\varphi}}\}, \quad (2.55)$$

де $\mathbf{ME_{ij}^{\varphi}} \subseteq \mathbf{ME_i^{\varphi}}$ $(j = \overline{1,n_{10i}})$ – j-те значення параметру $\mathbf{ME_i^{\varphi}}$ у межах i-ї підмножини, а n_{10i} кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.55) вираз (2.54) можна представити як:

$$\mathbf{ME^{\varphi}} = \{\bigcup_{i=1}^{n_{10}} \mathbf{ME_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}^{\varphi}}\}\} = \{\{\mathbf{ME_{11}^{\varphi}}, \mathbf{ME_{12}^{\varphi}}, ..., \mathbf{ME_{1n_{10i}}^{\varphi}}\},$$
$$\{\mathbf{ME_{21}^{\varphi}}, \mathbf{ME_{22}^{\varphi}}, ..., \mathbf{ME_{2n_{10i}}^{\varphi}}\}, ..., \{\mathbf{ME_{n_{10}1}^{\varphi}}, \mathbf{ME_{n_{10}2}^{\varphi}}, ..., \mathbf{ME_{n_{10}n_{10i}}^{\varphi}}\}\}. \quad (2.56)$$

Наприклад, при $n_{10} = 1$ $(i = 1)$, $n_{101} = 2$ $(j = \overline{1,2})$ формулу (2.56) можна представити як: $\mathbf{ME_i^{\varphi}} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}^{\varphi}}\}\} = \{\{\mathbf{ME_{11}^{\varphi}}, \mathbf{ME_{12}^{\varphi}}\}\}$, де: $\mathbf{ME_{11}^{\varphi}}$ = **«Так»**; $\mathbf{ME_{12}^{\varphi}}$ = **«Ні»**. Підмножину $\mathbf{ME_{ij}^{\varphi}}$ визначимо як:

$$\mathbf{ME_{ij}^{\varphi}} = \{\bigcup_{k=1}^{n_{10ij}} \mathbf{ME_{ijk}^{\varphi}}\} = \{\mathbf{ME_{ij1}^{\varphi}}, \mathbf{ME_{ij2}^{\varphi}}, ..., \mathbf{ME_{ijn_{10ij}}^{\varphi}}\}, \quad (2.57)$$

де $\mathbf{ME_{ijk}^{\varphi}} \subseteq \mathbf{ME_{ij}^{\varphi}}$ $(k = \overline{1,n_{10ij}})$ – k-те значення параметру $\mathbf{ME_{ij}^{\varphi}}$ у межах ij-ї підмножини, а n_{10ij} кількість альтернативних значень параметрів ij-ї підмножини. З урахуванням (2.57) вираз (2.56) можна представити як:

$$\mathbf{ME^{\varphi}} = \{\bigcup_{i=1}^{n_{10}} \mathbf{ME_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \{\bigcup_{k=1}^{n_{10ij}} \mathbf{ME_{ijk}^{\varphi}}\}\}\} =$$
$$\{\{\{\mathbf{ME_{111}^{\varphi}}, \mathbf{ME_{112}^{\varphi}}, ..., \mathbf{ME_{11n_{10ij}}^{\varphi}}\}, \{\mathbf{ME_{121}^{\varphi}}, \mathbf{ME_{122}^{\varphi}}, ..., \mathbf{ME_{12n_{10ij}}^{\varphi}}\}, ...,$$
$$\{\mathbf{ME_{1n_{10i}1}^{\varphi}}, \mathbf{ME_{1n_{10i}2}^{\varphi}}, ..., \mathbf{ME_{1n_{10i}n_{10ij}}^{\varphi}}\}\}, ..., \{\{\mathbf{ME_{n_{10}11}^{\varphi}}, \mathbf{ME_{n_{10}12}^{\varphi}}, ..., \mathbf{ME_{n_{10}1n_{10ij}}^{\varphi}}\},$$
$$\{\mathbf{ME_{n_{10}21}^{\varphi}}, \mathbf{ME_{n_{10}22}^{\varphi}}, ..., \mathbf{ME_{n_{10}2n_{10ij}}^{\varphi}}\}, ..., \{\mathbf{ME_{n_{10}n_{10i}1}^{\varphi}}, \mathbf{ME_{n_{10}n_{10i}2}^{\varphi}}, ..., \mathbf{ME_{n_{10}n_{10i}n_{10ij}}^{\varphi}}\}\}\}. \quad (2.58)$$

Наприклад, при $n_{10} = 1$ $(i = 1)$, $n_{101} = 2$ $(j = \overline{1,2})$ та при $n_{102} = 2$ $n_{1011} = 0$ $(k = 0)$, а при $n_{101} = 1$ $n_{1011} = 1$ $(k = \overline{1,1})$ формулу (2.58) можна представити як: $\mathbf{ME^{\varphi}}$ = $\{\bigcup_{i=1}^{1} \mathbf{ME_i^{\varphi}}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{2} \mathbf{ME_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{2} \{\bigcup_{k=1}^{n_{10ij}} \mathbf{ME_{ijk}^{\varphi}}\}\}\} = \{\{\{\mathbf{ME_{111}^{\varphi}}\}, \mathbf{ME_{12}^{\varphi}}\}\}$, де: $\mathbf{ME_{111}^{\varphi}}$ = **«Коригувальні заходи відповідно до Статті 58 (a-h та j) затверджено та**

передбачено Плани відновлення». Підмножину $\mathbf{ME^{\varphi}_{ijk}}$ визначимо як:

$$\mathbf{ME^{\varphi}_{ijk}} = \{\bigcup_{e=1}^{n_{10ijk}} ME^{\varphi}_{ijke}\} = \{ME^{\varphi}_{ijk1}, ME^{\varphi}_{ijk2}, ..., ME^{\varphi}_{ijkn_{10ijk}}\}, \quad (2.59)$$

де $ME^{\varphi}_{ijke} \subseteq \mathbf{ME^{\varphi}_{ijk}}$ $(e = \overline{1,n_{10ijk}})$ – e-те значення параметру $\mathbf{ME^{\varphi}_{ijk}}$ у межах ijk-ї підмножини, а n_{10ijk} кількість альтернативних значень параметрів ijk-ї підмножини. З урахуванням (2.59) вираз (2.58) можна представити як:

$$\mathbf{ME^{\varphi}} = \{\bigcup_{i=1}^{n_{10}} \mathbf{ME^{\varphi}_{i}}\} = \{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME^{\varphi}_{ij}}\}\} = \{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \{\bigcup_{k=1}^{n_{10ij}} \mathbf{ME^{\varphi}_{ijk}}\}\}\} =$$

$$\{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \{\bigcup_{k=1}^{n_{10ij}} \{\bigcup_{e=1}^{n_{10ijk}} ME^{\varphi}_{ijke}\}\}\}\} = \{\{\{\{ME^{\varphi}_{1111}, ME^{\varphi}_{1112}, ..., ME^{\varphi}_{111n_{10ijk}}\},$$

$$\{ME^{\varphi}_{1121}, ME^{\varphi}_{1122}, ..., ME^{\varphi}_{112n_{10ijk}}\}, ..., \{ME^{\varphi}_{11n_{10ij}1}, ME^{\varphi}_{11n_{10ij}2}, ..., ME^{\varphi}_{11n_{10ij}n_{10ijk}}\}\}, ...,$$

$$\{\{ME^{\varphi}_{n_{10}n_{10i}11}, ME^{\varphi}_{n_{10}n_{10i}12}, ..., ME^{\varphi}_{n_{10}n_{10i}1n_{10ijk}}\}, \{ME^{\varphi}_{n_{10}n_{10i}21}, ME^{\varphi}_{n_{10}n_{10i}22}, ..., ME^{\varphi}_{n_{10}n_{10i}2n_{10ijk}}\},$$

$$..., \{ME^{\varphi}_{n_{10}n_{10i}n_{10ij}1}, ME^{\varphi}_{n_{10}n_{10i}n_{10ij}2}, ..., ME^{\varphi}_{n_{10}n_{10i}n_{10ij}n_{10ijk}}\}\}\}\}. \quad (2.60)$$

Наприклад, при $n_{10} = 1$ $(i = 1)$, $n_{101} = 2$ $(j = \overline{1,2})$, та при $n_{102} = 2$ $n_{1011} = 0$ $(k = 0)$, а при $n_{101} = 1$ $n_{1011} = 1$ $(k = \overline{1,1})$, $n_{10111} = 3$ $(e = \overline{1,3})$ формулу (2.60) можна представити як: $\mathbf{ME^{\varphi}} = \{\bigcup_{i=1}^{1} \mathbf{ME^{\varphi}_{i}}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{2} \mathbf{ME^{\varphi}_{ij}}\}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{2} \{\bigcup_{k=1}^{n_{10ij}} \mathbf{ME^{\varphi}_{ijk}}\}\}\} =$

$$\{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \{\bigcup_{k=1}^{n_{10ij}} \{\bigcup_{e=1}^{n_{10ijk}} ME^{\varphi}_{ijke}\}\}\}\} = \{\{\{\{ME^{\varphi}_{1111}, ME^{\varphi}_{1112}, ME^{\varphi}_{1113}\}\}, ME^{\varphi}_{12}\}\}. \quad (2.61)$$

Дванадцятий компонент $\mathbf{AD^{\varphi}}$ – **«Дотримання кодексів»**, визначається виразом:

$$\mathbf{AD^{\varphi}} = \{\bigcup_{i=1}^{n_{11}} \mathbf{AD^{\varphi}_{i}}\} = \{\mathbf{AD^{\varphi}_{1}}, \mathbf{AD^{\varphi}_{2}}, ..., \mathbf{AD^{\varphi}_{n_{11}}}\}, \quad (2.62)$$

де $\mathbf{AD^{\varphi}}$ – множина критеріїв дотримання кодексів поведінки, $\mathbf{AD^{\varphi}_{i}} \subseteq \mathbf{AD^{\varphi}}$ $(i = \overline{1,n_{11}})$ i-та підмножина затверджених кодексів поведінки, а n_{11} – кількість таких підмножин. Наприклад, $n_{11} = 2$ $(i = \overline{1,2})$ формулу (2.62) можна представити як:

$\mathbf{AD^{\varphi}} = \{\bigcup_{i=1}^{2} \mathbf{AD_i^{\varphi}}\} = \{\mathbf{AD_1^{\varphi}}, \mathbf{AD_2^{\varphi}}\}$, де підмножини $\mathbf{AD_1^{\varphi}} \subseteq \mathbf{AD^{\varphi}}$ та $\mathbf{AD_2^{\varphi}} \subseteq \mathbf{AD^{\varphi}}$ відповідно характеризують значення: $\mathbf{AD_1^{\varphi}}$ = **«Наявність Кодексу поведінки працівників в організації (Стаття 40)»** та $\mathbf{AD_2^{\varphi}}$ = **«Наявність державного механізму сертифікації засобів захисту ПД»**. Підмножину $\mathbf{AD_i^{\varphi}}$ визначимо як:

$$\mathbf{AD_i^{\varphi}} = \{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}^{\varphi}}\} = \{\mathbf{AD_{i1}^{\varphi}}, \mathbf{AD_{i2}^{\varphi}}, ..., \mathbf{AD_{in_{11i}}^{\varphi}}\}, \quad (2.63)$$

де $\mathbf{AD_{ij}^{\varphi}} \subseteq \mathbf{AD_i^{\varphi}}$ ($j = \overline{1,n_{11i}}$) – j-те значення параметру $\mathbf{AD_i^{\varphi}}$ у межах i-ї підмножини, а n_{11i} кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.63) вираз (2.62) можна представити як: $\mathbf{AD^{\varphi}} = \{\bigcup_{i=1}^{n_{11}} \mathbf{AD_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{11}} \{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}^{\varphi}}\}\} = \{\{\mathbf{AD_{11}^{\varphi}}, \mathbf{AD_{12}^{\varphi}}, ..., \mathbf{AD_{1n_{11i}}^{\varphi}}\}, \{\mathbf{AD_{21}^{\varphi}}, \mathbf{AD_{22}^{\varphi}}, ..., \mathbf{AD_{2n_{11i}}^{\varphi}}\}, ..., \{\mathbf{AD_{n_{11}1}^{\varphi}}, \mathbf{AD_{n_{11}2}^{\varphi}}, ..., \mathbf{AD_{n_{11}n_{11i}}^{\varphi}}\}\}$. (2.64)

Наприклад, при $n_{11} = 2$ ($i = \overline{1,2}$), а саме, при $n_{11} = 1$ $n_{111} = 1$ (дані отримуються із відповідей користувача на 8 запитання компоненти $\mathbf{R^{\varphi}}$), а при $n_{11} = 2$ $n_{112} = 2$ ($j = \overline{1,2}$) формулу (2.64) можна представити як: $\mathbf{AD_i^{\varphi}} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}^{\varphi}}\}\} = \{\{\mathbf{AD_{11}^{\varphi}}\}, \{\mathbf{AD_{21}^{\varphi}}, \mathbf{AD_{22}^{\varphi}}\}\}$, де: $\mathbf{AD_{11}^{\varphi}}$ = **«Так/Ні»** (залежить від параметра $\mathbf{R_8^{\varphi}}$); $\mathbf{AD_{21}^{\varphi}}$ = **«Так»**; $\mathbf{AD_{22}^{\varphi}}$ = **«Ні».** Підмножину $\mathbf{AD_{ij}}$ визначимо як [58]:

$$\mathbf{AD_{ij}^{\varphi}} = \{\bigcup_{k=1}^{n_{11ij}} \mathbf{AD_{ijk}^{\varphi}}\} = \{\mathbf{AD_{ij1}^{\varphi}}, \mathbf{AD_{ij2}^{\varphi}}, ..., \mathbf{AD_{ijn_{11ij}}^{\varphi}}\}, \quad (2.65)$$

де $\mathbf{AD_{ijk}^{\varphi}} \subseteq \mathbf{AD_{ij}^{\varphi}}$ ($k = \overline{1,n_{11ij}}$) – k-те значення параметру $\mathbf{AD_{ij}^{\varphi}}$ у межах ij-ї підмножини, а n_{11ij} кількість альтернативних значень параметрів ij-ї підмножини. З урахуванням (2.65) вираз (2.64) можна представити як:

$$\mathbf{AD^{\varphi}} = \{\bigcup_{i=1}^{n_{11}} \mathbf{AD_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}}\{\bigcup_{k=1}^{n_{11ij}} \mathbf{AD_{ijk}^{\varphi}}\}\}\} =$$

$$\{\{\{\mathbf{AD_{111}^{\varphi}}, \mathbf{AD_{112}^{\varphi}}, ..., \mathbf{AD_{11n_{11ij}}^{\varphi}}\}, \{\mathbf{AD_{121}^{\varphi}}, \mathbf{AD_{122}^{\varphi}}, ..., \mathbf{AD_{12n_{11ij}}^{\varphi}}\}, ...,$$

$$\{\mathbf{AD_{1n_{11i}1}^{\varphi}}, \mathbf{AD_{1n_{11i}2}^{\varphi}}, ..., \mathbf{AD_{1n_{11i}n_{11ij}}^{\varphi}}\}\}, ..., \{\{\mathbf{AD_{n_{11}11}^{\varphi}}, \mathbf{AD_{n_{11}12}^{\varphi}}, ..., \mathbf{AD_{n_{11}1n_{11ij}}^{\varphi}}\},$$

$$\{\mathbf{AD_{n_{11}21}^{\varphi}}, \mathbf{AD_{n_{11}22}^{\varphi}}, ..., \mathbf{AD_{n_{11}2n_{11ij}}^{\varphi}}\}, ..., \{\mathbf{AD_{n_{11}n_{11i}1}^{\varphi}}, \mathbf{AD_{n_{11}n_{11i}2}^{\varphi}}, ..., \mathbf{AD_{n_{11}n_{11i}n_{11ij}}^{\varphi}}\}\}\}. \quad (2.66)$$

Наприклад, при $n_{11} = 2$ $(i = \overline{1,2})$, а саме, при $n_{11} = 1$ $n_{111} = 1$ (дані отримуються із відповідей користувача на 8 запитання компоненту $\mathbf{R^{\varphi}}$), а при $n_{11} = 2$ $n_{112} = 2$ $(j = \overline{1,2})$, $n_{1111} = 1$ $(k = \overline{1,1})$, формулу (2.66) можна представити як:

$$\mathbf{AD^{\varphi}} = \{\bigcup_{i=1}^{2} \mathbf{AD_i^{\varphi}}\} = \{\bigcup_{i=1}^{2}\{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{n_{11i}}\{\bigcup_{k=1}^{n_{11ij}} \mathbf{AD_{ijk}^{\varphi}}\}\}\} = \{\{\mathbf{AD_{11}^{\varphi}}\}, \{\{\mathbf{AD_{211}^{\varphi}}\}, \mathbf{AD_{22}^{\varphi}}\}\},$$

де: $\mathbf{AD_{211}^{\varphi}}$ = **«Організація сертифікована (знаходиться в процесі сертифікації)».** Підмножину $\mathbf{AD_{ijk}^{\varphi}}$ визначимо як:

$$\mathbf{AD_{ijk}^{\varphi}} = \{\bigcup_{e=1}^{n_{11ijk}} AD_{ijke}^{\varphi}\} = \{AD_{ijk1}^{\varphi}, AD_{ijk2}^{\varphi}, ..., AD_{ijkn_{11ijk}}^{\varphi}\}, \quad (2.67)$$

де $AD_{ijke}^{\varphi} \subseteq \mathbf{AD_{ijk}^{\varphi}}$ $(e = \overline{1,n_{11ijk}})$ – e-те значення параметру $\mathbf{AD_{ijk}^{\varphi}}$ у межах ijk-ї підмножини, а n_{11ijk} кількість альтернативних значень параметрів ijk-ї підмножини. З урахуванням (2.67) вираз (2.66) можна представити як:

$$\mathbf{AD^{\varphi}} = \{\bigcup_{i=1}^{n_{11}} \mathbf{AD_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}}\{\bigcup_{k=1}^{n_{11ij}} \mathbf{AD_{ijk}^{\varphi}}\}\}\} =$$

$$\{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}}\{\bigcup_{k=1}^{n_{11ij}}\{\bigcup_{e=1}^{n_{11ijk}} AD_{ijke}^{\varphi}\}\}\}\} = \{\{\{\{AD_{1111}^{\varphi}, AD_{1112}^{\varphi}, ..., AD_{111n_{11ijk}}^{\varphi}\},$$

$$\{AD_{1121}^{\varphi}, AD_{1122}^{\varphi}, ..., AD_{112n_{11ijk}}^{\varphi}\}, ..., \{AD_{11n_{11ij}1}^{\varphi}, AD_{11n_{11ij}2}^{\varphi}, ..., AD_{11n_{11ij}n_{11ijk}}^{\varphi}\}\}, ...,$$

$$\{\{AD_{n_{11}n_{11i}11}^{\varphi}, AD_{n_{11}n_{11i}12}^{\varphi}, ..., AD_{n_{11}n_{11i}1n_{11ijk}}^{\varphi}\}, \{AD_{n_{11}n_{11i}21}^{\varphi}, AD_{n_{11}n_{11i}22}^{\varphi}, ..., AD_{n_{1i}n_{11i}2n_{11ijk}}^{\varphi}\},$$

$$..., \{AD_{n_{11}n_{1i}n_{11ij}1}^{\varphi}, AD_{n_{11}n_{1i}n_{1!ij}2}^{\varphi}, ..., AD_{n_{11}n_{11i}n_{11ij}n_{11ijk}}^{\varphi}\}\}\}\}. \quad (2.68)$$

Наприклад, при $n_{11} = 2$ $(i = \overline{1,2})$, а саме, при $n_{11} = 1$ $n_{111} = 1$ (дані отримуються із відповідей користувача на 8 запитання компоненту $\mathbf{R^{\varphi}}$), а при

$n_{11}=2$ $n_{112}=2$ $(j=\overline{1,2})$, $n_{1111}=1$ $(k=\overline{1,1})$, $n_{11111}=3$ $(e=\overline{1,3})$ формулу (2.68) можна представити як: $\mathbf{AD^{\varphi}}=\{\bigcup_{i=1}^{2}\mathbf{AD_i^{\varphi}}\}=\{\bigcup_{i=1}^{2}\{\bigcup_{j=1}^{2}\mathbf{AD_{ij}^{\varphi}}\}\}=\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\{\bigcup_{k=1}^{n_{11ij}}\mathbf{AD_{ijk}^{\varphi}}\}\}\}=$

$$\{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}}\{\bigcup_{k=1}^{n_{11ij}}\{\bigcup_{e=1}^{n_{11jk}}AD_{ijke}^{\varphi}\}\}\}\}=\{\{AD_{11}^{\varphi}\},\{\{\{AD_{2111}^{\varphi},AD_{2112}^{\varphi},AD_{2113}^{\varphi}\}\},AD_{22}^{\varphi}\}\}. \quad (2.69)$$

Тринадцятий компонент $\mathbf{F^{\varphi}}$ – **«Визначаючий чинник»**, визначається виразом:

$$\mathbf{F^{\varphi}}=\{\bigcup_{i=1}^{n_{12}}\mathbf{F_i^{\varphi}}\}=\{\mathbf{F_1^{\varphi}},\mathbf{F_2^{\varphi}},...,\mathbf{F_{n_{12}}^{\varphi}}\}, \quad (2.70)$$

де $\mathbf{F^{\varphi}}$ – множина критеріїв чиннику порушення, $\mathbf{F_i^{\varphi}}\subseteq\mathbf{F^{\varphi}}$ $(i=\overline{1,n_{12}})$ i-та підмножина чинників порушення, а n_{12} – кількість таких підмножин. Наприклад, $n_{12}=2$ $(i=\overline{1,2})$ формулу (2.70) можна представити як: $\mathbf{F^{\varphi}}=\{\bigcup_{i=1}^{2}\mathbf{F_i^{\varphi}}\}=\{\mathbf{F_1^{\varphi}},\mathbf{F_2^{\varphi}}\}$, де підмножини $\mathbf{F_1^{\varphi}}\subseteq\mathbf{F^{\varphi}}$ та $\mathbf{F_2^{\varphi}}\subseteq\mathbf{F^{\varphi}}$ відповідно характеризують значення: $\mathbf{F_1^{\varphi}}$ = **«Отримано фінансову вигоду від витоку ПД»**; $\mathbf{F_2^{\varphi}}$ = **«Отримано фінансовий збиток від витоку ПД»**. Підмножину $\mathbf{F_i^{\varphi}}$ визначимо як [58, 59]:

$$\mathbf{F_i^{\varphi}}=\{\bigcup_{j=1}^{n_{12i}}\mathbf{F_{ij}^{\varphi}}\}=\{\mathbf{F_{i1}^{\varphi}},\mathbf{F_{i2}^{\varphi}},...,\mathbf{F_{in_{12i}}^{\varphi}}\}, \quad (2.71)$$

де $\mathbf{F_{ij}^{\varphi}}\subseteq\mathbf{F_i^{\varphi}}$ $(j=\overline{1,n_{12i}})$ – j-те значення параметру $\mathbf{F_i^{\varphi}}$ у межах i-ї підмножини, а n_{12i} кількість альтернативних значень параметрів i-ї підмножини. З урахуванням (2.71) вираз (2.70) можна представити як: $\mathbf{F^{\varphi}}=\{\bigcup_{i=1}^{n_{12}}\mathbf{F^{\varphi}}_{\mathbf{i}}\}=\{\bigcup_{i=1}^{n_{12}}\{\bigcup_{j=1}^{n_{12i}}\mathbf{F^{\varphi}}_{\mathbf{ij}}\}\}=$

$$\{\{\mathbf{F_{11}^{\varphi}},\mathbf{F_{12}^{\varphi}},...,\mathbf{F_{1n_{12i}}^{\varphi}}\},\{\mathbf{F_{21}^{\varphi}},\mathbf{F_{22}^{\varphi}},...,\mathbf{F_{2n_{12i}}^{\varphi}}\},...,\{\mathbf{F_{n_{12}1}^{\varphi}},\mathbf{F_{n_{12}2}^{\varphi}},...,\mathbf{F_{n_{12}n_{12i}}^{\varphi}}\}\}. \quad (2.72)$$

Наприклад, при $n_{12}=2$ $(i=\overline{1,2})$, $n_{121}=3$ $(j=\overline{1,3})$ формулу (2.72) можна представити як: $\mathbf{F_i^{\varphi}}=\{\bigcup_{i=1}^{2}\{\bigcup_{j=1}^{n_{12i}}\mathbf{F_{ij}^{\varphi}}\}\}=\{\{\mathbf{F_{11}^{\varphi}},\mathbf{F_{12}^{\varphi}},\mathbf{F_{13}^{\varphi}}\},\{\mathbf{F_{21}^{\varphi}},\mathbf{F_{22}^{\varphi}},\mathbf{F_{23}^{\varphi}}\}\}$, де: $\mathbf{F_{11}^{\varphi}}=\mathbf{F_{21}^{\varphi}}=$ **«Так»**; $\mathbf{F_{12}^{\varphi}}=\mathbf{F_{22}^{\varphi}}=$ **«Ні»**; $\mathbf{F_{13}^{\varphi}}=\mathbf{F_{23}^{\varphi}}=$ **«Невідомо»**. Підмножину $\mathbf{F_{ij}^{\varphi}}$ визначимо як:

$$\mathbf{F_{ij}^{\varphi}} = \{\bigcup_{k=1}^{n_{12ij}} \mathbf{F_{ijk}^{\varphi}}\} = \{\mathbf{F_{ij1}^{\varphi}}, \mathbf{F_{ij2}^{\varphi}}, ..., \mathbf{F_{ijn_{12ij}}^{\varphi}}\}, \tag{2.73}$$

де $\mathbf{F_{ijk}^{\varphi}} \subseteq \mathbf{F_{ij}^{\varphi}}$ $(k = \overline{1,n_{12ij}})$ – k-те значення параметру $\mathbf{F_{ij}^{\varphi}}$ у межах ij-ї підмножини, а n_{12ij} кількість альтернативних значень параметрів ij-ї підмножини. З урахуванням (2.73) вираз (2.72) можна представити як: $\mathbf{F^{\varphi}} = \{\bigcup_{i=1}^{n_{12}} \mathbf{F_{i}^{\varphi}}\} = \{\bigcup_{i=1}^{n_{12}} \{\bigcup_{j=1}^{n_{12i}} \mathbf{F_{ij}^{\varphi}}\}\} =$

$$\begin{aligned}\{\bigcup_{i=1}^{n_{12}} \{\bigcup_{j=1}^{n_{12i}} \{\bigcup_{k=1}^{n_{12ij}} \mathbf{F_{ijk}^{\varphi}}\}\}\} = \{\{\{\mathbf{F_{111}^{\varphi}}, \mathbf{F_{112}^{\varphi}}, ..., \mathbf{F_{11n_{12ij}}^{\varphi}}\}, \{\mathbf{F_{121}^{\varphi}}, \mathbf{F_{122}^{\varphi}}, ..., \mathbf{F_{12n_{12ij}}^{\varphi}}\}, ...,\\ \{\mathbf{F_{1n_{12i}1}^{\varphi}}, \mathbf{F_{1n_{12i}2}^{\varphi}}, ..., \mathbf{F_{1n_{12i}n_{12ij}}^{\varphi}}\}\}, ..., \{\{\mathbf{F_{n_{12}11}^{\varphi}}, \mathbf{F_{n_{12}12}^{\varphi}}, ..., \mathbf{F_{n_{12}1n_{12ij}}^{\varphi}}\},\\ \{\mathbf{F_{n_{12}21}^{\varphi}}, \mathbf{F_{n_{12}22}^{\varphi}}, ..., \mathbf{F_{n_{12}2n_{12ij}}^{\varphi}}\}, ..., \{\mathbf{F_{n_{12}n_{12i}1}^{\varphi}}, \mathbf{F_{n_{12}n_{12i}2}^{\varphi}}, ..., \mathbf{F_{n_{12}n_{12i}n_{12ij}}^{\varphi}}\}\}\}.\end{aligned} \tag{2.74}$$

Наприклад, при $n_{12} = 2$ $(i = \overline{1,2})$, $n_{121} = 3$ $(j = \overline{1,3})$, $n_{1211} = 2$ $(k = \overline{1,2})$ формулу (2.74) можна представити як: $\mathbf{F^{\varphi}} = \{\bigcup_{i=1}^{2} \mathbf{F_{i}^{\varphi}}\} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{12i}} \mathbf{F_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{12i}} \{\bigcup_{k=1}^{n_{12ij}} \mathbf{F_{ijk}^{\varphi}}\}\}\} =$

$\{\{\{\mathbf{F_{111}^{\varphi}}\}, \mathbf{F_{12}^{\varphi}}, \mathbf{F_{13}^{\varphi}}\}, \{\{\mathbf{F_{211}^{\varphi}}\}, \mathbf{F_{22}^{\varphi}}, \mathbf{F_{23}^{\varphi}}\}\}$, де: $\mathbf{F_{111}^{\varphi}}$ = **«Величина фінансової вигоди»**; $\mathbf{F_{211}^{\varphi}}$ = **«Величина фінансового збитку».** Підмножину $\mathbf{F_{ijk}^{\varphi}}$ визначимо як:

$$\mathbf{F_{ijk}^{\varphi}} = \{\bigcup_{e=1}^{n_{12ijk}} F_{ijke}^{\varphi}\} = \{F_{ijk1}^{\varphi}, F_{ijk2}^{\varphi}, ..., F_{ijkn_{12ijk}}^{\varphi}\}, \tag{2.75}$$

де $F_{ijke}^{\varphi} \subseteq \mathbf{F_{ijk}^{\varphi}}$ $(e = \overline{1,n_{12ijk}})$ – e-те значення параметру $\mathbf{F_{ijk}^{\varphi}}$ у межах ijk-ї підмножини, а n_{12ijk} кількість альтернативних значень параметрів ijk-ї підмножини. З урахуванням (2.75) вираз (2.74) можна представити як: $\mathbf{F^{\varphi}} = \{\bigcup_{i=1}^{n_{12}} \mathbf{F_{i}^{\varphi}}\} = \{\bigcup_{i=1}^{n_{12}} \{\bigcup_{j=1}^{n_{12i}} \mathbf{F_{ij}^{\varphi}}\}\} =$

$$\begin{aligned}\{\bigcup_{i=1}^{n_{12}} \{\bigcup_{j=1}^{n_{12i}} \{\bigcup_{k=1}^{n_{12ij}} \mathbf{F_{ijk}^{\varphi}}\}\}\} = \{\bigcup_{i=1}^{n_{12}} \{\bigcup_{j=1}^{n_{12i}} \{\bigcup_{k=1}^{n_{12ij}} \{\bigcup_{e=1}^{n_{12jk}} F_{ijke}^{\varphi}\}\}\}\} = \{\{\{\{F_{1111}^{\varphi}, F_{1112}^{\varphi}, ..., F_{111n_{12ijk}}^{\varphi}\},\\ \{F_{1121}^{\varphi}, F_{1122}^{\varphi}, ..., F_{112n_{12ijk}}^{\varphi}\}, ..., \{F_{11n_{12ij}1}^{\varphi}, F_{11n_{12ij}2}^{\varphi}, ..., F_{11n_{12ij}n_{12ijk}}^{\varphi}\}\}, ...,\\ \{\{F_{n_{12}n_{12i}11}^{\varphi}, F_{n_{12}n_{12i}12}^{\varphi}, ..., F_{n_{12}n_{12i}1n_{12ijk}}^{\varphi}\}, \{F_{n_{12}n_{12i}21}^{\varphi}, F_{n_{12}n_{12i}22}^{\varphi}, ..., F_{n_{12}n_{12i}2n_{12ijk}}^{\varphi}\}, ...,\\ \{F_{n_{12}n_{12i}n_{12ij}1}^{\varphi}, F_{n_{12}n_{12i}n_{12ij}2}^{\varphi}, ..., F_{n_{12}n_{12i}n_{12ij}n_{12ijk}}^{\varphi}\}\}\}\}.\end{aligned} \tag{2.76}$$

Наприклад, при $n_{12} = 2\ (i = \overline{1,2})$, $n_{121} = 3\ (j = \overline{1,3})$, $n_{1211} = 2\ (k = \overline{1,2})$ та $n_{12111} = 5\ (e = \overline{1,5})$ формулу (2.76) можна представити як: $\mathbf{F^{\varphi}} = \{\bigcup_{i=1}^{2} \mathbf{F_i^{\varphi}}\} =$

$$\{\bigcup_{i=1}^{2}\{\bigcup_{j=1}^{3}\mathbf{F_{ij}^{\varphi}}\}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{2}\{\bigcup_{k=1}^{n_{11ij}}\mathbf{F_{ijk}^{\varphi}}\}\}\} = \{\bigcup_{i=1}^{n_{11}}\{\bigcup_{j=1}^{n_{11i}}\{\bigcup_{k=1}^{n_{11ij}}\{\bigcup_{e=1}^{n_{11jk}} F_{ijke}^{\varphi}\}\}\}\} = \{\{\{\{F_{1111}^{\varphi}, F_{1112}^{\varphi}, F_{1113}^{\varphi},$$

$$F_{1114}^{\varphi}, F_{1115}^{\varphi}, F_{1116}^{\varphi}\}\}, F_{12}^{\varphi}, F_{13}^{\varphi}\}, \{\{\{F_{2111}^{\varphi}, F_{2112}^{\varphi}, F_{2113}^{\varphi}, F_{2114}^{\varphi}, F_{2115}^{\varphi}, F_{2116}^{\varphi}\}\}, F_{22}^{\varphi}, F_{23}^{\varphi}\}\}. \quad (2.77)$$

Чотирнадцятий компонент $\mathbf{RE^{\varphi}}$ – **«Превентивні рекомендації»**. Вони вказуються для всіх компонент від 3 до 13. В такому разі змінна n_{13} є константою та становить 11 підмножин. Дана компонента визначається виразом [58, 59]:

$$\mathbf{RE^{\varphi}} = \{\bigcup_{i=1}^{n_{13}} \mathbf{RE_i^{\varphi}}\} = \{\mathbf{RE_1^{\varphi}}, \mathbf{RE_2^{\varphi}}, ..., \mathbf{RE_{n_{13}}^{\varphi}}\}, \quad (2.78)$$

де $\mathbf{RE^{\varphi}}$ – множина рекомендацій, $\mathbf{RE_i^{\varphi}} \subseteq \mathbf{RE^{\varphi}}$ $(i = \overline{1,n_{13}})$ і-та підмножина компонент кортежу, а n_{13} кількість таких підмножин. Оскільки $n_{13} = 11\ (i = \overline{1,11})$, то формулу (2.78) можна представити як: $\mathbf{RE^{\varphi}} = \{\bigcup_{i=1}^{11} \mathbf{RE_i^{\varphi}}\} = \{\mathbf{RE_1^{\varphi}}, \mathbf{RE_2^{\varphi}}, \mathbf{RE_3^{\varphi}}, \mathbf{RE_4^{\varphi}},$ $\mathbf{RE_5^{\varphi}}, \mathbf{RE_6^{\varphi}}, \mathbf{RE_7^{\varphi}}, \mathbf{RE_8^{\varphi}}, \mathbf{RE_9^{\varphi}}, \mathbf{RE_{10}^{\varphi}}, \mathbf{RE_{11}^{\varphi}}\}$, де: $\mathbf{RE_1^{\varphi}}$ = **«Рекомендації для компоненти N»**; $\mathbf{RE_2^{\varphi}}$ = **«Рекомендації для компоненти CH»**; $\mathbf{RE_3^{\varphi}}$ = **«Рекомендації для компоненти A»**; $\mathbf{RE_4^{\varphi}}$ = **«Рекомендації для компоненти R»**; $\mathbf{RE_5^{\varphi}}$ = **«Рекомендації для компоненти I»**; $\mathbf{RE_6^{\varphi}}$ = **«Рекомендації для компоненти C»**; $\mathbf{RE_7^{\varphi}}$ = **«Рекомендації для компоненти CA»**; $\mathbf{RE_8^{\varphi}}$ = **«Рекомендації для компоненти M»**; $\mathbf{RE_9^{\varphi}}$ = **«Рекомендації для компоненти ME»**; $\mathbf{RE_{10}^{\varphi}}$ = **«Рекомендації для компоненти AD»**; $\mathbf{RE_{11}^{\varphi}}$ = **«Рекомендації для компоненти F».** Підмножину $\mathbf{RE_i^{\varphi}}$ визначимо як:

$$\mathbf{RE_i^{\varphi}} = \{\bigcup_{j=1}^{n_{13i}} RE_{ij}^{\varphi}\} = \{RE_{i1}^{\varphi}, RE_{i2}^{\varphi}, ..., RE_{in_{13i}}^{\varphi}\}, \quad (2.79)$$

де $RE_{ij}^{\varphi} \subseteq \mathbf{RE_i^{\varphi}}$ $(j = \overline{1,n_{13i}})$ – j-те значення параметру $\mathbf{RE_i^{\varphi}}$ у межах i-ї підмножини,

а n_{13i} кількість альтернативних значень параметрів *i*-ї підмножини. З урахуванням (2.79) вираз (2.78) можна представити як: $\mathbf{RE^{\varphi}} = \{\bigcup_{i=1}^{n_{13}} \mathbf{RE_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{13}} \{\bigcup_{j=1}^{n_{13i}} RE_{ij}^{\varphi}\}\} =$

$$\{\{RE_{11}^{\varphi}, RE_{12}^{\varphi}, ..., RE_{1n_{13i}}^{\varphi}\}, \{RE_{21}^{\varphi}, RE_{22}^{\varphi}, ..., RE_{2n_{13i}}^{\varphi}\}, ..., \{RE_{n_{13}1}^{\varphi}, RE_{n_{13}2}^{\varphi}, ..., RE_{n_{13}n_{13i}}^{\varphi}\}\}. \quad (2.80)$$

Наприклад, при $n_{13} = 11\,(i = \overline{1,11})$, $n_{131} = 4\,(j = \overline{1,4})$, $n_{132} = 3\,(j = \overline{1,3})$, $n_{133} = 3$ $(j = \overline{1,3})$, $n_{134} = 8\,(j = \overline{1,8})$, $n_{135} = 4\,(j = \overline{1,4})$, $n_{136} = 3\,(j = \overline{1,3})$, $n_{137} = 3\,(j = \overline{1,3})$, $n_{138} = 3\,(j = \overline{1,3})$, $n_{139} = 2\,(j = \overline{1,2})$, $n_{1310} = 3\,(j = \overline{1,3})$ і $n_{1311} = 4$ $(j = \overline{1,4})$ та враховуючи всі вище перераховані приклади формулу (2.80) можна представити як: $\mathbf{RE^{\varphi}} = \{\bigcup_{i=1}^{11} \mathbf{RE_i^{\varphi}}\} = \{\bigcup_{i=1}^{11} \{\bigcup_{j=1}^{n_{13i}} RE_{ij}^{\varphi}\}\} = \{\{RE_{11}^{\varphi}, RE_{12}^{\varphi}, RE_{13}^{\varphi}, RE_{14}^{\varphi}\}, \{RE_{21}^{\varphi}, RE_{22}^{\varphi}, RE_{23}^{\varphi}\},$

$$\{RE_{31}^{\varphi}, RE_{32}^{\varphi}, RE_{33}^{\varphi}\}, \{RE_{41}^{\varphi}, RE_{42}^{\varphi}, RE_{43}^{\varphi}, RE_{44}^{\varphi}, RE_{45}^{\varphi}, RE_{46}^{\varphi}, RE_{47}^{\varphi}, RE_{48}^{\varphi}\},$$
$$\{RE_{51}^{\varphi}, RE_{52}^{\varphi}, RE_{53}^{\varphi}, RE_{54}^{\varphi}\}, \{RE_{61}^{\varphi}, RE_{62}^{\varphi}, RE_{63}^{\varphi}\}, \{RE_{71}^{\varphi}, RE_{72}^{\varphi}, RE_{73}^{\varphi}\}, \{RE_{81}^{\varphi}, RE_{82}^{\varphi}, \quad (2.81)$$
$$RE_{83}^{\varphi}\}, \{RE_{91}^{\varphi}, RE_{92}^{\varphi}\}, \{RE_{101}, RE_{102}, RE_{103}\}, \{RE_{111}, RE_{112}, RE_{113}, RE_{114}\}\}.$$

2.2. Розробка ієрархічної структури параметрів GDPR-моделі

Ієрархічну структуру параметра $\mathbf{L^{\varphi}}$ можна представити у вигляді схеми на рис.2.1.

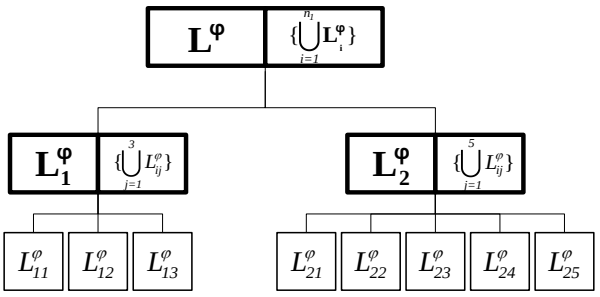


Рис. 2.1. Ієрархічна структура параметра $\mathbf{L^{\varphi}}$

Де, відповідно до (2.7): $L_{11}^{\varphi} = \{"Ст.83,п.4,пп.a"\}$, $L_{12}^{\varphi} = \{"Ст.83,п.4,пп.b"\}$, $L_{13}^{\varphi} = \{"Ст.83,п.4,пп.c"\}$, $L_{21}^{\varphi} = \{"Ст.83,п.5,пп.a"\}$, $L_{22}^{\varphi} = \{"Ст.83,п.4,пп.b"\}$, $L_{23}^{\varphi} = \{"Ст.83,п.4,пп.c"\}$, $L_{24}^{\varphi} = \{"Ст.83,п.4,пп.d"\}$ та $L_{25}^{\varphi} = \{"Ст.83,п.4,пп.e"\}$, що трактується як: «Обов'язки контролера і оператора відповідно до статей 8, 11, 25–

39, і 42, і 43», «Обов'язки органу з сертифікації відповідно до статей 42 і 43», «Обов'язки органу з моніторингу відповідно до статті 41 (п.4)», «Основні принципи опрацювання, в тому числі умови надання згоди, відповідно до статей 5, 6, 7 і 9», «Права суб'єктів даних відповідно до статей 12–22», «Акти передавання ПД до одержувача в третій країні чи до міжнародної організації відповідно до статей 44–49», «Будь-які обов'язки відповідно до закону держави-члена, ухваленого згідно з главою IX» та «Невідповідність постанові або тимчасовому чи остаточному обмеженню на опрацювання чи призупинення потоків даних наглядового органу відповідно до статті 58 (п.2) або ненадання доступу як порушення статті 58 (п.1)» [58, 59].

Ієрархічну структуру параметра $\mathbf{N^{\varphi}}$ можна представити у вигляді схеми на рис.2.2.

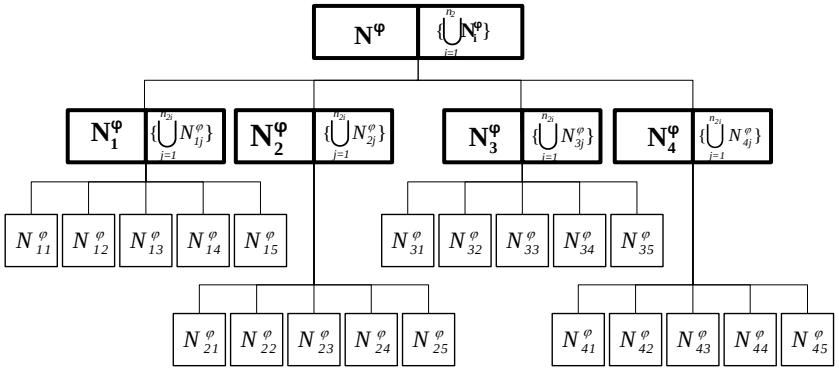


Рис. 2.2. Ієрархічна структура параметра $\mathbf{N^{\varphi}}$

Де, відповідно до (2.11):: N_{11}^{φ} = «Публічна»; N_{12}^{φ} = «Комерційна»; N_{13}^{φ} = «Конфіденційна»; N_{14}^{φ} = «Секретна»; N_{15}^{φ} = «Цілком секретна»; N_{21}^{φ} =]0; Тиждень]»; N_{22}^{φ} =]Тиждень; Місяць]; N_{23}^{φ} =]Місяць; 6 Місяців]; N_{24}^{φ} =]6 Місяців; Рік]; N_{25}^{φ} =] Рік; ∞[; N_{31}^{φ} =]0; 1000]; N_{32}^{φ} =]1000; 50000]; N_{33}^{φ} =]50000; 100000]; N_{34}^{φ} =]100000; 1000000]; N_{35}^{φ} =]1000000; ∞[; N_{41}^{φ} = «Незначний»; N_{42}^{φ} = «Низький»; N_{43}^{φ} = «Середній»; N_{44}^{φ} = «Високий»; N_{45}^{φ} = «Катастрофічний».

Ієрархічну структуру параметра $\mathbf{CH^{\varphi}}$ можна представити на рис. 2.3.

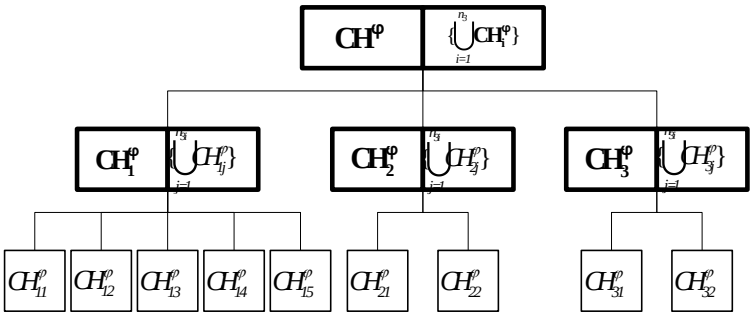


Рис. 2.3. Ієрархічна структура параметра $\mathbf{CH}^{\varphi}$

Де, відповідно до (2.15):: CH_{11}^{φ} = «Максимальний»; CH_{12}^{φ} = «Високий»; CH_{13}^{φ} = «Середній»; CH_{14}^{φ} = «Низький»; CH_{15}^{φ} = «Незначний»; CH_{21}^{φ} = «Так»; CH_{22}^{φ} = «Ні»; CH_{31}^{φ} = «Ігнорування»; CH_{32}^{φ} = «Застосування».

Ієрархічну структуру параметра $\mathbf{A}^{\varphi}$ можна інтерпретувати за допомогою схеми на рис.2.4.

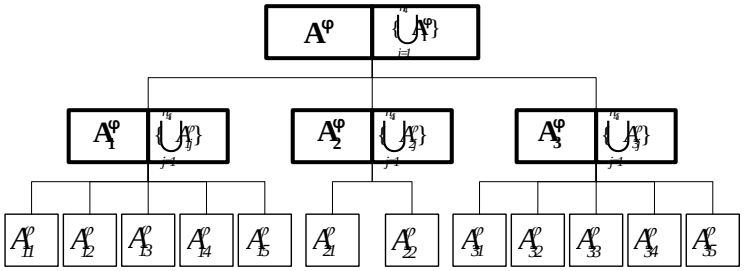


Рис. 2.4. Ієрархічна інтерпретація параметра $\mathbf{A}^{\varphi}$

Де, відповідно до (2.19): A_{11}^{φ} = «Повна»; A_{12}^{φ} = «Значна»; A_{13}^{φ} = «Середня»; A_{14}^{φ} = «Незначна»; A_{15}^{φ} = «Відсутня»; A_{21}^{φ} = «Так»; A_{22}^{φ} = «Ні»; A_{31}^{φ} =]∞; €1.000.000[; A_{32}^{φ} = [€1.000.000; €500.000[; A_{33}^{φ} = [€500.000; €100.000[; A_{34}^{φ} = [€100.000€; 0[; A_{35}^{φ} = [$\varnothing$].

Ієрархічну структуру параметра $\mathbf{R}^{\varphi}$ інтерпретуємо у вигляді схеми на рис. 2.5.

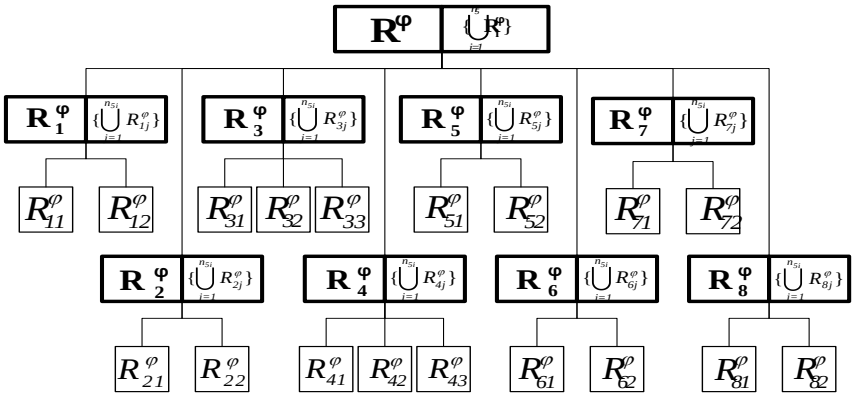


Рис. 2.5. Ієрархічна структура параметра $\mathbf{R}^{\varphi}$

Де, відповідно до (2.23): $R_{11}^{\varphi} = R_{21}^{\varphi} = R_{31}^{\varphi} = R_{41}^{\varphi} = R_{51}^{\varphi} = R_{61}^{\varphi} = R_{71}^{\varphi} = R_{81}^{\varphi} =$ «Так»; $R_{12}^{\varphi} = R_{22}^{\varphi} = R_{32}^{\varphi} = R_{42}^{\varphi} = R_{52}^{\varphi} = R_{62}^{\varphi} = R_{72}^{\varphi} = R_{82}^{\varphi} =$ «Ні»; $R_{33}^{\varphi} = R_{43}^{\varphi} =$ «Невідомо».

Ієрархічну структуру параметра $\mathbf{I}^{\varphi}$ інтерпретуємо у вигляді схеми на рис. 2.6.

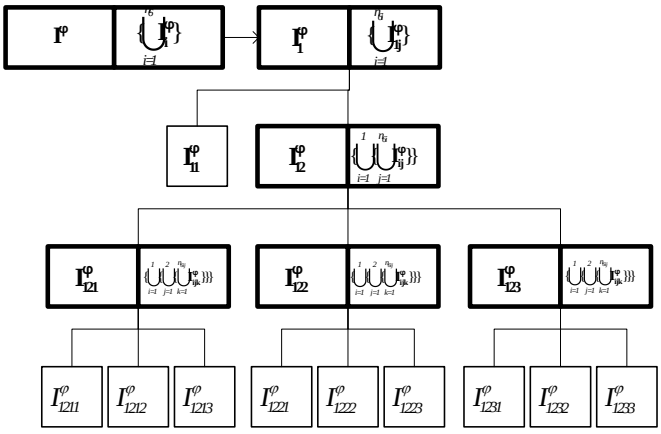


Рис. 2.6. Ієрархічна структура параметра $\mathbf{I}^{\varphi}$

Де, відповідно до (2.33): $I_{1211}^{\varphi} = I_{1221}^{\varphi} = I_{1231}^{\varphi} =$ «Так»; $I_{1212}^{\varphi} = I_{1222}^{\varphi} = I_{1232}^{\varphi} =$ «Ні»; $I_{1213}^{\varphi} = I_{1223}^{\varphi} = I_{1233}^{\varphi} =$ «Невідомо».

Ієрархічну структуру параметра $\mathbf{C}^{\varphi}$ інтерпретуємо у вигляді схеми на рис. 2.7.

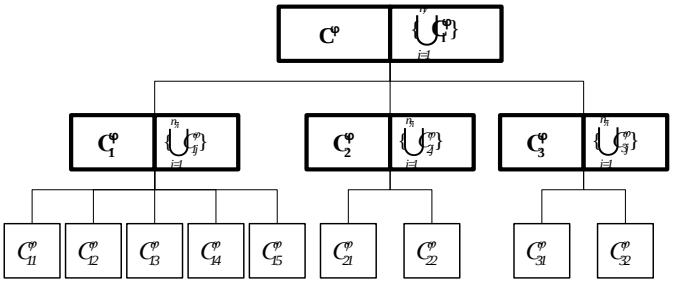


Рис. 2.7. Ієрархічна структура параметра $\mathbf{C^{\varphi}}$

Де, відповідно до (2.37): C_{11}^{φ} = [100%; 75%[; C_{12}^{φ} = [75%; 50%[; C_{13}^{φ} = [50%; 25%[; C_{14}^{φ} = [25%; 0%[; C_{15}^{φ} = [$\varnothing$]; C_{21}^{φ} = «Так»; C_{22}^{φ} = «Ні»; C_{31}^{φ} = «План по відновленню»; C_{32}^{φ} = «Наказ».

Ієрархічну структуру параметра $\mathbf{CA^{\varphi}}$ інтерпретуємо у вигляді схеми на рис.2.8.

Де, відповідно до (2.41): $CA_{11}^{\varphi} = CA_{21}^{\varphi} = CA_{31}^{\varphi}$ = «Так»; $CA_{12}^{\varphi} = CA_{22}^{\varphi} = CA_{32}^{\varphi}$ = «Ні».

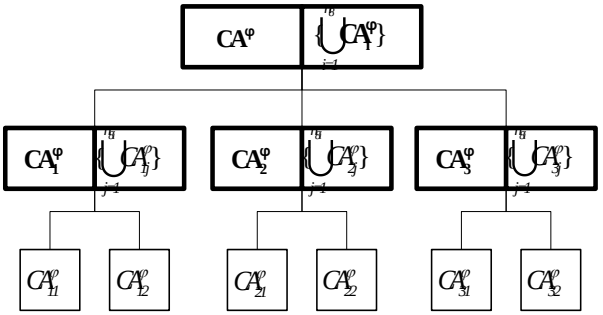


Рис.2.8. Ієрархічна структура параметра $\mathbf{CA^{\varphi}}$

Ієрархічну структуру параметра $\mathbf{M^{\varphi}}$ інтерпретуємо у вигляді схеми на рис. 2.9.

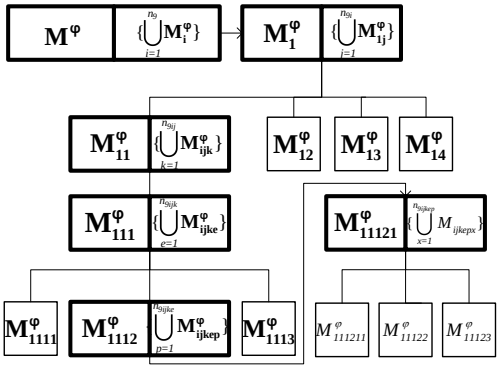


Рис.2.9. Ієрархічна структура параметра $\mathbf{M^{\varphi}}$

Де, відповідно до (2.53): M^{φ}_{111211} = «Так»; M^{φ}_{11122} = «Ні»; M^{φ}_{11123} = «Невідомо».

Ієрархічну структуру параметра $\mathbf{ME^{\varphi}}$ інтерпретуємо у вигляді схеми на рис. 10.

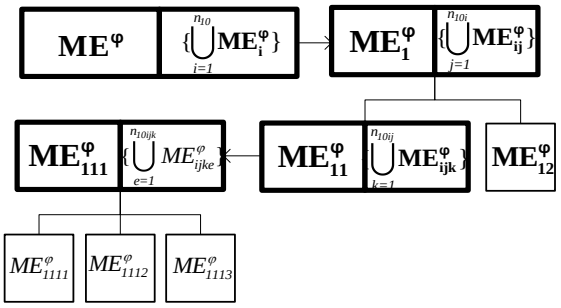


Рис. 2.10. Ієрархічна структура параметра $\mathbf{ME^{\varphi}}$

Де, відповідно до (2.61): ME^{φ}_{1111} = «Так»; ME^{φ}_{1112} = «Ні»; ME^{φ}_{1113} = «Невідомо».

Ієрархічну структуру параметра $\mathbf{AD^{\varphi}}$ інтерпретуємо у вигляді схеми на рис. 2.11.

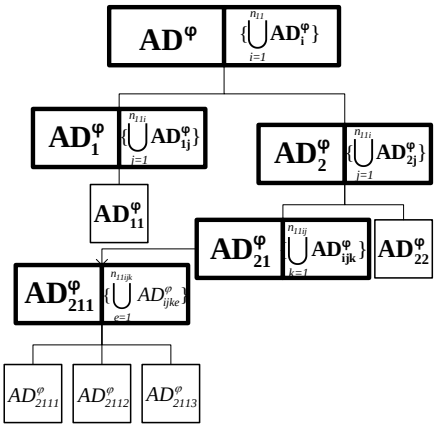


Рис. 2.11. Ієрархічна структура параметра $\mathbf{AD^{\varphi}}$

Де, відповідно до (2.69): AD^{φ}_{2111} = «Так»; AD^{φ}_{2112} = «Ні»; AD^{φ}_{2113} = «Невідомо».

Ієрархічну структуру параметра $\mathbf{F^{\varphi}}$ інтерпретуємо у вигляді схеми на рис. 2.12.

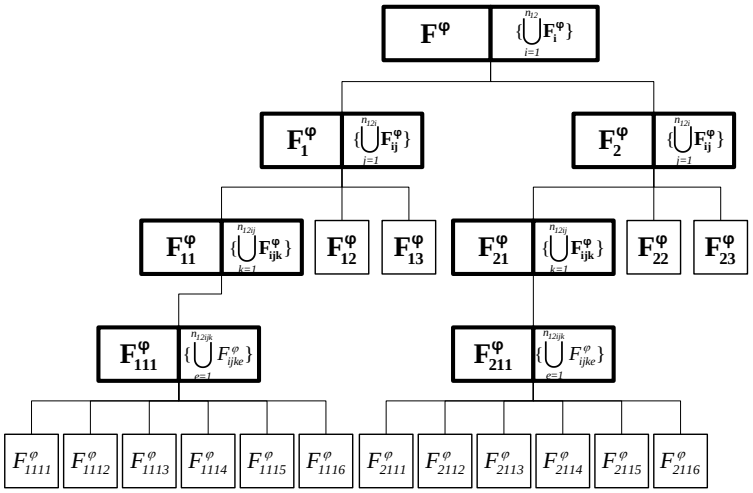


Рис. 2.12. Ієрархічна структура параметра $\mathbf{F^{\varphi}}$

Де, відповідно до (2.77): $F^{\varphi}_{1111} = F^{\varphi}_{2111} =$]∞; €1000000[; $F^{\varphi}_{1112} = F^{\varphi}_{2112} =$ [€1000000; €500000[; $F^{\varphi}_{1113} = F^{\varphi}_{2113} =$ [€500000; €100000[»; $F^{\varphi}_{1114} = F^{\varphi}_{2114} =$ [€100000; €0[; $F^{\varphi}_{1115} = F^{\varphi}_{2115} = [\varnothing]$; $F^{\varphi}_{1116} = F^{\varphi}_{2116} =$ «Невідомо».

Ієрархічну структуру параметра $\mathbf{RE^{\varphi}}$ предствимо у вигляді схеми на рис. 2.13.

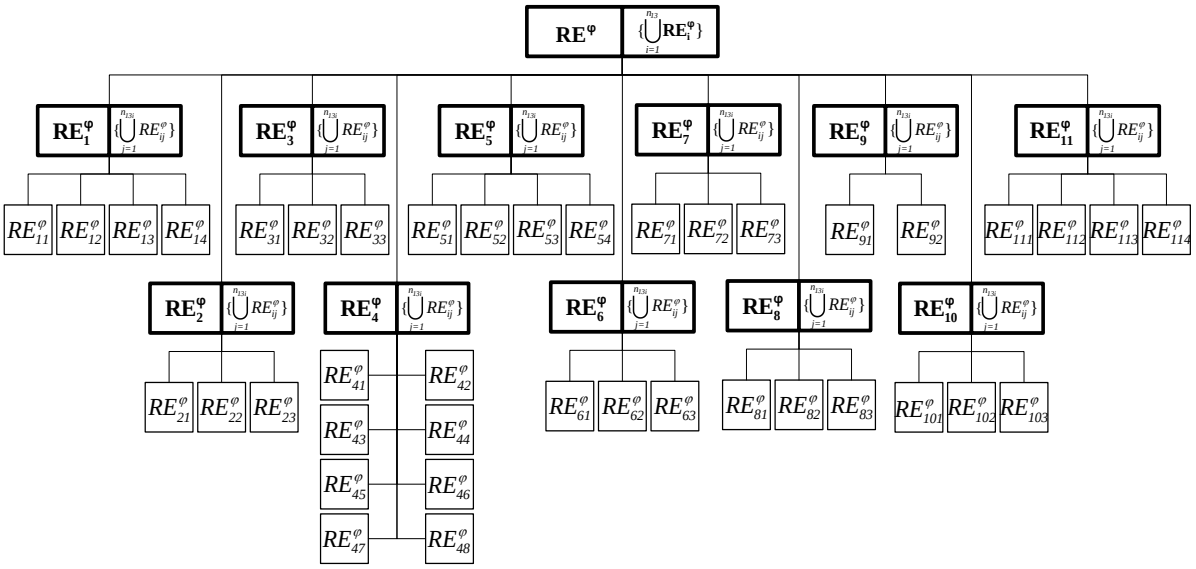


Рис. 2.13. Ієрархічна структура параметра $\mathbf{RE^{\varphi}}$

Де, відповідно до (2.81): RE^{φ}_{11} = «Здійснювати періодичну інвентаризацію даних в організації»; RE^{φ}_{12} = «Виконувати періодичний аналіз недоліків в забезпеченні захисту ПД організації»; RE^{φ}_{13} = «Проводити заходи, пов’язані з

оцінкою, веденням обліку активів та управлінням активами, в тому числі їх зберіганням, переміщенням, захистом»; RE_{14}^{φ}= «Проводити систематичне та масштабне оцінювання впливу передбачених автоматизованих операцій опрацювання ПД суб'єктів, що може призвести до виникнення високого ризику для прав і свобод суб'єкта ПД»; RE_{21}^{φ}= «Виконувати періодичний аналіз недоліків в забезпеченні захисту ПД організації відповідно до ISO 27001»; RE_{22}^{φ}= «Вище керівництво повинно демонструвати лідерство та обов'язки по відношенню до СМІБ організації» [58]; RE_{23}^{φ}= «Встановити, впровадити, підтримувати функціонування та безперервно покращувати СМІБ у відповідності до вимог ISO 27001 в організації»; RE_{31}^{φ}= «Контролер або оператор повинні відшкодувати будь-яку шкоду, заподіяну суб'єкту ПД в результаті опрацювання з порушенням Регламенту»; RE_{32}^{φ}= «Розробити відповідний план усунення недоліків, пом'якшення негативних наслідків або інших коригуючих дій при виявленні порушень захисту ПД»; RE_{33}^{φ}= «Проводити оцінку зниження витрат при їх застосуванні в умовах пом'якшення наслідків збитків»;. RE_{41}^{φ}= «Проводити періодичний аналіз відповідності СМІБ до вимог ISO 27001»; RE_{42}^{φ}= «Вибір та удосконалення засобів шифрування ПД у відповідності до методів обробки ПД суб'єктів»; RE_{43}^{φ}= «Проводити перевірку використаних засобів шифрування у відповідності до потужностей організації, мети обробки та сфери застосування ПД суб'єктів»; RE_{44}^{φ}= «Здійснювати періодичний аудит інформаційної системи організації для перевірки засобів шифрування та зберігання ключів шифрування»; RE_{45}^{φ}= «Проводити аналіз інцидентів, що відбулися, з метою планування превентивних заходів захисту та поліпшення процесу забезпечення захисту ПД суб'єктів та інших критично важливих даних організації»; RE_{46}^{φ}= «Впровадити та періодично проводити тестування на проникнення у відповідності до PTES, та використовувати сканери вразливостей для своєчасного їх виявлення для попередження витоку ПД» [65]; RE_{47}^{φ}= «Впровадити систему управління ризиками та періодично проводити аналіз інформаційної системи

організації у відповідності до ISO/IEC 31010:2009» [66]; RE_{48}^{φ} = «Узагальнювати та вдосконалювати Кодекс поведінки (або відповідний до нього) в організації для дотримання правил обробки ПД суб'єктів у відповідності до Резолюції 34/169 ООН» [67]; RE_{51}^{φ} = «Проводити розслідування для з'ясування причин втрати ПД суб'єктів шляхом дослідження журналів реєстрації відповідної інформаційної системи та перевіряти засоби їх захисту»; RE_{52}^{φ} = «Проводити аудит щодо осіб контролера/оператора, які були причасні до попереднього порушення, на предмет відповідності займаним посадам»; RE_{53}^{φ} = «Перевірити наявність та проводити аналіз впроваджених заходів запобігання витоку ПД суб'єктів, що ґрунтуються на попередніх втратах ПД»; RE_{54}^{φ} = «Проводити перевірку на відповідність скоєного порушення Регламенту для отримання детальних рекомендацій щодо його попередження в майбутньому»; RE_{61}^{φ} = «Забезпечувати тісну співпрацю контролера/оператора з наглядовим органом для зменшення розміру можливого штрафу»; RE_{62}^{φ} = «Весь персонал організації повинен бути відповідним чином проінформований та навчений, а також сповіщений про зміни в політиках та процедурах організації, що були впроваджені на основі рекомендацій наглядового органу»; RE_{63}^{φ} = «Розробити та впровадити план(и) по відновленню для можливості зменшення дії порушення на інформаційну систему організації та зробити їх невід'ємною частиною реагування на витоки ПД суб'єктів»; RE_{71}^{φ} = «Впровадити сучасні засоби криптографічного захисту інформації для шифрування ПД суб'єктів, або якщо такі вже впроваджені, перевірити яким чином ПД не пройшли етап шифрування»; RE_{72}^{φ} = «Перед внесенням Чутливих ПД в базу даних організації обов'язково перевіряйте чи було здійснено їх шифрування, оскільки Чутливі ПД є критично-важливими для всієї організації загалом та їх власника»; RE_{73}^{φ} = «Перед внесенням Даних про кримінальні правопорушення в базу даних організації обов'язково перевіряйте чи було здійснено їх шифрування, оскільки їх витік може гарантувати крах всієї організації»; RE_{81}^{φ} = «Реагування на порушення захисту ПД

повинно відбуватися у відповідності з документованими процедурами організації, що розроблені з урахуванням Регламенту»; RE_{82}^{φ} = «Як тільки контролеру стає відомо про порушення захисту ПД, він повинен повідомити наглядовий орган про це, але не пізніше ніж за 72 години після того, як йому стало про це відомо»; RE_{83}^{φ} = «Якщо неможливо здійснити повідомлення про порушення захисту ПД протягом 72 годин, у такому разі разом із повідомленням необхідно надати відомості про причини затримки»; RE_{91}^{φ} = «Провести перевірку відповідності отриманих коригувальних заходів від наглядового органу у відповідності до пунктів Статті 58»; RE_{92}^{φ} = «Провести перевірку, чи отримані коригувальні заходи були впроваджені в розроблені Плани по відновленню»; RE_{101}^{φ} = «Узагальнювати та вдосконалювати Кодекс поведінки (або відповідний до нього) в організації для дотримання правил обробки ПД суб'єктів у відповідності до Резолюції 34/169 ООН»; RE_{102}^{φ} = «Перед відкриттям діяльності в країні ЄС, необхідно здійснити перевірку щодо наявності механізмів сертифікації основних засобів захисту ПД»; RE_{103}^{φ} = «Провести сертифікацію організації в рамках певної системи та за вибраною схемою, що діє на ринку держави країни ЄС»; RE_{111}^{φ} = «Проводити внутрішні аудити на предмет виявлення контролера/оператора, який створив умови для витоку ПД суб'єктів та дослідити всі можливі прогалини в системі менеджменту інформаційної безпеки»; RE_{112}^{φ} = «Здійснити аналіз втрачених ПД суб'єктів та вияснити, яким чином організація/контролер/оператор отримали від цього вигоду»; RE_{113}^{φ} = «Проводити внутрішні аудити на предмет виявлення контролера/оператора, який створив умови для витоку ПД суб'єктів та дослідити всі можливі прогалини в СМІБ»; RE_{114}^{φ} = «Здійснити аналіз втрачених ПД суб'єктів та вияснити, яким чином організація отримала від цього збиток» [58, 59].

Загальну ієрархічну структуру моделі можемо представити у наступному вигляді (рис.2.14).

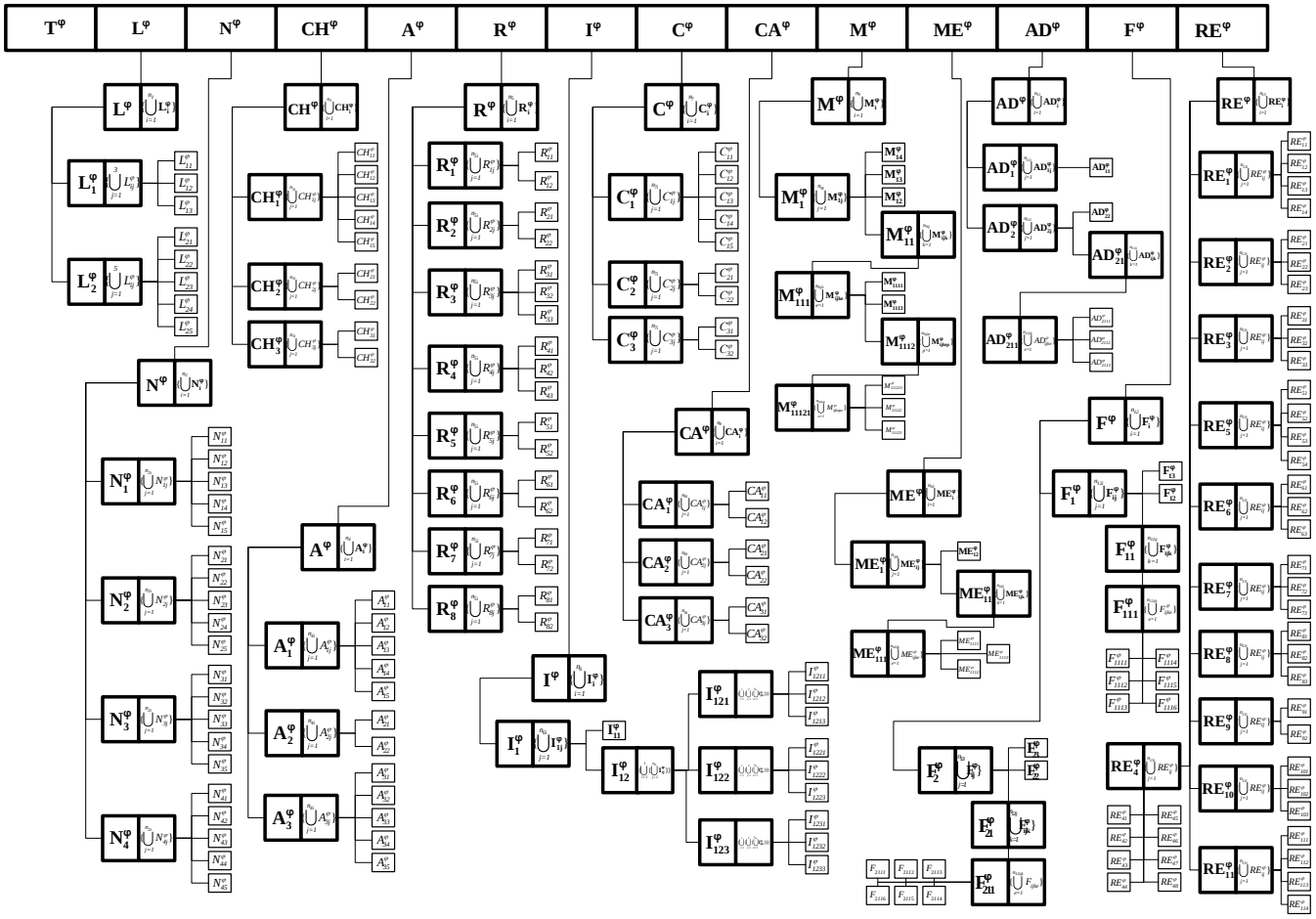


Рис. 2.14. Ієрархічна структура моделі

Отже, на основі теоретико-множинного представлення розроблена GDPR-модель, яка за рахунок множин кортежних моделей інтегрованого представлення параметрів персональних даних, що відображають величини річного обігу, множини, що характеризують рівень, специфіку, характер та рецидив порушення, зниження шкоди, відповідність заходам, визначаючий чинник, ступінь відповідальності, рівень співпраці, категорії даних, спосіб виявлення, дотримання кодексів і превентивні рекомендації дозволяє відповідно до положень Регламенту GDPR визначити необхідну низку множин вхідних та вихідних величин для формалізації процесу оцінювання збитків від втрати ПД, як на державному рівні, так і на рівні організації.

В подальшому, для реалізації зазначеного процесу необхідна розробка методу оцінювання негативних наслідків від витоку ПД відповідно до положень регламенту GDPR, що дозволить визначити максимальний та фактичний збитки для організації.

2.3. Кортежна модель параметрів персональних даних

Для визначення вхідних, вихідних та внутрішніх параметрів забезпечення захисту ПД, які використовуються для оцінки ризиків, проведено дослідження міжнародних стандартів та існуючих методик [33-57] на основі яких розроблено кортежну модель параметрів персональних даних. Дана модель містить набір параметрів представлення ризиків захисту ПД, що обробляються в АС та має типову структуру (рис. 2.15).

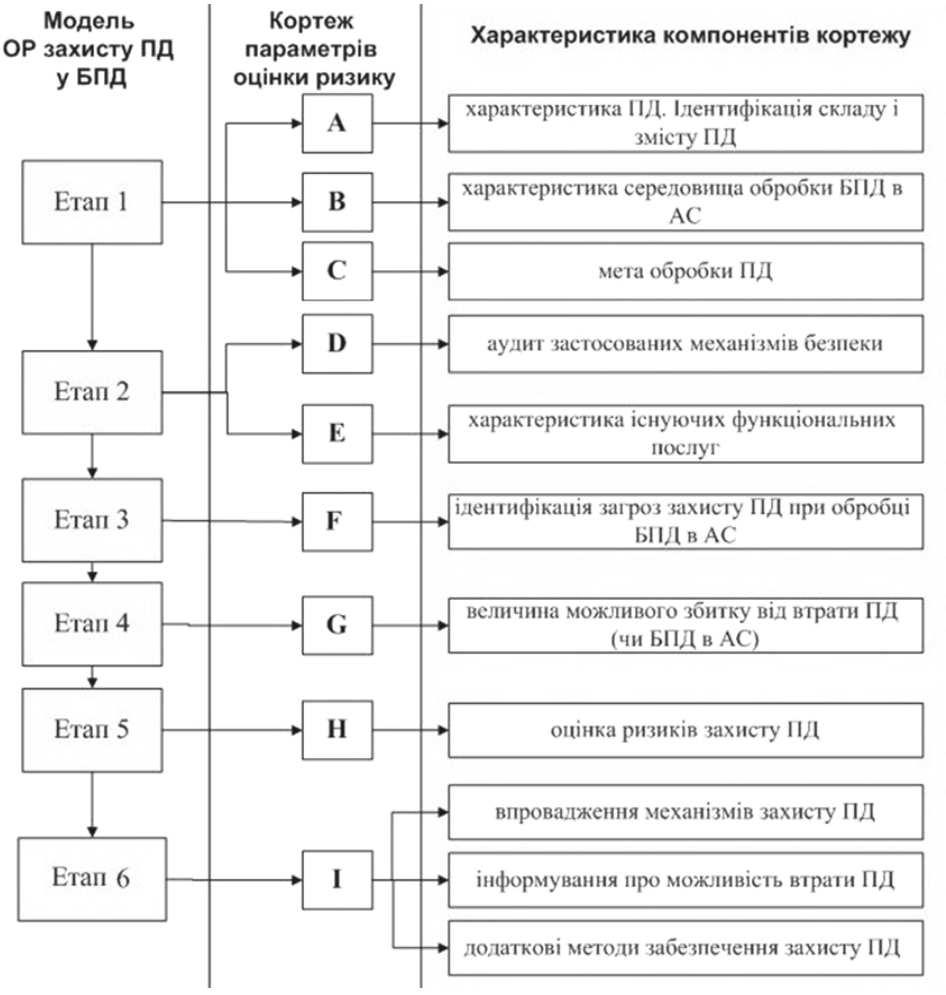


Рис. 2.15. Модель ОР захисту ПД під час їх обробки в АС

Інтегроване представлення параметрів ризику з відображенням на сферу захисту ПД в АС здійснюється у вигляді кортежу, який можна представити у наступному вигляді [68]: **<A, B, C, D, E, F, G, H, I>**, де **A** – характеристика ПД (ідентифікація їх складу та змісту); **B** – характеристика середовища обробки БПД в АС; **C** – мета обробки ПД; **D** – аудит застосованих механізмів безпеки; **E** –

характеристика існуючих функціональних послуг безпеки; **F** – ідентифікація загроз безпеці ПД при обробці БПД в АС; **G** – величина можливих збитків від втрати ПД; **H** – оцінка ризику захисту ПД в АС; **I** – керування ризиком та досягнення необхідного рівня гарантій захисту ПД.

Перший наведений в кортежі компонент – характеристика та ідентифікація складу і змісту ПД **(A)**. Законодавством визначено [67, 70-73], що до ПД відносять відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. Розглянемо загальновідомі ПД склад та зміст яких можна відобразити у вигляді символьної змінної A_n, $A_n \in \{A_1, A_2, A_3, A_4, A_5, A_6, A_7 ... A_i\}$ (індекс n – номер ідентифікатору матеріального носія, що містить такі ПД (наприклад, документу). До складу зазначених ПД належать відомості про: A_1= «Прізвище, ім'я, по батькові»; A_2= «Дата і місце народження»; A_3= «Відомості про освіту»; A_4= «Ідентифікаційний код»; A_5= «Відомості з військового квитка»; A_6= «Відомості з водійських прав»; A_7= «Відомості з свідоцтва про народження (одруження, тощо)»; A_8= «Паспортні дані»; A_9= «Відомості про склад сім'ї»; A_{10}= «Відомості про стан здоров'я»; A_i= «Інші дані (видані на ім'я особи, тощо)». Приклад загальновідомих документів, що містять ПД та їх коефіцієнти важливості K_{vd} (або цінності для власника) приведено у таблиці 2.2.

Таблиця 2.2

Приклад документів, що містять ПД та їх важливість

Параметр	Документ, що містить персональні дані	Коефіцієнт важливості K_{vd}
1	2	3
A_1	Паспорт (в т.ч. закордонний)	0,9
A_2	Військовий квиток	0,8
A_3	Свідоцтво про народження	0,7
A_4	Ідентифікаційний код	0,6

Продовження таблиці 2.2

1	2	3
A_5	Водійські права	0,6
A_6	Свідоцтво про шлюб	0,5
A_7	Трудова книжка	0,5
A_8	Медична картка	0,4
A_i	Інші документи	[0 ÷ 1]

Під другим компонентом кортежу – середовищем обробки БПД (**B**), слід розуміти ПЗ у якому виконувалися будь-які дії, пов'язані з внесенням, модифікацією, знищенням ПД у БПД. У таблиці 2.3 наведено перелік такого ПЗ та його рівень функціональної складності K_{vp} для користувача.

Таблиця 2.3

Середовище обробки ПД та його складність

Параметр	Середовище обробки	Рівень складності K_{vp}
B_1	«MS Word»	0,3
B_2	«MS Excel»	0,4
B_3	«MS Access»;	0,5
B_4	«Кадри»	0,6
B_5	«Працівники»	0,7
B_6	«M.E.Doc (Медок)»	0,8
B_7	«IT-Enterprise»	0,9
B_i	«Інші засоби»	[0 ÷ 1]

Третій параметр оцінювання ризику – мета обробки ПД (**C**). Мета обробки ПД визначається в залежності від того, саме де та для якого очікуваного кінцевого результату такі ПД будуть оброблятися. Даний параметр представляється у вигляді множини ідентифікаторів згідно до законодавства: $C_n \in \{C_1, C_2, C_3, C_4, C_5, C_6 ... C_i\}$: C_1= «Забезпечення реалізації трудових, соціально-трудових відносин, відносин у сфері управління персоналом, військового обліку»; C_2= «Забезпечення адміністративно-правових відносин»; C_3= «Забезпечення

відносин у сфері бухгалтерського і податкового обліку»; C_4 = «Забезпечення національної безпеки, економічного добробуту та прав людини»; C_5 = «Захист прав і свобод фізичних осіб, ПД яких обробляються, чи прав інших суб'єктів відносин, пов'язаних із ПД, а також з метою боротьби із злочинністю»; C_6 = «Забезпечення суб'єктів відносин, пов'язаних із ПД, зведеною знеособленою інформацією щодо ПД згідно закону»; C_i = «Інша мета».

Наступним компонентом кортежу є *аудит застосованих механізмів безпеки* (**D**). Даний компонент описується набором елементів $D_n \in \{D_1, D_2, D_3, D_4, D_5 ... D_i\}$ та визначається перевіркою наявних в АС організаційно-правових та програмно-технічних заходів та механізмів захисту ПД оброблюваних в АС, до яких можна віднести D_1 = «Наявність згоди суб'єкта ПД на їх обробку в АС»; D_2 = «Ідентифіковано володільця чи розпорядника БПД, третю особу та встановлено Типовий порядку обробки ПД у БПД»; D_3 = «Отримано Свідоцтво про реєстрації БПД уповноваженим органом з питань захисту ПД у Державному реєстрі БПД»; D_4 = «Призначено відповідальну особу за обробку та захист ПД або створено службу захисту інформації (з обов'язками захисту ПД)»; D_5 = «Застосовано систему управління (менеджменту) інформаційною безпекою або атестовану КСЗІ з реалізованим стандартним профілем *х.КЦ.х*, *х.КД.х*, *х.КЦД.х* (за додатком А НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»)»; D_i = «Інші механізми захисту».

Після проведення аудиту застосованих механізмів безпеки, доцільним є визначення наявних послуг безпеки (**E**), як п'ятого елементу кортежу, що визначаються множиною ідентифікаторів $E_n \in \{E_1, E_2, E_3, E_4\}$. З урахуванням того, що у сфері захисту інформації ризик пов'язаний з такими базовими характеристиками безпеки як конфіденційність, цілісність, доступність і спостережність, то на даному етапі слід встановити існуючі в АС критерії

захищеності [74]: E_1= «Конфіденційність {*КА, КВ*}»; E_2= «Цілісність {*ЦА, ЦВ*}»; E_3= «Доступність {*ДС*}»; E_4= «Спостережність {*НР, НИ, НО, НВ, НА, НП, НК*}».

Шостим параметром є ідентифікація загроз безпеці ПД при обробці БПД в АС (**F**). Перелік можливих загроз визначається існуючими стандартами та методиками аналізу і оцінки ризиків інформаційної безпеки [75] і може доповнюватись самостійно. Даний параметр наводиться у вигляді набору елементів відомих загроз безпеці ПД, а саме [68]: $F_n \in \{F_1, F_2, F_3, F_4, F_5, F_6 ... F_i\}$: F_1= «Шпигунство»; F_2= «Неумисні помилки користувачів»; F_3= «Несанкціонований доступ (збирання, видалення, пошкодження, модифікація, поширення тощо)»; F_4= «Блокування інформації і порушення встановленого порядку її маршрутизації»; F_5= «Збій у роботі обладнання та внутрішня відмова АС»; F_6= «Неналежна передача ПД третій особі; F_i= «Інші можливі загрози». По відношенню до визначених загроз визначається ймовірність їх реалізації (настання) (**P**) як: «низька» P_{r_1}, «середня» P_{r_2} та «висока» P_{r_3}, що приведено формулою (2.82):

$$P_{riv\_zag} = \{\bigcup_{i=1}^{n} P_{r_i}\} = \{P_{r_1}, P_{r_2}, P_{r_3}, ... P_{r_i}\}, R_{riv\_zag} \in \{R_{riv\_zag_{i_{max}}}\}, (i=\overrightarrow{1,n}) \qquad (2.82)$$

де n – кількість запропонованих загроз, i – номер загрози.

Сьомий параметр кортежу – величина нанесених збитків (**G**), може визначатися як кількісними так і якісними показниками. Оцінка збитків проводиться за шкалами відомих методик, що характеризують матеріальну чи моральну шкоду, шкоду національній безпеці [74], шкоду від порушення прав і свобод людини тощо. Шкали величини можливих збитків від втрати ПД приведені у таблиці 2.4.

Після визначення загальних параметрів, переходимо безпосередньо до восьмого параметра кортежу – оцінки ризику захисту ПД в АС (**H**). Під ризиком захисту ПД під час їх обробки в АС розуміється функція ймовірності реалізації загрози до виду і величини завданих збитків від можливої втрати ПД при

наявності уразливостей та ступеня їх прийнятності для експлуатації АС, що визначається за формулою:

$$H=P\times G \qquad (2.83)$$

де P – ймовірність реалізації загрози; G – величина завданих збитків.

Таблиця 2.4

Шкали величини можливих збитків від втрати ПД

Величина збитку (G)	Інтервальна шкала (I)	Бальна шкала	Відсоткова шкала	Грошова шкала
G_1	0 ÷ 0,1	1	0 – 10%	0 – 100$
G_2	0,11 ÷ 0,3	2	11% – 30%	100– 1000$
G_3	0,31 ÷ 0,6	3	31% – 60%	1000– 10000$
G_4	0,61 ÷ 0,8	4	61% – 80%	10000– 100000$
G_5	0,81 ÷ 1,0	5	81 % – 100%	>100000$

Завершальним етапом є визначення останнього параметру кортежу – керування ризиком та досягнення необхідного рівня захищеності ПД в АС (**I**). На даному етапі за допомогою таблиці відповідності отриманих значень параметрів P та G (табл. 2.5) визначається необхідний рівень захищеності ПД в АС від 1 до 5 балів для застосування рекомендованої політики безпеки.

Таблиця 2.5

Оцінка рівня захищеності ПД в АС

Величина завданих збитків (G)	Ймовірність реалізації певної загрози (P)				
	0-0,1	0,1-0,3	0,3-0,6	0,6-0,8	0,8-1,0
0-100$	1	1	2	3	3
100-1000$	1	2	2	3	4
1000-10000$	2	2	3	4	4
10000-1000000$	3	2	4	4	5
>1000000$	3	4	4	5	5

Рекомендовані політики безпеки, що сформовані за результатами аналізу вимог законодавства України у сфері забезпечення захисту ПД, приведені у таблиці 2.6.

Таблиця 2.6

Рекомендовані політики безпеки

Рівень в балах	**Рекомендовані політики безпеки**
1	Виконання ОЗЗІ (організаційно-провових заходів захисту інформації)
2	Створення СЗІ (служби ЗІ) або призначення відповідальної особи
3	Використання ТЗІ/КЗІ (технічного та/або криптографічного ЗІ)
4	Використання КЗЗ (комплексу засобів захисту)
5	Застосування КСЗІ (комплексної системи захисту інформації)

Передбачається перегляд сукупності заходів щодо оцінки ризику, вибору, реалізації і впровадження заходів (механізмів) захисту ПД у БПД в АС, що проводяться протягом всього життєвого циклу АС і спрямовані на досягнення прийнятного рівня залишкового ризику. Проводиться необхідне інформування про можливість несанкціонованого доступу або втрати ПД уповноваженого державного органу з питань захисту ПД. Вживаються додаткові заходи щодо забезпечення захисту ПД (обов’язкові чи вибіркові) [76], спеціальні засоби технічного та криптографічного захисту інформації (шифрування даних) згідно з політикою безпеки. Далі, в основі рекомендованої політики безпеки, передбачено застосування необхідних заходів та засобів через їх впровадження в АС для підвищення рівня захищеності ПД.

2.4. Модель параметрів для оцінювання рівня критичності кризових ситуацій, пов’язаних з витоком персональних даних

В умовах зростаючої цифровізації та інтенсивного використання інформаційних систем збереження та обробки персональних даних, питання оперативного реагування на кризові ситуації, пов’язані з витоками або втратами персональних даних, набуває особливого значення. Зростає потреба у побудові ефективних моделей, що дозволяють не лише виявляти потенційні загрози, але й об'єктивно оцінювати рівень критичності кризових ситуацій, які загрожують

цілісності, доступності та конфіденційності персональної інформації.

В роботах [77, 78] описані методи виявлення та ідентифікації інцидентів / потенційних кризових ситуацій (ІПКС), а також оцінювання рівня критичності інцидентів, які засновані на нечіткій логіці та методах експертного оцінювання. В [79] описана інтегрована модель представлення ІПКС. Проте в цих роботах неврахована ситуація появи декількох (двох і більше) ІПКС одночасно, їх узгодження та визначення середнього та сумарного рівня критичності. Тому основною метою є розробка механізму кореляції інцидентів інформаційної безпеки та визначення середнього та сумарного рівня критичності спричиненого ними впливу на інформаційну систему з застосуванням методів нечіткої логіки [80].

Для формалізації процесів прогнозування, виявлення, ідентифікації та оцінки КС введемо множину ІПКС:

$$\mathbf{IKS} = \{\bigcup_{i=1}^{n} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \ldots, \mathbf{IKS_n}\}, (i = \overline{1,n}), \tag{2.84}$$

де n визначає кількість потенційних КС i, тобто інцидентів, що можуть спричинити кризовий стан, кожен з яких відображається у вигляді узагальненого шестикомпонентного кортежу [80]:

$$\mathbf{IKS_i} = < IKS_i, \mathbf{P_i}, \mathbf{T_i^e}, \underset{\sim}{\mathbf{P}}_{\mathbf{i}}, \mathbf{ER_i}, LCS_i >, \tag{2.85}$$

в якому: IKS_i – ідентифікатор i-го ІПКС, що є (або може стати) причиною виникнення КС; $\mathbf{P_i}$ – підмножина можливих параметрів, що використовуються для прогнозування чи ідентифікації i-го інциденту; $\mathbf{T_i^e}$ – підмножина всіх можливих нечітких (лінгвістичних) еталонів, що відображають еталоні стани відповідних параметрів з підмножини $\mathbf{P_i}$; $\underset{\sim}{\mathbf{P}}_{\mathbf{i}}$ – підмножина поточних значень параметрів за певний проміжок часу; $\mathbf{ER_i}$ – підмножина евристичних правил, побудованих на основі нечітких параметрів, які використовуються для виявлення/ідентифікації i-го ІПКС; LCS_i – рівень критичності ситуації, спричиненої i-м ІПКС.

Детальний опис процедури виявлення, ідентифікації ІПКС, описаний в [77]. Виявлена ситуація відноситься до кризової лише якщо рівень її критичності

вищий середнього або більший, тобто $LCS_i \gtrsim BC^e$. В іншому разі інцидент або взагалі залишається поза увагою (при достатньо низькому рівні критичності) або проводиться реагування на нього з метою контролю і усунення як для звичайного інциденту інформаційної безпеки. Кожен інцидент характеризується рівнем критичності, що задається множиною $\mathbf{LCS} = \{\bigcup_{i=1}^{n} \underset{\sim}{LCS}_i\} = \{\underset{\sim}{LCS}_1, ..., \underset{\sim}{LCS}_n\}$, $(i = \overline{1,n})$. Рівень критичності визначається через параметри оцінки критичності ситуації з врахуванням їх вагових коефіцієнтів, тобто $\underset{\sim}{LCS}_i = \sum_{e=1}^{E} (\Omega_e \times \underset{\sim}{L}_e)$.

Недоліком даної моделі є неврахування взаємного впливу інцидентів, дія яких збігається у часі, на середовище інформаційної системи. Оскільки той чи інший ІПКС характеризується набором оціночних параметрів рівня критичності, що визначають ступінь впливу інциденту на середовищі в певному аспекті, то кожен з ІПКС може посилювати загальний рівень впливу на систему залежно від величини їх кореляції один з одним. Так, коефіцієнт кореляції встановлює залежність між різними ІПКС і може набувати значень від 0 до 1. Запропонуємо застосування в моделі представлення ІПКС механізму кореляції подій. Даний механізм ґрунтується на визначенні спільних оціночних параметрів рівня критичності для різних ІПКС, причому чим більша кількість однакових параметрів тим більший коефіцієнт кореляції.

Так кожен інцидент можна оцінити застосувавши загальний набір параметрів оцінки рівня критичності [77], такі як: «Тривалість інциденту (TR)», «Ступінь порушення функціоналу критичних ресурсів/процесів (DVF)», «Географічний масштаб інциденту (GS)», «Масштаб інциденту в організаційному аспекті (OS)», «Загальний рівень економічних збитків (OLED)», «Відношення рівня економічних збитків за поточний період до відповідного рівня за попередній період (RD)», «Рівень загрози життю та здоров'ю людей (RTLH)», «Питомий показник смертності на поточний момент (RM)», «Частота проявів інцидентів (інтенсивність) (F)», «Степінь руйнування інфраструктури (DDI)»,

«Співвідношення орієнтовного часу відновлення і показника RTO (CRT)», «Відношення рівня втрат ресурсів і показника RPO (CRP)», «Рівень панічних, протестних та антидержавних настроїв персоналу/населення (LM)», «Ступінь впливу зовнішніх дестабілізуючих та психологічних чинників (DIEPF)», «Ступінь порушення характеристик безпеки ІР з ОД (DVChS)». Кількість і склад характерних параметрів для кожного ІПКС можуть мати різні значення і визначаються експертами.

Основним елементом інтегрованої моделі представлення ІПКС є ідентифікатор IKS_i що зв'язує елемент множини **ІКS** з певним інцидентом, який визначається через відповідне йому ім'я. Наприклад, при $n=5$ отримаємо

$$\mathbf{ІКS} = \{\bigcup_{i=1}^{5} \mathbf{ІКS_i}\} = \{\mathbf{ІКS_1}, \mathbf{ІКS_2}, \mathbf{ІКS_3}, \mathbf{ІКS_4}, \mathbf{ІКS_5}\} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}\}, \quad (2.86)$$

де **A**,**B**,**C**,**D**,**E** – назви інцидентів. Відповідно для кожного з цих інцидентів характерні свої набори оціночних параметрів

$$\mathbf{L_i} = \bigcup_{i=1}^{N} \left\{ \bigcup_{e=1}^{E} \underset{\sim}{L_e} \right\} = \bigcup_{i=1}^{N} \left\{ \underset{\sim}{L_1}, \underset{\sim}{L_2}, ..., \underset{\sim}{L_E} \right\}, e = \overline{1, E}, \quad (2.87)$$

де E – кількість параметрів. Наприклад, за умов дослідження для інциденту **A** при E=15,

$$\mathbf{L_A} = \left\{ \bigcup_{e=1}^{15} \underset{\sim}{L_e} \right\} = \left\{ \underset{\sim}{L_1}, \underset{\sim}{L_2}, ..., \underset{\sim}{L_{15}} \right\} = \{TR, DVF, GS, OS, OLED, \quad (2.88)$$

$$RD, RTLH, RM, F, DDI, CRT, CRP, LM, DIEPF, DVChS\}.$$

Для визначення залежності між ІПКС введемо дві категорії подій: основна та залежні від неї інциденти. Можна виділити два способи розподілення і привласнення значення основної та залежних подій, такі як: за часом – ІПКС, який був виявлений першим набуває статусу основного, а всі інші – залежних від нього ІПКС; за рівнем критичності – статус основного ІПКС привласнюється інциденту з найбільшим рівнем критичності.

В такому разі необхідно провести процедуру ранжування ІПКС за рівнем критичності. Зібрані відомості про КС формують значення оціночних параметрів,

які обробляються (шляхом визначення коефіцієнту важливості, проведення їхньої фазифікації, обраховування як суми з врахуванням коефіцієнта важливості і дефазифікації) і визначають загальний рівень критичності ситуації, що склалася в результаті впливу ІПКС [80].

Запропоновано модель параметрів для оцінювання рівня критичності кризових ситуацій, пов'язаних з витоком персональних даних, основними параметрами якої є: 1) ІПКС та набор оціночних параметрів з загальної множини, що характеризують їх вплив на середовище; 2) основні і залежні ІПКС, а також відповідна зміна нумерації інцидентів в системі; 3) коефіцієнти кореляції кожного залежного ІПКС з основним, що визначає взаємозалежності між ними. Отримані коефіцієнти кореляції можуть бути використані для обрахунку середнього та сумарного рівнів критичності ситуації, що виникає під впливом декількох взаємопов'язаних і одночасних інцидентів (потенційних кризових ситуацій).

2.5. Висновки до розділу 2

У розділі було розроблено низку моделей, що дозволяють комплексно підійти до оцінювання ризиків, збитків і критичності інцидентів витоку персональних даних як на рівні окремої організації, так і в масштабах держави.

Розроблено теоретико-множинну модель представлення параметрів персональних даних у контексті відповідності вимогам Регламенту GDPR. Сформовано формальний підхід до оцінювання шкоди через введення структури з 14 параметрів, які охоплюють юридичні, технічні та організаційні аспекти обробки ПД (масштаби порушення, категорії даних, ступінь відповідальності, рівень співпраці, тощо). Запропонований підхід дозволяє відобразити вплив кожного параметра на ймовірний обсяг штрафних санкцій і репутаційних втрат, забезпечуючи основу для подальшої розробки методу оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR.

Побудовано ієрархічну структуру параметрів GDPR-моделі, що дозволило деталізувати складові оцінки відповідності дій організації вимогам законодавства. Ієрархія відображає взаємозв'язок між групами параметрів та глибиною аналізу

кожного з них, що є критичним для коректного визначення рівня відповідальності та потенційного штрафного навантаження.

Розроблено кортежну модель параметрів персональних даних, яка дозволяє формалізовано та комплексно оцінити ризики, пов’язані з обробкою персональних даних в АС. Введення дев’яти взаємопов’язаних параметрів – від ідентифікації складу ПД до механізмів управління ризиком – дало змогу створити структуровану основу для аналізу загроз і оцінки захищеності. Модель дає змогу оцінити ймовірність реалізації загроз та потенційні збитки, а також обґрунтовано визначити рівень необхідної безпеки та рекомендовану політику захисту ПД відповідно до вітчизняного законодавства.

Розроблено модель параметрів для оцінювання критичності кризових ситуацій, що дозволяє враховувати як індивідуальні характеристики інцидентів, так і їх взаємозалежність через механізм кореляції подій. Окрему увагу приділено моделюванню сукупного впливу декількох одночасних інцидентів та їх кореляції, що дозволяє підвищити точність прогнозування та реагування на надзвичайні ситуації у сфері захисту ПД. У контексті захисту ПД це дає змогу не лише відокремлювати критично небезпечні інциденти, а й визначати їх кумулятивний вплив на інформаційну систему. Такий підхід дозволяє своєчасно мобілізувати ресурси на реагування, мінімізувати втрати та забезпечити відповідність вимогам міжнародного законодавства, зокрема GDPR.

Таким чином, у розділі сформовано комплексний інструментарій для аналітики у сфері захисту персональних даних. Це включає як оцінку ризиків і збитків, так і визначення критичності інцидентів. Отримані результати мають важливе прикладне значення для формування політик безпеки, удосконалення нормативно-правових підходів до захисту ПД та розробки методів та систем оцінювання негативних наслідків від витоку персональних даних.

РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ТА СИСТЕМИ ОЦІНЮВАННЯ НЕГАТИВНИХ НАСЛІДКІВ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних

Розробка методу оцінювання негативних наслідків від порушення конфіденційності ПД за Регламентом GDPR визначається декількома ключовими аспектами [11]: вимоги GDPR; захист прав суб'єктів даних; фінансова відповідальність; підвищення свідомості та культури безпеки; ефективне управління ризиками. Оцінювання негативних наслідків дозволяє організаціям ідентифікувати потенційні ризики та визначити стратегії зменшення цих ризиків. Це важливо для забезпечення сталої відповідності та дотримання норм GDPR. Таким чином, розробка методу оцінювання негативних наслідків від порушення конфіденційності ПД допоможе організаціям ефективно впроваджувати вимоги GDPR, забезпечуючи високий рівень захисту даних та відповідального управління ризиками.

Для визначення негативних наслідків від витоку ПД, які пропонується відображати максимально наближеним штрафом застосуємо експертний підхід, який також дозволить надавати рекомендації щодо усунення проблем, які були виявлені під час аналізу інформаційної структури підприємства наглядовим органом чи власне підприємством. Пропонований метод дозволить створити автоматизовану систему оцінювання шкоди та отримання інформації про порушення відповідно до суджень експерта [81-83].

Метод орієнтований на вирішення проблем, що викликані появою прогалин у захисті ПД клієнтів і співробітників компанії та узагальнений вимогами Регламенту GDPR. Метод ґрунтується на чотирьох базових етапах [81]:

Етап 1 – Ідентифікація об’єкта оцінювання (надання інформації про підприємство);

Етап 2 – Визначення рівня порушення;

Етап 3 – Формування первинної експертної інформації: Крок 1 – Визначення показника «Специфіка порушення»; Крок 2 – Визначення показника

«Характер порушення»; Крок 3 – Визначення показника «Зниження шкоди»; Крок 4 – Визначення показника «Ступінь відповідальності»; Крок 5 – Визначення показника «Рецидив порушення»; Крок 6 – Визначення показника «Рівень співпраці»; Крок 7 – Визначення показника «Категорії даних»; Крок 8 – Визначення показника «Спосіб виявлення»; Крок 9 – Визначення показника «Відповідність заходам»; Крок 10 – Визначення показника «Дотримання кодексів»; Крок 11 – Визначення показника «Визначаючий чинник»;

Етап 4 – Фіналізована процедура обробки експертних даних: Крок 1 – Вибір рекомендацій на основі суджень експерта; Крок 2 – Підрахунок набраних балів відповідно до суджень експерта; Крок 3 – Обчислення максимально наближеного штрафу для підприємства.

Етап 1. Ідентифікація об'єкта оцінювання (надання інформації про підприємство)

Визначення глобального річного обігу підприємства за минулий рік. Формування компонента T^{φ} здійснюється шляхом визначення експертом річного обігу в €. Даний компонент методу немає розгалужень та має лише 1 елемент. Наприклад, якщо компанія за минулий фінансовий рік мала глобальний річний обіг 3 млрд. €, то даний компонент матиме наступний вигляд [83]:

$$T^{\varphi} = 3\,000\,000\,000\ €, \tag{3.1}$$

де: T^{φ} = «загальний глобальний річний обіг підприємства за минулий фінансовий рік».

Етап 2. Визначення рівня порушення

Показник рівня порушення $P_{РП}^{\varphi}$ обчислюється на основі множини визначених рівнів порушення, відносно яких формується коефіцієнт максимально можливого збитку. Для визначення показника рівня порушення $P_{РП}^{\varphi}$ для φ-го об'єкту скористаємося виразом: $P_{РП}^{\varphi} = \bigvee_{i=1}^{n_1} \bigvee_{j=1}^{n_{1i}} B_{ij}^{\varphi L} C_{ij}^{\varphi L} = (B_{11}^{\varphi L} C_{11}^{\varphi L} \vee B_{12}^{\varphi L} C_{12}^{\varphi L} \vee ... \vee B_{1n_{11}}^{\varphi L} C_{1n_{11}}^{\varphi L}) \vee$

$$(B_{21}^{\varphi L} C_{21}^{\varphi L} \vee B_{22}^{\varphi L} C_{22}^{\varphi L} \vee ... \vee B_{2n_{12}}^{\varphi L} C_{2n_{12}}^{\varphi L}) \vee ... \vee (B_{n_1 1}^{\varphi L} C_{n_1 1}^{\varphi L} \vee B_{n_1 2}^{\varphi L} C_{n_1 2}^{\varphi L} \vee ... \vee B_{n_1 n_{1n1}}^{\varphi L} C_{n_1 n_{1n1}}^{\varphi L}), \tag{3.2}$$

де $B_{ij}^{\varphi L} = \begin{cases} 1 \ \textit{при} \ b(L_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(L_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(L_{ij}^{\varphi})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти L_{ij}^{φ} підмножини $\mathbf{L_i^{\varphi}}$ (див. (2.6)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими. Слід зазначити, що коефіцієнт максимально-можливого збитку буде становити 0,04 від компоненти T^{φ} = «Загальний глобальний річний обіг підприємства за минулий фінансовий рік», так як коефіцієнти не додаються, а серед двох вибирається більший, що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства.

Етап 3. Формування первинної експертної інформації

Крок 1. Визначення показника «Специфіка порушення»

Для визначення показника специфіки порушення $P_{СП}^{\varphi}$ для φ-го об'єкту скористаємося виразом: $P_{СП}^{\varphi} = \sum_{i=1}^{n_2} \bigvee_{j=1}^{n_{2i}} B_{ij}^{\varphi N} C_{ij}^{\varphi N} = (B_{11}^{\varphi N} C_{11}^{\varphi N} \vee B_{12}^{\varphi N} C_{12}^{\varphi N} \vee ... \vee B_{1n_{21}}^{\varphi N} C_{1n_{21}}^{\varphi N}) +$

$$(B_{21}^{\varphi N} C_{21}^{\varphi N} \vee B_{22}^{\varphi N} C_{22}^{\varphi N} \vee ... \vee B_{2n_{22}}^{\varphi N} C_{2n_{22}}^{\varphi N}) + ... + (B_{n_2 1}^{\varphi N} C_{n_2 1}^{\varphi N} \vee B_{n_2 2}^{\varphi N} C_{n_2 2}^{\varphi N} \vee ... \vee B_{n_2 n_{2n_2}}^{\varphi N} C_{n_2 n_{2n_2}}^{\varphi N}), \qquad (3.3)$$

де $B_{ij}^{\varphi N} = \begin{cases} 1 \ \textit{при} \ b(N_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(N_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(N_{ij}^{\varphi})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти N_{ij}^{φ} підмножини $\mathbf{N_i^{\varphi}}$ (див. (2.10)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 2. Визначення показника «Характер порушення»

Визначимо показник характеру порушення $P_{ХП}^{\varphi}$ для φ-го об'єкту:

$$\begin{aligned} P_{ХП}^{\varphi} = \sum_{i=1}^{n_3} \bigvee_{j=1}^{n_{3i}} B_{ij}^{\varphi CH} C_{ij}^{\varphi CH} &= (B_{11}^{\varphi CH} C_{11}^{\varphi CH} \vee B_{12}^{\varphi CH} C_{12}^{\varphi CH} \vee ... \vee B_{1n_{31}}^{\varphi CH} C_{1n_{31}}^{\varphi CH}) + \\ &(B_{21}^{\varphi CH} C_{21}^{\varphi CH} \vee B_{22}^{\varphi CH} C_{22}^{\varphi CH} \vee ... \vee B_{2n_{32}}^{\varphi CH} C_{2n_{32}}^{\varphi CH}) + ... \\ &+ (B_{n_3 1}^{\varphi CH} C_{n_3 1}^{\varphi CH} \vee B_{n_3 2}^{\varphi CH} C_{n_3 2}^{\varphi CH} \vee ... \vee B_{n_3 n_{3n_3}}^{\varphi CH} C_{n_3 n_{3n_3}}^{\varphi CH}), \end{aligned} \qquad (3.4)$$

де $B_{ij}^{\varphi CH} = \begin{cases} 1 \ \textit{при} \ b(CH_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(CH_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(CH_{ij}^{\varphi})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти CH_{ij}^{φ} підмножини $\mathbf{CH_i^{\varphi}}$ (див. (2.14)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими [83].

Крок 3. Визначення показника «Зниження шкоди»

Для визначення показника зниження шкоди $P_{ЗШ}^{\varphi}$ для φ-го об'єкту скористаємося виразом: $P_{ЗШ}^{\varphi} = \sum_{i=1}^{n_4} \bigvee_{j=1}^{n_{4i}} B_{ij}^{\varphi A} C_{ij}^{\varphi A} = (B_{11}^{\varphi A} C_{11}^{\varphi A} \vee B_{12}^{\varphi A} C_{12}^{\varphi A} \vee ... \vee B_{1n_{41}}^{\varphi A} C_{1n_{41}}^{\varphi A}) +$

$$(B_{21}^{\varphi A} C_{21}^{\varphi A} \vee B_{22}^{\varphi A} C_{22}^{\varphi A} \vee ... \vee B_{2n_{42}}^{\varphi A} C_{2n_{42}}^{\varphi A}) + ... + (B_{n_4 1}^{\varphi A} C_{n_4 1}^{\varphi A} \vee B_{n_4 2}^{\varphi A} C_{n_4 2}^{\varphi A} \vee ... \vee B_{n_4 n_{4n_4}}^{\varphi A} C_{n_4 n_{4n_4}}^{\varphi A}), \quad (3.5)$$

де $B_{ij}^{\varphi A} = \begin{cases} 1 \ \textit{при} \ b(A_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(A_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(A_{ij}^{\varphi})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти A_{ij}^{φ} підмножини $\mathbf{A_i^{\varphi}}$ (див. (2.18)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 4. Визначення показника «Ступінь відповідальності»

Для визначення показника ступінь відповідальності P_{CB}^{φ} для φ-го об'єкту скористаємося виразом: $P_{CB}^{\varphi} = \sum_{i=1}^{n_5} \bigvee_{j=1}^{n_{5i}} B_{ij}^{\varphi R} C_{ij}^{\varphi R} = (B_{11}^{\varphi R} C_{11}^{\varphi R} \vee B_{12}^{\varphi R} C_{12}^{\varphi R} \vee ... \vee B_{1n_{51}}^{\varphi R} C_{1n_{51}}^{\varphi R}) +$

$$(B_{21}^{\varphi R} C_{21}^{\varphi R} \vee B_{22}^{\varphi R} C_{22}^{\varphi R} \vee ... \vee B_{2n_{52}}^{\varphi R} C_{2n_{52}}^{\varphi R}) + ... + (B_{n_5 1}^{\varphi R} C_{n_5 1}^{\varphi R} \vee B_{n_5 2}^{\varphi R} C_{n_5 2}^{\varphi R} \vee ... \vee B_{n_5 n_{5n_5}}^{\varphi R} C_{n_5 n_{5n_5}}^{\varphi R}), \quad (3.6)$$

де $B_{ij}^{\varphi R} = \begin{cases} 1 \ \textit{при} \ b(R_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(R_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(R_{ij}^{\varphi})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти R_{ij}^{φ} підмножини $\mathbf{R_i^{\varphi}}$ (див. (2.22)) в результаті

поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 5. Визначення показника «Рецидив порушення»

Для визначення показника рецидив порушення $P^{\varphi}_{РЦП}$ для φ-го об'єкту скористаємося виразом: $P^{\varphi}_{РЦП} = \sum_{i=1}^{n_6} \bigvee_{j=1}^{n_{6i}} B^{\varphi I}_{ij} C^{\varphi I}_{ij} = (B^{\varphi I}_{11} C^{\varphi I}_{11} \vee B^{\varphi I}_{12} C^{\varphi I}_{12} \vee ... \vee B^{\varphi I}_{1n_{61}} C^{\varphi I}_{1n_{61}}) +$

$$(B^{\varphi I}_{21} C^{\varphi I}_{21} \vee B^{\varphi I}_{22} C^{\varphi I}_{22} \vee ... \vee B^{\varphi I}_{2n_{62}} C^{\varphi I}_{2n_{62}}) + ... + (B^{\varphi I}_{n_6 1} C^{\varphi I}_{n_6 1} \vee B^{\varphi I}_{n_6 2} C^{\varphi I}_{n_6 2} \vee ... \vee B^{\varphi I}_{n_6 n_{6n_6}} C^{\varphi I}_{n_6 n_{6n_6}}), \quad (3.7)$$

де $B^{\varphi I}_{ij} = \begin{cases} 1 \ \textit{при} \ b(I^{\varphi}_{ij}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(I^{\varphi}_{ij}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(I^{\varphi}_{ij})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти I^{φ}_{ij} підмножини $\mathbf{I^{\varphi}_i}$ (див. (2.32)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 6. Визначення показника «Рівень співпраці»

Для визначення показника рівень співпраці $P^{\varphi}_{РС}$ для φ-го об'єкту скористаємося виразом: $P^{\varphi}_{РС} = \sum_{i=1}^{n_7} \bigvee_{j=1}^{n_{7i}} B^{\varphi C}_{ij} C^{\varphi C}_{ij} = (B^{\varphi C}_{11} C^{\varphi C}_{11} \vee B^{\varphi C}_{12} C^{\varphi C}_{12} \vee ... \vee B^{\varphi C}_{1n_{71}} C^{\varphi C}_{1n_{71}}) +$

$$(B^{\varphi C}_{21} C^{\varphi C}_{21} \vee B^{\varphi C}_{22} C^{\varphi C}_{22} \vee ... \vee B^{\varphi C}_{2n_{72}} C^{\varphi C}_{2n_{72}}) + ... + (B^{\varphi C}_{n_7 1} C^{\varphi C}_{n_7 1} \vee B^{\varphi C}_{n_7 2} C^{\varphi C}_{n_7 2} \vee ... \vee B^{\varphi C}_{n_7 n_{7n_7}} C^{\varphi C}_{n_7 n_{7n_7}}), \quad (3.8)$$

де $B^{\varphi C}_{ij} = \begin{cases} 1 \ \textit{при} \ b(C^{\varphi}_{ij}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(C^{\varphi}_{ij}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(C^{\varphi}_{ij})$ - бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти C^{φ}_{ij} підмножини $\mathbf{C^{\varphi}_i}$ (див. (2.36)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 7. Визначення показника «Категорії даних»

Для визначення показника категорії даних $P^{\varphi}_{КД}$ для φ-го об'єкту скористаємося виразом: $P^{\varphi}_{КД} = \sum_{i=1}^{n_8} \bigvee_{j=1}^{n_{8i}} B^{\varphi CA}_{ij} C^{\varphi CA}_{ij} = (B^{\varphi CA}_{11} C^{\varphi CA}_{11} \vee B^{\varphi CA}_{12} C^{\varphi CA}_{12} \vee ... \vee B^{\varphi CA}_{1n_{81}} C^{\varphi CA}_{1n_{81}}) + (B^{\varphi CA}_{21} C^{\varphi CA}_{21} \vee$

$$B_{22}^{\varphi CA}C_{22}^{\varphi CA} \vee ... \vee B_{2n_{82}}^{\varphi CA}C_{2n_{82}}^{\varphi CA}) + ... + (B_{n_8 1}^{\varphi CA}C_{n_8 1}^{\varphi CA} \vee B_{n_8 2}^{\varphi CA}C_{n_8 2}^{\varphi CA} \vee ... \vee B_{n_8 n_{8n_8}}^{\varphi CA}C_{n_8 n_{8n_8}}^{\varphi CA}), \quad (3.9)$$

де $B_{ij}^{\varphi CA} = \begin{cases} 1 \ при \ b(CA_{ij}^{\varphi}) = «TRUE» \\ 0 \ при \ b(CA_{ij}^{\varphi}) = «FALSE», \end{cases}$

а $b(CA_{ij}^{\varphi})$- бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти CA_{ij}^{φ} підмножини $\mathbf{CA_i^{\varphi}}$ (див. (2.40)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 8. Визначення показника «Спосіб виявлення»

Для визначення показника $P_{СПВ}^{\varphi}$ для φ-го об'єкту скористаємося виразом:

$$\begin{aligned} P_{СПВ}^{\varphi} = \sum_{i=1}^{n_9} \bigvee_{j=1}^{n_{9i}} B_{ij}^{\varphi M}C_{ij}^{\varphi M} = (B_{11}^{\varphi M}C_{11}^{\varphi M} \vee B_{12}^{\varphi M}C_{12}^{\varphi M} \vee ... \vee B_{1n_{91}}^{\varphi M}C_{1n_{91}}^{\varphi M}) + \\ (B_{21}^{\varphi M}C_{21}^{\varphi M} \vee B_{22}^{\varphi M}C_{22}^{\varphi M} \vee ... \vee B_{2n_{92}}^{\varphi M}C_{2n_{92}}^{\varphi M}) + ... + \\ (B_{n_9 1}^{\varphi M}C_{n_9 1}^{\varphi M} \vee B_{n_9 2}^{\varphi M}C_{n_9 2}^{\varphi M} \vee ... \vee B_{n_9 n_{9n_9}}^{\varphi M}C_{n_9 n_{9n_9}}^{\varphi M}), \end{aligned} \quad (3.10)$$

де $B_{ij}^{\varphi M} = \begin{cases} 1 \ при \ b(M_{ij}^{\varphi}) = «TRUE» \\ 0 \ при \ b(M_{ij}^{\varphi}) = «FALSE», \end{cases}$

а $b(M_{ij}^{\varphi})$- бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти M_{ij}^{φ} підмножини $\mathbf{M_i^{\varphi}}$ (див. (2.52)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 9. Визначення показника «Відповідність заходам»

Для визначення показника $P_{ВЗ}^{\varphi}$ для φ-го об'єкту скористаємося виразом:

$$\begin{aligned} P_{ВЗ}^{\varphi} = \sum_{i=1}^{n_{10}} \bigvee_{j=1}^{n_{10i}} B_{ij}^{\varphi ME}C_{ij}^{\varphi ME} = (B_{11}^{\varphi ME}C_{11}^{\varphi ME} \vee B_{12}^{\varphi ME}C_{12}^{\varphi ME} \vee ... \vee B_{1n_{101}}^{\varphi ME}C_{1n_{101}}^{\varphi ME}) + \\ (B_{21}^{\varphi ME}C_{21}^{\varphi ME} \vee B_{22}^{\varphi ME}C_{22}^{\varphi ME} \vee ... \vee B_{2n_{102}}^{\varphi ME}C_{2n_{102}}^{\varphi ME}) + ... + \\ (B_{n_{10}1}^{\varphi ME}C_{n_{10}1}^{\varphi ME} \vee B_{n_{10}2}^{\varphi ME}C_{n_{10}2}^{\varphi ME} \vee ... \vee B_{n_{10}n_{10m_{10}}}^{\varphi ME}C_{n_{10}n_{10m_{10}}}^{\varphi ME}), \end{aligned} \quad (3.11)$$

де $B_{ij}^{\varphi ME} = \begin{cases} 1 \ \textit{при} \ b(ME_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(ME_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(ME_{ij}^{\varphi})$- бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти ME_{ij}^{φ} підмножини $\mathbf{ME_i^{\varphi}}$ (див. (2.60)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими [82].

Крок 10. Визначення показника «Дотримання кодексів»

Визначимо показник дотримання кодексів $P_{ДК}^{\varphi}$ для φ-го об'єкту:

$$P_{ДК}^{\varphi} = \sum_{i=1}^{n_{11}} \bigvee_{j=1}^{n_{11i}} B_{ij}^{\varphi AD} C_{ij}^{\varphi AD} = (B_{11}^{\varphi AD} C_{11}^{\varphi AD} \vee B_{12}^{\varphi AD} C_{12}^{\varphi AD} \vee ... \vee B_{1n_{111}}^{\varphi AD} C_{1n_{111}}^{\varphi AD}) + (B_{21}^{\varphi AD} C_{21}^{\varphi AD} \vee B_{22}^{\varphi AD} C_{22}^{\varphi AD} \vee ... \vee B_{2n_{112}}^{\varphi AD} C_{2n_{112}}^{\varphi AD}) + ... + (B_{n_{11}1}^{\varphi AD} C_{n_{11}1}^{\varphi AD} \vee B_{n_{11}2}^{\varphi AD} C_{n_{11}2}^{\varphi AD} \vee ... \vee B_{n_{11}n_{11n_{11}}}^{\varphi AD} C_{n_{11}n_{11n_{11}}}^{\varphi AD}), \quad (3.12)$$

де $B_{ij}^{\varphi AD} = \begin{cases} 1 \ \textit{при} \ b(AD_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(AD_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(AD_{ij}^{\varphi})$- бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти AD_{ij}^{φ} підмножини $\mathbf{AD_i^{\varphi}}$ (див. (2.68)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Крок 11. Визначення показника «Визначаючий чинник»

Для визначення показника визначаючий чинник $P_{ВЧ}^{\varphi}$ для φ-го об'єкту скористаємося виразом: $P_{ВЧ}^{\varphi} = \sum_{i=1}^{n_{12}} \bigvee_{j=1}^{n_{12i}} B_{ij}^{\varphi F} C_{ij}^{\varphi F} = (B_{11}^{\varphi F} C_{11}^{\varphi F} \vee B_{12}^{\varphi F} C_{12}^{\varphi F} \vee ... \vee B_{1n_{121}}^{\varphi ME} C_{1n_{121}}^{\varphi ME}) + (B_{21}^{\varphi F} C_{21}^{\varphi F} \vee B_{22}^{\varphi F} C_{22}^{\varphi F} \vee ... \vee B_{2n_{122}}^{\varphi F} C_{2n_{122}}^{\varphi F}) + ... + (B_{n_{12}1}^{\varphi F} C_{n_{12}1}^{\varphi F} \vee B_{n_{12}2}^{\varphi F} C_{n_{12}2}^{\varphi F} \vee ... \vee B_{n_{12}n_{12n_{12}}}^{\varphi F} C_{n_{12}n_{12n_{12}}}^{\varphi F}), \quad (3.13)$

де $B_{ij}^{\varphi F} = \begin{cases} 1 \ \textit{при} \ b(F_{ij}^{\varphi}) = \text{«}TRUE\text{»} \\ 0 \ \textit{при} \ b(F_{ij}^{\varphi}) = \text{«}FALSE\text{»}, \end{cases}$

а $b(F_{ij}^{\varphi})$- бінарна функція, яка приймає значення «TRUE» або «FALSE» в залежності від того, які компоненти F_{ij}^{φ} підмножини $\mathbf{F_i^{\varphi}}$ (див. (2.76)) в результаті поточного оцінювання було відповідно визначено істинними або помилковими.

Звернемо увагу, що в процесі оцінювання (кроки 1÷11) вибір певних характеристик порушення засновується на конкретних оцінках діяльності підприємства, які в результаті сформують значення показників $P_{СП}^{\varphi}$, $P_{ХП}^{\varphi}$, $P_{ЗШ}^{\varphi}$, $P_{СВ}^{\varphi}$, $P_{РЦП}^{\varphi}$, $P_{РС}^{\varphi}$, $P_{КД}^{\varphi}$, $P_{СПВ}^{\varphi}$, $P_{ВЗ}^{\varphi}$, $P_{ДК}^{\varphi}$ та $P_{ВЧ}^{\varphi}$, що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства.

Етап 4. Фіналізована процедура обробки експертних даних

Крок 1. Вибір рекомендацій на основі суджень експерта

Для вибору рекомендацій необхідно отримати множину $\mathbf{RE}$ та підмножину $\mathbf{RE_i}$, які утворять:

$$\{\bigcup_{i=1}^{n_{13}} \mathbf{RE_i^{\varphi}}\} = \{\mathbf{RE_1^{\varphi}}, \mathbf{RE_2^{\varphi}}, ..., \mathbf{RE_{n_{13}}^{\varphi}}\}, \tag{3.14}$$

де $\mathbf{RE_i^{\varphi}} \subseteq \mathbf{RE^{\varphi}}$ $(i = \overline{1, n_{13}})$ визначимо як:

$$\mathbf{RE_i^{\varphi}} = \{\bigcup_{j=1}^{n_{13i}} RE_{ij}^{\varphi}\} = \{RE_{i1}^{\varphi}, RE_{i2}^{\varphi}, ..., RE_{in_{13i}}^{\varphi}\}, \tag{3.15}$$

де $RE_{ij}^{\varphi} \subseteq \mathbf{RE_i^{\varphi}}$ $(j = \overline{1, n_{13i}})$ – j-а підмножина груп вжитих дій для зниження рівня шкоди споріднених за певною темою чи близьких за певними характеристиками у межах i-ї підмножини, а n_{13i} кількість груп i-ї підмножини.

З урахуванням (3.15) вираз (3.14) зможемо відобразити в наступному вигляді:

$$\begin{aligned}\{\bigcup_{i=1}^{n_{13}} \mathbf{RE_i^{\varphi}}\} = \{\bigcup_{i=1}^{n_{13}} \{\bigcup_{j=1}^{n_{13i}} RE_{ij}^{\varphi}\}\} = \{\{RE_{11}^{\varphi}, RE_{12}^{\varphi}, ..., RE_{1n_{13i}}^{\varphi}\},\\ \{RE_{21}^{\varphi}, RE_{22}^{\varphi}, ..., RE_{2n_{13i}}^{\varphi}\}, ..., \{RE_{n_{13}1}^{\varphi}, RE_{n_{13}2}^{\varphi}, ..., RE_{n_{13}n_{13i}}^{\varphi}\}\},\end{aligned} \tag{3.16}$$

Таким чином, з урахуванням $RE_{ij} \subseteq \mathbf{RE_i}$ відносно j-го параметра система автоматично вибирає рекомендації для зниження рівня заподіяної шкоди. Всі рекомендації виставляються тільки для Етапу 3, відповідно до суджень експерта

та своєї приналежності до певної категорії.

Крок 2. Підрахунок набраних балів відповідно до суджень експерта

Для виконання даного кроку необхідно використати значення показників, отриманих на Етапі 3 на основі виразів (3.3) - (3.13). Сумарне значення для кожного виразу присвоюється його власному ідентифікатору P_i^{φ}. Саме тому, для того щоб порахувати набрану кількість балів з усіх етапів, необхідно просумувати значення їх ідентифікаторів. Даний вираз матиме наступний вигляд:

$$\sum_{i=1}^{11} P_i^{\varphi} = P_{СП}^{\varphi} + P_{ХП}^{\varphi} + P_{ЗШ}^{\varphi} + P_{СВ}^{\varphi} + P_{РЦП}^{\varphi} + P_{РС}^{\varphi} + P_{КД}^{\varphi} + P_{СПВ}^{\varphi} + P_{ВЗ}^{\varphi} + P_{ДК}^{\varphi} + P_{ВЧ}^{\varphi}, \quad (3.17)$$

де $P_i^{\varphi} \subseteq \mathbf{P}^{\boldsymbol{\varphi}}$ $(i = \overline{1,11})$ – сума всіх набраних балів виходячи із суджень експерта.

Максимальна сума для всіх кроків Етапу 3 складає 160 балів. Тому, виходячи з цього, введемо змінну TMC^{φ}, що буде містити коефіцієнт обчисленої кількості отриманих балів (total marks coefficient) для всіх 11 кроків Етапу 3. Саме тому, формула матиме наступний вигляд:

$$TMC^{\varphi} = \sum_{i=1}^{11} P_i^{\varphi} \,/\, 160. \quad (3.18)$$

Крок 3. Обчислення максимально-наближеного штрафу для підприємства

Для виконання даного етапу, необхідно використати дані з Етапу 1 та Етапу 2. Це такі формули як: (3.1) та (3.2). Для того, щоб порахувати максимальний збиток для підприємства, вводимо нову змінну MF^{φ}, що буде відповідати за максимальний штраф (maximum fine). Для неї, формула матиме наступний вигляд:

$$MF^{\varphi} = T^{\varphi} \times P_{СП}^{\varphi}. \quad (3.19)$$

Для обчислення максимально наближеного штрафу (МНШ), необхідно ввести кінцеву зміну AF^{φ}, яка буде відповідати за обчислення МНШ (approximate fine) та матиме наступний вигляд [81]:

$$AF^{\varphi} = MF^{\varphi} \times TMC^{\varphi}. \quad (3.20)$$

Розроблено метод оцінювання негативних наслідків від порушення

конфіденційності ПД відповідно до положень Регламенту GDPR, який за рахунок етапів ідентифікації об’єкта оцінювання (надання інформації про підприємство), визначення рівня порушення, формування первинної експертної інформації та фіналізованої процедури обробки експертних даних, що здійснюють аналітичне перетворення множин вхідних даних розробленої моделі інтегрованого представлення параметрів, значень величин, що відображають судження експертів, розроблених нових правил оцінювання, розсіювання балів та визначеної множини рекомендацій дозволяє визначати величину максимального та фактичного збитків для організації у разі порушення конфіденційності ПД та надавати рекомендації щодо вибору політики безпеки ПД і послуг безпеки відповідно до функціонального профілю захищеності. Для реалізації розробленого методу необхідно розробити автоматизовану систему оцінювання потенційних фінансових наслідків від витоку ПД, що дозволить організаціям ефективно впроваджувати вимоги GDPR забезпечуючи високий рівень захисту даних.

3.2. Метод оцінювання безпеки персональних даних

Кортежна модель (див. підрозділ 2.3), забезпечує формалізоване представлення критичних параметрів, що впливають на рівень захищеності персональних даних в автоматизованих системах. Проте сама модель є лише структурною основою – без розробки відповідного методу оцінювання вона не може бути застосована у практичних сценаріях для аналізу, прогнозування або прийняття рішень щодо заходів безпеки. Метод дозволить перейти від декларативного опису параметрів до алгоритмічного обчислення рівня ризику втрати ПД з урахуванням взаємозв’язків між компонентами моделі.

Етап 1. Визначаємо документи у яких наявні ПД та коефіцієнт їх важливості, відповідно до табл. 2.2. Сумарна величина коефіцієнтів важливості визначається за формулами (3.21), (3.22) [68]:

$$K_{vd}=\sum_{i=1}^{n}K_{vd_n},(i=\overline{1,n}),K_{vd}=K_{vd_1}+K_{vd_2}+K_{vd_3}...+K_{vd_i}, \qquad (3.21)$$

Наступним кроком відбувається визначення середовища обробки ПД, що містяться у вказаних документах, відповідно до таблиці 2.3. Аналогічно, за формулою (3.21), визначаються коефіцієнти K_v та K_{vr} для ПЗ обробки ПД. Визначення максимально можливого розрахункового значення ризику R_{max} знаходиться за відношенням суми коефіцієнтів важливості всіх об'єктів (документів та ПЗ), що знаходяться під загрозою, до сумарної величини коефіцієнтів важливості об'єктів та визначається за формулою:

$$R_{max}=(K_{vdr}+K_{vpr})/(K_{vd}+K_{vp}) \tag{3.22}$$

Проте, для оцінки ризику захисту ПД, необхідно дослідити використані в АС механізми безпеки ПД, існуючі загрози захисту ПД та визначити відповідний їм рівень реалізації.

Етап 2. На даному етапі проводиться аналіз функціонуючих механізмів безпеки. Кожен із запропонованих механізмів безпеки в моделі забезпечує корегування визначеного максимально можливого розрахункового значення ризику на коефіцієнт 0,2. Нехай в АС наявні 3 механізми безпеки (D_i, $i=1\div3$), тоді сумарний коефіцієнт

$$K_m=\sum_{n=1}^{i} D_n\times 0{,}2,(i=\overline{1,n}), \tag{3.23}$$

Етап 3. Передбачається ідентифікація можливих загроз ПД. Перелік цих загроз (**F**) визначається запропонованим методом. Згідно формули (2.82), якщо у всіх обраних загрозах було визначено «низький» рівень загрози, то $P_{riv\_zag}=0{,}3$, якщо встановлено хоча б один «середній» рівень», то $P_{riv\_zag}=0{,}6$ та хоча б один «високий» – $P_{riv\_zag}=1$. Тоді розрахункове значення ризику з урахуванням рівня реалізації загроз $R_{zag_{corr}}$ корегується і визначатиметься за формулою:

$$R_{zag_{corr}}=P_{riv\_zag}\times R_{max}. \tag{3.24}$$

Після розрахунку $R_{zag_{corr}}$, визначимо розрахунковий інтервал – в межах якого і знаходиться реальний ризик захисту ПД. Весь інтервал $I\in(I_{min},I_{max})$ згідно таблиці 2.4 поділено на підінтервали [0÷0,1], [0,1÷0,3], [0,3÷0,6], [0,6÷0,8],

[0,8÷1].

Етап 4. Визначення величини можливого збитку від витоку ПД може визначатися як кількісними, так і якісними показниками. Згідно до розробленого методу ПД в БПД, а саме таблиці 2.4, наведено шкали показників величин можливих збитків: розрахунковий інтервал ризику можливого витоку ПД; грошовий еквівалент ризику можливих збитків; бальна оцінка ризику втрати ПД.

Етап 5. Проводиться оцінка ризиків захисту ПД. На даному етапі визначається корекція ймовірності з врахуванням механізмів захисту (R_{C_corr}) за формулою:

$$R_{C\_corr}=(I_{min}+(I_{max}-I_{min})\times(1-K_m)),I\in(I_{min},I_{max}). \quad (3.25)$$

Даний інтервал витоку ПД визначається збитками в грошовому еквіваленті на рівні $G\in(G_{min},G_{max})$. Таким чином ймовірні збитки в грошах, визначаються як:

$$R_g=G_{min}+(G_{max}-G_{min})\times R_{C\_corr}. \quad (3.26)$$

Етап 6. Керування ризиком захисту ПД. Після проведення аналізу та оцінки ризиків ПД в БПД, можна сформувати кінцеві висновки про стан рівня захищеності ПД в конкретній АС. А отже, можна надати рекомендації щодо підвищення цього стану, а саме через впровадження тих чи інших механізмів безпеки, що запропоновані в таблиці 2.6.

Отже, розроблено метод оцінювання безпеки персональних даних в АС, який оснований на положеннях міжнародного стандарту ISO/IEC 27005 у відповідності до вимог діючого законодавства України. Розроблений метод захисту ПД в державних АС, який орієнтований на те, що власником системи є держава і в цих системах обробляється інформація з обмеженим доступом (насамперед, ПД), дає можливість визначити достатні заходи та способи (механізми) захисту для забезпечення необхідного рівня захищеності за допустимих затратах і заданому рівні обмежень видів інформаційної діяльності. Окремо розроблений метод може бути додатковим заходом до комплексу існуючих щодо захисту державних інформаційних ресурсів або інформації з обмеженим доступом (насамперед ПД, що належать до конфіденційної інформації) під час її обробки в інформаційних системах.

3.3. Метод оцінювання рівня критичності у разі витоку персональних даних

В роботах [77, 78] описані методи виявлення та ідентифікації інцидентів / потенційних кризових ситуацій, а також оцінювання рівня критичності інцидентів, які засновані на нечіткій логіці та методах експертного оцінювання. Проте в цих роботах неврахована ситуація появи декількох (двох і більше) кризових ситуацій одночасно, їх узгодження та визначення середнього та сумарного рівня критичності. Тому необхідно розробити метод оцінювання рівня критичності у разі витоку персональних даних на основі механізму кореляції інцидентів інформаційної безпеки та визначення середнього та сумарного рівня критичності спричиненого ними впливу на інформаційну систему з застосуванням методів нечіткої логіки.

Сам механізм має кілька етапів, зокрема [80]:

Етап 1. Визначення кількості кризових ситуацій, з якими проводяться операції, та наборів оціночних параметрів для кожної з них. Для визначення кількості кризових ситуацій, з якими проводяться операції та самих кризових ситуацій скористаємося формулою (2.86). Відповідно для кожного з цих інцидентів характерні свої набори оціночних параметрів (див.2.87-2.88).

Етап 2. Визначення основної і залежних кризових ситуацій. Для визначення залежності між кризовими ситуаціями (ІПКС) введемо дві категорії подій: основна та залежні від неї інциденти. Можна виділити два способи розподілення і привласнення значення основної та залежних подій, такі як: за часом – ІПКС, який був виявлений першим набуває статусу основного, а всі інші – залежних від нього ІПКС; за рівнем критичності – статус основного ІПКС привласнюється інциденту з найбільшим рівнем критичності. В такому разі необхідно провести процедуру ранжування ІПКС за рівнем критичності. Зібрані відомості про КС формують значення оціночних параметрів, які обробляються (шляхом визначення коефіцієнту важливості, проведення їхньої фазифікації, обраховування як суми з врахуванням коефіцієнта важливості і дефазифікації) і визначають загальний рівень критичності ситуації, що склалася в результаті

впливу ІПКС.

Етап 3. Визначення коефіцієнтів кореляції для кожного залежного та основного ІПКС відповідно. Оскільки коефіцієнт кореляції дає змогу оцінити залежність ІПКС між собою і направлений на оцінку середнього та сумарного впливу їх сукупності за певним аспектом, то можливий випадок коли основний ІПКС вибирається експертом або оператором системи, користувачем, виходячи з позицій який з аспектів КС він вважає найбільш загрозливим. Коефіцієнт кореляції показує однакові аспекти впливу різних ІПКС і визначається кількістю спільних параметрів між основною та залежною подіями за формулою: $K_{IKS_{осн}IKS_{зал_i}} = \frac{|(\mathbf{L}_{\mathbf{осн}} \cap \mathbf{L}_{\mathbf{зал_i}})|}{|\mathbf{L}_{\mathbf{зал_i}}|}$, до тих пір, поки не будуть враховані всі залежності між ІПКС, причому $\mathbf{L}_{\mathbf{осн}}$ – множина оціночних параметрів основного ІПКС і $\mathbf{L}_{\mathbf{зал}}$ – множина оціночних параметрів залежних ІПКС. Таким чином, як зазначалось раніше, коефіцієнт кореляції може приймати значення від 0 (абсолютно незалежні події) до 1 (повністю залежні події).

Далі розглянемо проблему визначення середнього та сумарного рівнів критичності для набору тих чи інших виявлених ІПКС. Скористаємось для визначення середнього рівня критичності ситуації, що виникла впливом декількох одночасних інцидентів, наступними формулами:

– без врахування коефіцієнта кореляції: $\underset{\sim}{LCS}_{сер} = \frac{1}{N}\sum_{i=1}^{N}\underset{\sim}{LCS}_i$, де $\underset{\sim}{LCS}_{сер}$ - середній рівень критичності декількох ІПКС з врахуванням залежності між ними, $\underset{\sim}{LCS}_{осн}$ - рівень критичності основного ІПКС, $\underset{\sim}{LCS}_i$ - рівень критичності *i*-ого ІПКС, N - загальна кількість інцидентів.

– з врахуванням коефіцієнта кореляції, для оцінки рівня критичності в конкретному аспекті прояву ідентифікованих ІПКС: $\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{N}(\underset{\sim}{LCS}_{осн} + \sum_{i=2}^{N} K_{IKS_{осн}IKS_{заг_i}} * \underset{\sim}{LCS}_i)$, де $\underset{\sim}{LCS}_{сер}$ – середній рівень критичності

декількох ІПКС з врахуванням залежності між ними, $\underset{\sim}{LCS}_{осн}$ – рівень критичності основного ІПКС, $\underset{\sim}{LCS}_i$ – рівень критичності інших (залежних) ІПКС і $K_{IKS_{осн}IKS_{заг_i}}$ – коефіцієнт кореляції між основним та залежним ІПКС, N – загальна кількість інцидентів.

Схематично процес знаходження середнього рівня критичності ІПКС та відповідних коефіцієнтів кореляції зображено на рисунку 3.1.

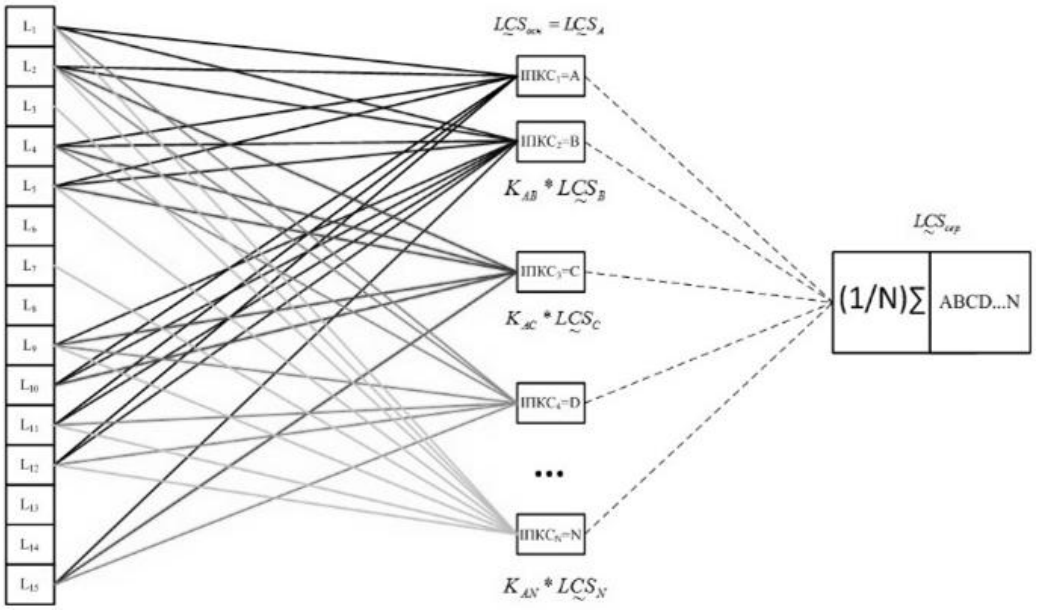


Рис. 3.1. Механізм кореляції ІПКС для визначення середнього рівня критичності ситуації

Сумарний рівень критичності ситуації, що виникла внаслідок впливу сукупності інцидентів важлива для вибору адекватних заходів для реагування на них. Це пояснюється тим, що контрзаходи, підібрані лише для одного ІПКС будуть не достатніми для нейтралізації їх сукупності, оскільки кожен інцидент привносить свою частку до зростаючого загального рівня. У випадку, якщо рівень критичності окремого інциденту оцінюється від 0 до 100 балів, то ймовірно, що сумарний рівень буде перевищувати 100 балів. Така ситуація є недопустимою. Очевидно, що в такому разі визначення сумарного рівня не можна здійснювати банальним додаванням рівнів критичності окремих ІПКС. Скористаємось для цього формулою Шортліффа, яка використовуються для визначення міри довіри

двом і більше свідченням, що взаємопов'язані, в прийняті рішень експертними системами. Замінивши в ній «міру довіри» на «рівень критичності» зможемо її використати для нашої задачі.

Узагальнивши і систематизувавши сформуємо формулу визначення сумарного рівня критичності для n інцидентів (потенційних кризових ситуацій) при відсутності кореляції між ними: $\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_N + \sum_{i=1}^{N-1} \underset{\sim}{LCS}_i \prod_{i=i+1}^{N} (1 - \underset{\sim}{LCS}_i)$, де $\underset{\sim}{LCS}_{сум}$ – сумарний рівень критичності декількох ІПКС без врахуванням залежності між ними (кореляції), $\underset{\sim}{LCS}_i$ – рівень критичності *i*-ого ІПКС, N – загальна кількість інцидентів. Аналогічно до середнього значення рівня критичності можемо застосувати до виявлених ІПКС механізм кореляції подій. Тоді сумарний рівень критичності з врахуванням залежності між окремими інцидентами в аспекті спричиненого ними впливу обчислимо за формулою: $\underset{\sim}{LCS}^K_{сум} = \underset{\sim}{LCS}^K_N + \sum_{i=1}^{N-1} \underset{\sim}{LCS}^K_i \prod_{i=i+1}^{N} (1 - \underset{\sim}{LCS}^K_i)$, де $\underset{\sim}{LCS}^K_{сум}$ – сумарний рівень критичності декількох ІПКС з врахуванням кореляції, $\underset{\sim}{LCS}^K_i = K_{IKS_{осн} IKS_{заг_i}} * \underset{\sim}{LCS}_i, i = \overline{2,N}$ – рівень критичності корельованого *i*-ого ІПКС, $\underset{\sim}{LCS}^K_1 = \underset{\sim}{LCS}_{осн}, N$ – загальна кількість інцидентів.

Розроблено метод оцінювання рівня критичності у разі витоку персональних даних на основі механізму кореляції, основними етапами якого є: 1) вибір ІПКС та наборів оціночних параметрів з загальної множини, що характеризують їх вплив на середовище; 2) вибір основного і залежних ІПКС, а також відповідна зміна нумерації інцидентів в системі; 3) визначення коефіцієнта кореляції кожного залежного ІПКС з основним, що визначає взаємозалежності між ними. В основі механізму, так як і в методах виявлення та оцінювання ІПКС, лежать методи нечіткої логіки та експертного оцінювання.

3.4. Система забезпечення безпеки персональних даних у соціально-кіберфізичних системах

В умовах формування соціокіберфізичних систем (СКФС), які об'єднують фізичні об'єкти, цифрові платформи, соціальні мережі та засоби автоматизованого управління, захист персональних даних набуває критичного значення. СКФС генерують та обробляють великі обсяги чутливої інформації про користувачів, включно з біометричними, поведінковими, локаційними та іншими даними, що підлягають захисту згідно із законодавством, зокрема Регламентом ЄС (GDPR) та Законом України «Про захист персональних даних». З урахуванням цього, персональні дані у СКФС виступають як один із ключових активів, що потребують захисту не менш суворо, ніж самі технологічні елементи.

Тому підвищення захищеності ПД у СКФС вимагає застосування багаторівневих систем безпеки, які інтегрують методи аналізу ризиків, криптографічні засоби (включно з постквантовими алгоритмами), політики доступу на основі атрибутів та системи постійного моніторингу інцидентів [84-87].

Для забезпечення послуг безпеки в соціокіберфізичних системах (об’єктах критичної інфраструктури) пропонується використовувати постквантові криптоалгоритми на основі криптокодових конструкцій Мак-Еліса [84-85, 90-93]. Крім того, проведені дослідження [94-97] дозволяють використовувати різні алгебро-геометричні коди, LDPC-коди з дефектними кодами, що дозволяє будувати гібридні криптокодові конструкції та забезпечувати необхідні показники оперативності та стійкості конфіденційної криптографії. Вхідними даними для побудови таких конструкцій є необхідні параметри стійкості та оперативності переданої інформації. Для побудови багатоконтурних систем безпеки використовується класифікатор загроз, який враховує гібридність, синергію та комплексування змішаних загроз із методами соціальної інженерії [98]. Крім того, пропонується використовувати модифікований протокол SSL/TLS на постквантових алгоритмах [99].

Для побудови структурної схеми системи забезпечення безпеки персональних даних у соціокіберфізичних системах пропонується наступна послідовність дій:

Етап 1. На цьому етапі формується класифікація загроз на основі множини загроз до основних послуг безпеки. При цьому враховуються властивості гібридності та синергізму загроз, можливість їх комплексування з методами соціальної інженерії, а також їх вплив на контури кожної з платформ SCPS [100].

Етап 2. Оцінка (за наявності даних) соціально-політичного, економічного стану суспільства (регіону). Для цього використовується підхід із [101]:

Математична модель оцінки сприйнятливості до соціального впливу елементів державних інститутів, медіа та неформальних лідерів на регіональні спільноти: $\mathbf{IMP} = \mathbf{AA} \cup \mathbf{IL} \cup \mathbf{MM} \cup \mathbf{PP}$, де матриця **IMP** – узагальнена матриця впливу різних інституцій на відповідні вікові групи регіональної спільноти [101].

Етап 3. Оцінка співвідношення загроз до кількості зловмисників («хижаків») та елементів інфраструктури соціокіберфізичних систем («жертв») на основі підходу з [102].

Етап 4. Оцінка інтегрованого показника поточного рівня безпеки багатоконтурної системи захисту.

Етап 5. Модифікація механізмів послуг безпеки в багатоконтурній системі захисту інформації (інтеграція постквантових алгоритмів). Використання постквантових алгоритмів для забезпечення основних послуг безпеки.

На рис. 3.2. представлена структурна схеми системи забезпечення безпеки персональних даних у соціокіберфізичних системах [84]. Основною відмінністю від відомих підходів є можливість синтезу як експертного, так і системного аналізу не тільки цільових загроз на соціокіберфізичні системи, але й можливість об'єктивної оцінки поточного стану захищеності інформації. Такий підхід дозволяє своєчасно реагувати на можливі зміни (модифікації) цільових загроз, а також враховувати їх синергію та гібридність, можливість комплексування з методами соціальної інженерії. Запропоновані практичні рішення забезпечення

послуг безпеки на основі постквантових алгоритмів дозволяють забезпечити необхідний рівень стійкості конфіденційної інформації з різними рівнями їх секретності.

Для оцінки інтегрованого показника безпеки пропонується використовувати програмний комплекс оцінки [98], а також запропоновану методику та обмеження:

Крок 1. Формування експертних оцінок загроз, їх вплив на послуги безпеки, можливість ознак синергії та гібридності, а також комплексування методів соціальної інженерії. Визначення впливу загрози на рівень інфраструктури (моделі ISO/OSI). При цьому формується матриця вагових коефіцієнтів. $S^*_{\text{sthreats}} = \left\| S_{\text{sthreats}_{ij}} \right\|$, де i – послуги безпеки, j – відповідна загроза, $j \in \forall \overline{1 \ldots N}$.

Крок 2. Формування матриці відповідності між інформаційними ресурсами та послугами безпеки: $S^*_{\text{inf}} = \left\| S_{\text{inf}_{il}} \right\|$, де i – послуги безпеки, l – інформаційний ресурс, $l \in \forall \overline{1 \ldots L}$. При заповненні матриці враховується необхідність надання відповідної послуги безпеки (1 – послуга, 0 – послуга не потрібна).

Крок 3. Формування залежності між інформаційними ресурсами та рівнями інфраструктури (моделі ISO/OSI), де циркулює і/або зберігається інформація: $S^*_{\text{ISO}} = \left\| S_{ISO_{kl}} \right\|$, де k – наявність і тип зв'язку, елемент інфраструктури (рівень), де зберігається інформація, l – інформаційний ресурс, $l \in \forall \overline{1 \ldots L}$.

Крок 4. Формування залежності загроз та інформаційних ресурсів (оцінка критичності інфраструктури): $S^*_{\text{inf/sthreats}} = \left\| S_{\text{inf}_{lj}} \right\|$, де l – інформаційний ресурс, $l \in \forall \overline{1 \ldots L}$. j – відповідна загроза, $j \in \forall \overline{1 \ldots N}$. Крок дозволяє визначити критичність несанкціонованого доступу до того чи іншого інформаційного ресурсу.

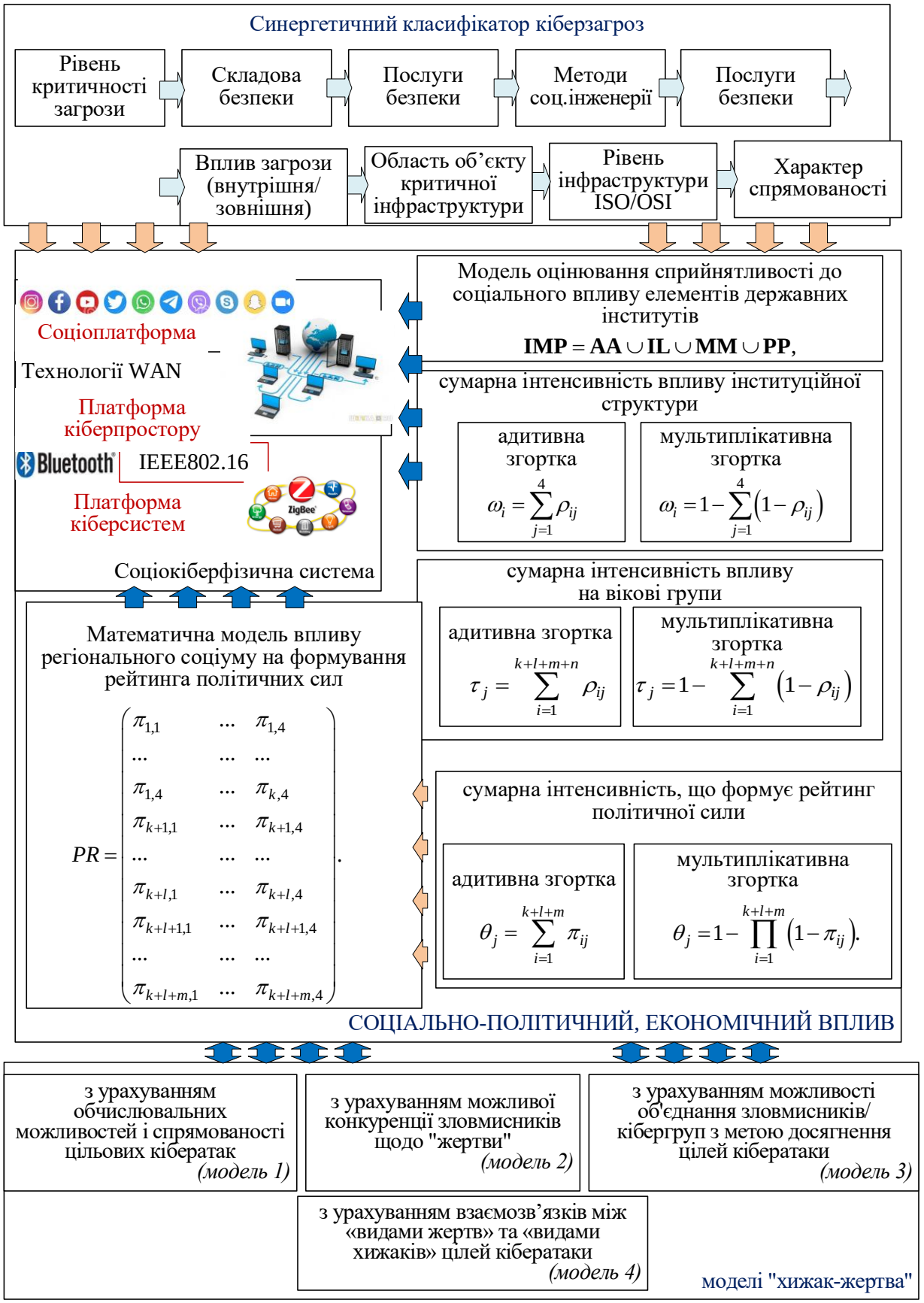


Рис. 3.2. Структурна схема системи

Крок 5. Формування залежності загроз та елементів інфраструктури (рівень моделі ISO/OSI): $S^{*}_{\text{sthreats}/ISO} = \left\| S_{\text{sthreats}/ISO_{kj}} \right\|$, де k – наявність і тип зв'язку, елемент інфраструктури (рівень), де зберігається інформація, j – відповідна загроза, $j \in \forall\overline{1\ldots N}$. Крок дозволяє визначити критичні точки в інфраструктурі та заздалегідь визначити превентивні заходи безпеки.

Крок 6. Формування оцінки захищеності соціокіберфізичної системи на основі аналізу кроків 2 та 3 (знаходження зв'язку між інформаційними ресурсами, елементами інфраструктури (критичними точками несанкціонованого доступу/витоку інформації) і послугами безпеки).

Крок 7. Формування оцінки можливостей діючої системи захисту інформації протистояти загрозам: $S^{*}_{\text{sthreats}/\text{protection system}} = \left\| S_{\text{sthreats}/\text{protection system}_{qj}} \right\|$, де q – наявність механізму протидії загрозі, j – відповідна загроза, $j \in \forall\overline{1\ldots N}$.

Крок 8. Формування оцінки регуляторів і законодавчих актів.

Крок 9. Формування оцінки поточного стану системи безпеки. При цьому враховуються результати кроків 7–9.

Представлена система використовує наступні вимоги:

Після розрахунку ключових матриць відповідності необхідно визначити синергетичний ефект взаємодії компонентів кібербезпеки (послуг безпеки, інформаційних ресурсів і елементів інфраструктури). Для матриці відповідності між послугами безпеки та інформаційними ресурсами: $S^{*}_{\text{inf}} = \left\| S_{\text{inf}_{il}} \right\|$, де i – послуги безпеки, l – інформаційний ресурс. Після розрахунку матриці визначається рівень важливості кожної послуги (S_{inf_i}) та кожного ресурсу (S_{inf_l}), де i=1,…,5, l=1,…,8, за формулами: $S_{\text{inf}_i} = \sum_{l=1}^{8} S_{\text{inf}_{il}}$, $S_{\text{inf}_l} = \sum_{i=1}^{5} S_{\text{inf}_{il}}$. Після цього визначаються сумарні рівні важливості послуг ($S_{\text{inf}_i s}$) та ресурсів ($S_{\text{inf}_l s}$) за формулами: $S_{\text{inf}_i s} = \sum_{i=1}^{5} S_{\text{inf}_i}$,

$S_{\inf_l s} = \sum_{l=1}^{8} S_{\inf_l}$. Наступними визначаються вагові коефіцієнти для послуг ($\alpha S_{\inf_i}$) та ресурсів ($\alpha S_{\inf_l}$) за формулами: $\alpha S_{\inf_i} = \frac{S_{\inf_i}}{S_{\inf_i s}}$, де i=1,…,5; $\alpha S_{\inf_l} = \frac{S_{\inf_l}}{S_{\inf_l s}}$, де l=1,…,8. Після цього послуги і ресурси ранжуються за визначеними ваговими коефіцієнтами від найбільшого до найменшого для визначення найбільш значущих послуг/ресурсів відповідно до матриці їх взаємодії.

Далі формується інтегральний показник поточного рівня безпеки для матриці відповідності між послугами безпеки та інформаційними ресурсами. Для цього визначається абсолютне та відносне значення інтегрального показника:

$$IS_{\inf\_abs} = \frac{\sum S_{\inf_{il}}}{i \times l}, \; IS_{\inf\_rel} = \frac{IS_{\inf\_abs} - S_{\inf_{il}\min}}{S_{\inf_{il}\max} - S_{\inf_{il}\min}},$$

де $IS_{\inf\_abs}$ – абсолютний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та інформаційних ресурсів; $IS_{\inf\_rel}$ – відносний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та інформаційних ресурсів; $S_{\inf_{il}}$ – елементи загальної матриці відповідності послуг безпеки та інформаційних ресурсів; i – кількість послуг безпеки; l – кількість інформаційних ресурсів; $S_{\inf_{il}\min}$ – мінімальний елемент матриці відповідності послуг безпеки та інформаційних ресурсів; $S_{\inf_{il}\max}$ – мінімальний елемент матриці відповідності послуг безпеки та інформаційним ресурсам.

Для матриці залежності між інформаційними ресурсами та рівнями інфраструктури (моделі ISO/OSI), де циркулює і/або зберігається інформація: $S^*_{\text{ISO}} = \left\| S_{ISO_{kl}} \right\|$, де k – наявність і тип зв’язку, елемент інфраструктури (рівень), де зберігається інформація, l – інформаційний ресурс. Після розрахунку матриці визначається рівень важливості кожного інформаційного ресурсу (S_{ISO_k}) і кожного рівня інфраструктури (S_{ISO_l}), де k=1,…,8, l=1,…,7, за формулами: $S_{ISO_k} = \sum_{l=1}^{7} S_{ISO_{kl}}$,

$S_{ISO_l} = \sum_{k=1}^{8} S_{ISO_{kl}}$. Після цього визначаються сумарні рівні інформаційних ресурсів ($S_{ISO_k s}$) і рівнів інфраструктури ($S_{ISO_l s}$) за формулами: $S_{ISO_k s} = \sum_{k=1}^{8} S_{ISO_k}$, $S_{ISO_l s} = \sum_{l=1}^{7} S_{ISO_l}$. Наступними визначаються вагові коефіцієнти для ресурсів (αS_{ISO_k}) і рівнів інфраструктури (αS_{ISO_l}) за формулами: $\alpha S_{ISO_k} = \frac{S_{ISO_k}}{S_{ISO_k s}}$, де k=1,…,8; $\alpha S_{ISO_l} = \frac{S_{ISO_l}}{S_{ISO_l s}}$, де l=1, …, 7. Після цього ресурси і рівні інфраструктури ранжуються за визначеними ваговими коефіцієнтами від найбільшого до найменшого для визначення найбільш значущих ресурсів/рівнів відповідно до матриці їх взаємодії.

Далі формується інтегральний показник поточного рівня безпеки для матриці відповідності між інформаційними ресурсами та рівнями інфраструктури. Для цього визначається абсолютне та відносне значення інтегрального показника:

$$IS_{ISO\_abs} = \frac{\sum S_{ISO_{kl}}}{k \times l}, \; IS_{ISO\_rel} = \frac{IS_{ISO\_abs} - S_{ISO_{kl}\min}}{S_{ISO_{kl}\max} - S_{ISO_{kl}\min}},$$

де IS_{ISO_abs} – абсолютний інтегральний показник поточного рівня захищеності інформації для матриці відповідності між інформаційними ресурсами та рівнями інфраструктури; IS_{ISO_rel} – відносний інтегральний показник поточного рівня захищеності інформації для матриці відповідності між інформаційними ресурсами та рівнями інфраструктури; $S_{ISO_{kl}}$ – елементи загальної матриці відповідності між інформаційними ресурсами та рівнями інфраструктури; k – кількість інформаційних ресурсів; l – кількість рівнів інфраструктури; $S_{ISO_{kl}\min}$ – мінімальний елемент матриці відповідності між інформаційними ресурсами та рівнями інфраструктури; $S_{ISO_{kl}\max}$ – мінімальний елемент матриці відповідності між інформаційними ресурсами та рівнями інфраструктури.

Для матриці відповідності між послугами безпеки та рівнями інфраструктури: $S^{*}_{serv} = \left\| S_{serv_{ij}} \right\|$, де i – послуга безпеки, l – рівень інфраструктури. Після розрахунку матриці визначається рівень важливості кожної послуги (S_{serv_i}) і кожного рівня інфраструктури (S_{serv_l}), де i=1,…,5, l=1,…,7, за формулами: $S_{serv_i} = \sum_{l=1}^{7} S_{serv_{il}}$, $S_{serv_l} = \sum_{i=1}^{5} S_{serv_{il}}$. Після цього визначаються сумарні рівні важливості послуг (αS_{serv_i}) та рівнів інфраструктури. ($S_{\inf_l s}$) за формулами: $S_{serv_i s} = \sum_{i=1}^{5} S_{serv_i}$, $S_{serv_l s} = \sum_{l=1}^{7} S_{serv_l}$. Наступними визначаються вагові коефіцієнти для послуг (αS_{serv_i}) і рівнів (αS_{serv_l}) за формулами: $\alpha S_{serv_i} = \frac{S_{serv_i}}{S_{serv_i s}}$, де i=1,…,5; $\alpha S_{serv_l} = \frac{S_{serv_l}}{S_{serv_l s}}$, де l=1,…,7. Після цього послуги та ресурси ранжуються за визначеними ваговими коефіцієнтами від найбільшого до найменшого для визначення найбільш значущих послуг/рівнів інфраструктури відповідно до матриці їхньої взаємодії.

Далі формується інтегральний показник поточного рівня безпеки для матриці відповідності між послугами безпеки та рівнями інфраструктури. Для цього визначаються абсолютне та відносне значення інтегрального показника:

$$IS_{serv\_abs} = \frac{\sum S_{serv_{il}}}{i \times l}, \; IS_{serv\_rel} = \frac{IS_{serv\_abs} - S_{serv_{il}\min}}{S_{serv_{il}\max} - S_{serv_{il}\min}},$$

де IS_{serv_abs} – абсолютний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та рівнів інфраструктури; IS_{serv_rel} – відносний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та рівнів інфраструктури; $S_{serv_{il}}$ – елементи загальної матриці відповідності послуг безпеки та рівнів інфраструктури; $S_{serv_{il}\min}$ – мінімальний елемент матриці відповідності послуг безпеки та рівнів інфраструктури.

Загальний інтегральний показник поточного рівня захищеності інформації

в аналізованій системі безпеки формується шляхом адитивного згортання окремих абсолютних інтегральних показників та мультиплікативного згортання окремих відносних інтегральних показників. Адитивний інтегральний показник поточного рівня захищеності інформації в системі безпеки розраховується за формулою: $IS_{add} = IS_{\inf\_abs} + IS_{ISO\_abs} + IS_{serv\_abs}$. Мультиплікативний інтегральний показник поточного рівня захищеності інформації в системі безпеки розраховується за формулою: $IS_{mult} = IS_{\inf\_rel} + IS_{ISO\_rel} + IS_{serv\_rel}$. Таким чином можна визначити загальну інтегральну оцінку захищеності системи: чим ближче значення відносного показника до 1, тим вищий вплив відповідних факторів на захищеність інформації в системі безпеки [84].

Розроблена система дозволяє здійснювати як експертну, так і об’єктивну кількісну оцінку поточного рівня захищеності ПД за допомогою формалізованих матричних розрахунків, що включають показники вагомості, важливості, критичності та інтегральні коефіцієнти захищеності. Таким чином, сформовано основу для подальшої розробки програмно-аналітичних засобів забезпечення конфіденційності ПД у СКФС та може бути використано для адаптації систем кібербезпеки до вимог новітніх стандартів та загроз.

3.5. Система оцінки негативних наслідків втрати персональних даних

Згідно з вимогами 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.

На основі розробленої теоретико-множинної GDPR-моделі параметрів персональних даних [58] та методу оцінювання негативних наслідків від порушення конфіденційності персональних даних [81] розроблено структурну модель системи оцінки негативних наслідків втрати персональних даних (рис. 3.3), 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) [103, 104].

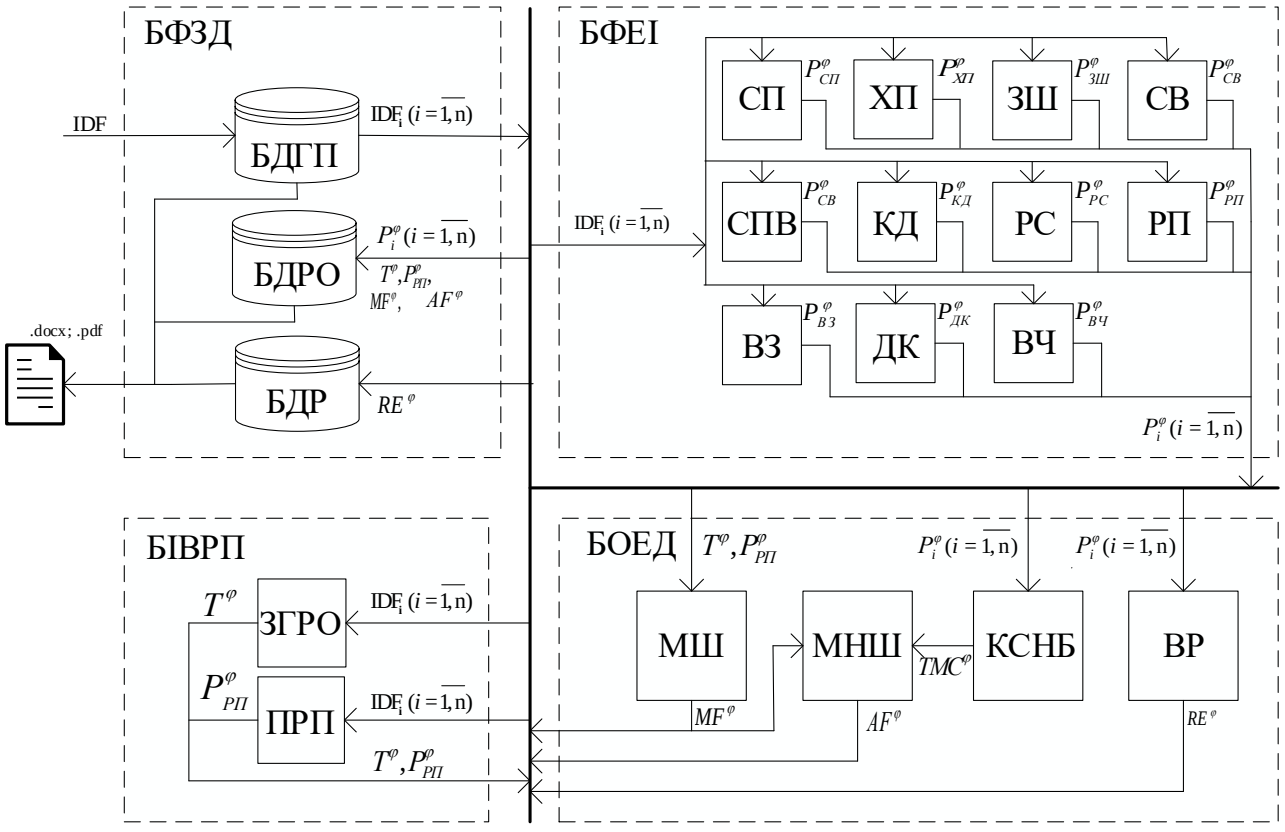


Рис.3.3. Структурна модель системи оцінки негативних наслідків втрати персональних даних

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^{φ} 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.

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 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 $Т^{\varphi}$ (див. (3.1)) шляхом визначення експертом річного обігу в євро (на основі фінансової звітності або оцінки). Модуль ПРП обчислює показник рівня порушення $P_{РП}^{\varphi}$ (див. (3.2)) 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 [103].

В БФЕІ на основі n-компонентного експертного запиту 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. (3.3) – (3.13)), 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 $Т^{\varphi}$, $P_{РП}^{\varphi}$, 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. (3.16)) 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. (3.17)), де P_i^{φ} $(i = \overline{1,11})$ – сума всіх набраних балів виходячи із суджень фахівців відповідної предметної галузі та формується TMC^{φ} (див. (3.18)), 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^{φ} та $P_{РП}^{\varphi}$ відповідно, та обчислюється змінна MF^{φ} (див. (3.19)), що буде відповідати за максимальний штраф за правилами GDPR. На основі MF^{φ} в блоці МНШ обчислюється максимально наближений штраф AF^{φ} (див. (3.20)), 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 [104].

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.

3.6. Висновки до розділу 3

У розділі було запропоновано комплекс методів і систем, орієнтованих на оцінювання ризиків, визначення рівня критичності та наслідків порушення конфіденційності персональних даних у сучасних інформаційних середовищах, зокрема у соціокіберфізичних системах.

Розроблено метод оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до вимог Регламенту GDPR. Метод передбачає багаторівневу експертну оцінку характеристик інциденту та дозволяє обчислювати максимально наближений штраф для підприємства. Це забезпечує формалізований підхід до аналізу інцидентів витоку даних і дозволяє підвищити ефективність прийняття рішень щодо захисту ПД.

Розроблено метод оцінювання безпеки персональних даних в автоматизованих системах на основі кортежної моделі. Метод враховує важливість даних, середовище їх обробки, наявні механізми захисту та рівень реалізації загроз, дозволяючи обґрунтовано визначати рівень ризику витоку ПД та відповідні заходи захисту, особливо в державних АС відповідно до національного законодавства.

Розроблено метод оцінювання рівня критичності інцидентів порушення безпеки на основі механізму кореляції інформаційних подій (ІПКС). Запропоновано формули для обчислення середнього та сумарного рівня критичності з урахуванням взаємозв’язків між інцидентами, що дозволяє моделювати кризові ситуації комплексно та об’єктивно в умовах множинних загроз.

Запропоновано систему забезпечення безпеки персональних даних у соціокіберфізичних системах. Розроблено багатоконтурну архітектуру захисту з урахуванням гібридності загроз, соціальної інженерії, оцінки соціально-

політичного стану та використання постквантових криптографічних алгоритмів. Запропоновано математичний апарат для обчислення інтегрального показника поточного рівня захищеності ПД.

Розроблено структурну модель системи оцінювання негативних наслідків втрати ПД. Система включає блоки ідентифікації рівня порушень, формування експертних оцінок, обробки експертних даних та обчислення наближеного штрафу, забезпечуючи реалізацію вимог GDPR в автоматизованому режимі.

Отже, сформовано методологічну основу для побудови інформаційно-аналітичних та захисних систем у сфері захисту персональних даних. Запропоновані методи та системи дозволяють не лише кількісно оцінювати ризики та збитки, а й формувати практичні рекомендації для зниження рівня загроз, забезпечуючи адаптацію до нових умов цифрової безпеки та нормативних вимог.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ ЗАСОБІВ ДЛЯ ОЦІНЮВАННЯ НЕГАТИВНИХ НАСЛІДКІВ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

4.1. Експериментальне дослідження методу оцінювання негативних наслідків від порушення конфіденційності персональних даних

Дослідження розробленого методу оцінювання негативних наслідків порушення конфіденційності персональних даних [81] необхідне для перевірки його ефективності та надійності. Це допоможе вчасно виявляти ризики, зменшувати шкоду для суб'єктів даних і забезпечувати кращий захист інформації. Крім того, дослідження сприятиме адаптації методу до змін у законодавстві та практичних вимогах, що підвищить довіру користувачів та рівень безпеки даних. Опишемо кожен з етапів.

Етап 1. Ідентифікація об'єкта оцінювання (надання інформації про підприємство). Визначення глобального річного обігу підприємства за минулий рік. Наприклад, якщо компанія за минулий фінансовий рік мала глобальний річний обіг 3 млрд. €, то даний компонент матиме наступний вигляд:

$$\text{Т}^{\varphi} = 3\,000\,000\,000\ €, \tag{4.1}$$

де: Т^{φ} = «загальний глобальний річний обіг підприємства за минулий фінансовий рік».

Етап 2. Визначення рівня порушення. Показник рівня порушення $P_{РП}^{\varphi}$ обчислюється на основі множини визначених рівнів порушення, відносно яких формується коефіцієнт максимально можливого збитку. Для визначення показника рівня порушення $P_{РП}^{\varphi}$ для φ-го об'єкту скористаємося виразом (3.2). Наприклад, при $n_1 = 2$ $(i = \overline{1,2})$, $n_{11} = 3$ $(j = \overline{1,3})$, $n_{12} = 5$ $(j = \overline{1,5})$ з урахуванням прикладу (2.7) значення:

$$C_{1j}^{\varphi L}=\begin{cases}0{,}02\ \ при\ L_{11}^{\varphi}=\text{«}Cm.83,n.4,nn.a\text{»}\\ 0{,}02\ \ при\ L_{12}^{\varphi}=\text{«}Cm.83,n.4,nn.b\text{»}\\ 0{,}02\ \ при\ L_{13}^{\varphi}=\text{«}Cm.83,n.4,nn.c\text{»};\end{cases}\quad C_{2j}^{\varphi L}=\begin{cases}0{,}04\ \ при\ L_{21}^{\varphi}=\text{«}Cm.83,n.5,nn.a\text{»}\\ 0{,}04\ \ при\ L_{22}^{\varphi}=\text{«}Cm.83,n.5,nn.b\text{»}\\ 0{,}04\ \ при\ L_{23}^{\varphi}=\text{«}Cm.83,n.5,nn.c\text{»}\\ 0{,}04\ \ при\ L_{24}^{\varphi}=\text{«}Cm.83,n.5,nn.d\text{»}\\ 0{,}04\ \ при\ L_{25}^{\varphi}=\text{«}Cm.83,n.5,nn.e\text{»}.\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти L_{12}^{φ} = «$Cm.83,n.4,nn.b$» та L_{23}^{φ} = «$Cm.83,n.5,nn.c$» з підмножин $\mathbf{L_1^{\varphi}}$, $\mathbf{L_2^{\varphi}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(L_{12}^{\varphi})=\ b(L_{23}^{\varphi})=\text{«}TRUE\text{»}$. З урахуванням зазначеного $B_{12}^{\varphi L}=B_{23}^{\varphi L}=1$, а $C_{12}^{\varphi L}=0{,}02$ і $C_{23}^{\varphi L}=0{,}04$. Таким чином, вираз (3.2) матиме наступний вигляд:

$$P_{СП}^{\varphi}=\bigvee_{i=1}^{2}\bigvee_{j=1}^{n_{1i}}B_{ij}^{\varphi L}C_{ij}^{\varphi L}=\ (B_{11}^{\varphi L}C_{11}^{\varphi L}\vee B_{12}^{\varphi L}C_{12}^{\varphi L}\vee B_{13}^{\varphi L}C_{13}^{\varphi L})\vee(B_{21}^{\varphi L}C_{21}^{\varphi L}\vee B_{22}^{\varphi L}C_{22}^{\varphi L}\vee B_{23}^{\varphi L}C_{23}^{\varphi L}\vee$$

$$B_{24}^{\varphi L}C_{24}^{\varphi L}\vee B_{25}^{\varphi L}C_{25}^{\varphi L})=(0\cdot 0{,}02\vee 1\cdot 0{,}02\vee 1\cdot 0{,}02)\vee$$
$$(0\cdot 0{,}04\vee 0\cdot 0{,}04\vee 1\cdot 0{,}04\vee 0\cdot 0{,}04\vee 0\cdot 0{,}04)=0{,}04. \qquad (4.2)$$

Слід зазначити, що коефіцієнт максимально-можливого збитку буде становити 0,04 від компоненти T^{φ} = «Загальний глобальний річний обіг підприємства за минулий фінансовий рік», так як коефіцієнти не додаються, а серед двох вибирається більший, що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства [82].

Етап 3. Формування первинної експертної інформації

Крок 1. Визначення показника «Специфіка порушення». Показник специфіки порушення $P_{СП}^{\varphi}$ для φ-го об'єкту визначається виразом (3.3). Наприклад, при $n_2=4\ (i=\overline{1,4})$, $n_{21}=n_{22}=n_{23}=n_{24}=5\ (j=\overline{1,5})$ з урахуванням (2.11) значення:

$$C_{1j}^{\varphi N}=\begin{cases}1\ при\ N_{11}^{\varphi}=\text{«}Публічна\text{»}\\ 2\ при\ N_{12}^{\varphi}=\text{«}Комерційна\text{»}\\ 3\ при\ N_{13}^{\varphi}=\text{«}Конфіденційна\text{»}\\ 4\ при\ N_{14}^{\varphi}=\text{«}Секретна\text{»}\\ 5\ при\ N_{15}^{\varphi}=\text{«}Цілком\ секретна\text{»};\end{cases}\qquad C_{2j}^{\varphi N}=\begin{cases}1\ при\ N_{21}^{\varphi}=\left]0;\ Тиждень\right]\\ 2\ при\ N_{22}^{\varphi}=\left]Тиждень;\ Місяць\right]\\ 3\ при\ N_{23}^{\varphi}=\left]Місяць;\ 6\ Місяців\right]\\ 4\ при\ N_{24}^{\varphi}=\left]6\ Місяців;\ Рік\right]\\ 5\ при\ N_{25}^{\varphi}=\left]Рік;\ \infty\right[;\end{cases}$$

$$C_{3j}^{\varphi N}=\begin{cases}1\ при\ N_{31}^{\varphi}=\left]0;\ 1000\right]\\ 2\ при\ N_{32}^{\varphi}=\left]1000;\ 50000\right]\\ 3\ при\ N_{33}^{\varphi}=\left]50000;\ 100000\right]\\ 4\ при\ N_{34}^{\varphi}=\left]100000;\ 1000000\right]\\ 5\ при\ N_{35}^{\varphi}=\left]1000000;\ \infty\right[;\end{cases}\qquad C_{4j}^{\varphi N}=\begin{cases}1\ при\ N_{41}^{\varphi}=\text{«}Незначний\text{»}\\ 2\ при\ N_{42}^{\varphi}=\text{«}Низький\text{»}\\ 3\ при\ N_{43}^{\varphi}=\text{«}Середній\text{»}\\ 4\ при\ N_{44}^{\varphi}=\text{«}Високий\text{»}\\ 5\ при\ N_{45}^{\varphi}=\text{«}Катастрофічний\text{»}.\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти N_{13}^{φ} = «Конфіденційна», N_{25}^{φ} =]Рік; ∞[, N_{35}^{φ} =]1000000; ∞[та N_{45}^{φ} = «Катастрофічний» з підмножин $\mathbf{N_1^{\varphi}}$, $\mathbf{N_2^{\varphi}}$, $\mathbf{N_3^{\varphi}}$, $\mathbf{N_4^{\varphi}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції $b(N_{13}^{\varphi})=b(N_{25}^{\varphi})=b(N_{35}^{\varphi})=b(N_{45}^{\varphi})=\text{«}TRUE\text{»}$. З урахуванням зазначеного $B_{13}^{\varphi N}=B_{25}^{\varphi N}=B_{35}^{\varphi N}=B_{45}^{\varphi N}=1$, а $C_{13}^{\varphi N}=3$ і $C_{25}^{\varphi N}=C_{35}^{\varphi N}=C_{45}^{\varphi N}=5$.

Таким чином, вираз (3.3) матиме наступний вигляд: $P_{СП}^{\varphi}=\sum_{i=1}^{4}\bigvee_{j=1}^{n_{2i}}B_{ij}^{\varphi N}C_{ij}^{\varphi N}=$

$$\begin{gathered}(B_{11}^{\varphi N}C_{11}^{\varphi N}\vee B_{12}^{\varphi N}C_{12}^{\varphi N}\vee B_{13}^{\varphi N}C_{13}^{\varphi N}\vee B_{14}^{\varphi N}C_{14}^{\varphi N}\vee B_{15}^{\varphi N}C_{15}^{\varphi N})+(B_{21}^{\varphi N}C_{21}^{\varphi N}\vee B_{22}^{\varphi N}C_{22}^{\varphi N}\vee\\ B_{23}^{\varphi N}C_{23}^{\varphi N}\vee B_{24}^{\varphi N}C_{24}^{\varphi N}\vee B_{25}^{\varphi N}C_{25}^{\varphi N})+(B_{31}^{\varphi N}C_{31}^{\varphi N}\vee B_{32}^{\varphi N}C_{32}^{\varphi N}\vee B_{33}^{\varphi N}C_{33}^{\varphi N}\vee B_{34}^{\varphi N}C_{34}^{\varphi N}\vee\\ B_{35}^{\varphi N}C_{35}^{\varphi N})+(B_{41}^{\varphi N}C_{41}^{\varphi N}\vee B_{42}^{\varphi N}C_{42}^{\varphi N}\vee B_{43}^{\varphi N}C_{43}^{\varphi N}\vee B_{44}^{\varphi N}C_{44}^{\varphi N}\vee B_{45}^{\varphi N}C_{45}^{\varphi N})=\qquad(4.3)\\ (0\cdot1\vee0\cdot2\vee1\cdot3\vee0\cdot4\vee0\cdot5)+(0\cdot1\vee0\cdot2\vee0\cdot3\vee0\cdot4\vee1\cdot5)+(0\cdot1\vee0\cdot2\vee\\ 0\cdot3\vee0\cdot4\vee1\cdot5)+(0\cdot1\vee0\cdot2\vee0\cdot3\vee0\cdot4\vee1\cdot5)=3+5+5+5=18.\end{gathered}$$

Крок 2. Визначення показника «Характер порушення». Показник характеру порушення $P_{ХП}^{\varphi}$ для φ-го об'єкту визначається виразом (3.4). Наприклад, при $n_3=3$ $(i=\overline{1,3})$, $n_{31}=5$ $(j=\overline{1,5})$, $n_{32}=2$ $(j=\overline{1,2})$, $n_{33}=2$ $(j=\overline{1,2})$ з урахуванням (2.15) значення:

$$C_{1j}^{\varphi CH}=\begin{cases}1\ при\ CH_{11}^{\varphi}=\text{«}Максимальний\text{»}\\ 2\ при\ CH_{12}^{\varphi}=\text{«}Високий\text{»}\\ 3\ при\ CH_{13}^{\varphi}=\text{«}Середній\text{»}\\ 4\ при\ CH_{14}^{\varphi}=\text{«}Низький\text{»}\\ 5\ при\ CH_{15}^{\varphi}=\text{«}Незначний\text{»};\end{cases}\quad C_{2j}^{\varphi CH}=\begin{cases}3\ при\ CH_{21}^{\varphi}=\text{«}Так\text{»}\\ 5\ при\ CH_{22}^{\varphi}=\text{«}Ні\text{»};\end{cases}$$

$$C_{3j}^{\varphi CH}=\begin{cases}5\ при\ CH_{31}^{\varphi}=\text{«}Ігнорування\text{»}\\ 0\ при\ CH_{32}^{\varphi}=\text{«}Застосування\text{»}.\end{cases}$$

В результаті поточного оцінювання компоненти CH_{11}^{φ} = «Максимальний», CH_{21}^{φ} = «Так», CH_{31} = «Ігнорування» з підмножин $\mathbf{CH_1^{\varphi}}$, $\mathbf{CH_2^{\varphi}}$, $\mathbf{CH_3^{\varphi}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(CH_{11}^{\varphi})=b(CH_{21}^{\varphi})=b(CH_{31}^{\varphi})=\text{«}TRUE\text{»}$. З урахуванням зазначеного $B_{11}^{\varphi CH}=B_{21}^{\varphi CH}=B_{31}^{\varphi CH}=1$, а $C_{11}^{\varphi CH}=1$, $C_{21}^{\varphi CH}=3$ і $C_{31}^{\varphi CH}=5$. Таким чином, вираз (3.4) матиме наступний вигляд: $P_{ХП}^{\varphi}=\sum_{i=1}^{3}\bigvee_{j=1}^{n_{3i}}B_{ij}^{\varphi CH}C_{ij}^{\varphi CH}=(B_{11}^{\varphi CH}C_{11}^{\varphi CH}\vee B_{12}^{\varphi CH}C_{12}^{\varphi CH}\vee$

$$B_{13}^{\varphi CH}C_{13}^{\varphi CH}\vee B_{14}^{\varphi CH}C_{14}^{\varphi CH}\vee B_{15}^{\varphi CH}C_{15}^{\varphi CH})+(B_{21}^{\varphi CH}C_{21}^{\varphi CH}\vee B_{22}^{\varphi CH}C_{22}^{\varphi CH})+$$
$$(B_{31}^{\varphi CH}C_{31}^{\varphi CH}\vee B_{32}^{\varphi CH}C_{32}^{\varphi CH})=(1\cdot 1\vee 0\cdot 2\vee 0\cdot 3\vee 0\cdot 4\vee 0\cdot 5)+ \qquad (4.4)$$
$$(1\cdot 3\vee 0\cdot 5)+(1\cdot 5\vee 0\cdot 0)=1+3+5=9.$$

Крок 3. Визначення показника «Зниження шкоди». Показник зниження шкоди $P_{ЗШ}^{\varphi}$ для φ-го об'єкту визначається виразом (3.5). Наприклад, при $n_4=3$ $(i=\overline{1,3})$, $n_{41}=5$ $(j=\overline{1,5})$, $n_{42}=2$ $(j=\overline{1,2})$, $n_{43}=5$ $(j=\overline{1,5})$ з урахуванням (2.19) значення:

$$C_{1j}^{\varphi A}=\begin{cases}1\ при\ A_{11}^{\varphi}=\text{«}Повна\text{»}\\ 2\ при\ A_{12}^{\varphi}=\text{«}Значна\text{»}\\ 3\ при\ A_{13}^{\varphi}=\text{«}Середня\text{»}\\ 4\ при\ A_{14}^{\varphi}=\text{«}Незначна\text{»}\\ 5\ при\ A_{15}^{\varphi}=\text{«}Відсутня\text{»};\end{cases}\quad C_{3j}^{\varphi A}=\begin{cases}1\ при\ A_{31}^{\varphi}=\left]\infty;\ €1.000.000\right[\\ 2\ при\ A_{32}^{\varphi}=\left[€1.000.000;\ €500.000\right[\\ 3\ при\ A_{33}^{\varphi}=\left[€500.000;\ €100.000\right[\\ 4\ при\ A_{34}^{\varphi}=\left[€100.000€;\ 0\right[\\ 5\ при\ A_{35}^{\varphi}=[\varnothing].\end{cases}$$

$$C_{2j}^{\varphi A}=\begin{cases}1\ при\ A_{21}^{\varphi}=\text{«}Так\text{»}\\ 5\ при\ A_{22}^{\varphi}=\text{«}Ні\text{»};\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти A_{15}^{φ} = «Відсутня», A_{22}^{φ} = «Ні», A_{31} =]∞; €1.000.000[з підмножин $\mathbf{A_1^{\varphi}}$, $\mathbf{A_2^{\varphi}}$, $\mathbf{A_3^{\varphi}}$ відповідно визначено

істинними, а інші помилковими. В такому випадку значення функції є: $b(A_{15}^{\varphi}) = b(A_{22}^{\varphi}) = b(A_{31}^{\varphi}) =$ «*TRUE*». З урахуванням зазначеного $B_{15}^{\varphi A} = B_{22}^{\varphi A} = B_{31}^{\varphi A} = 1$, а $C_{15}^{\varphi A} = C_{22}^{\varphi A} = 5$ і $C_{31}^{\varphi A} = 1$. Таким чином, вираз (3.5) матиме наступний вигляд [81]:

$$P_{3Ш}^{\varphi} = \sum_{i=1}^{3} \bigvee_{j=1}^{n_{4i}} B_{ij}^{\varphi A} C_{ij}^{\varphi A} = (B_{11}^{\varphi A} C_{11}^{\varphi A} \vee B_{12}^{\varphi A} C_{12}^{\varphi A} \vee B_{13}^{\varphi A} C_{13}^{\varphi A} \vee B_{14}^{\varphi A} C_{14}^{\varphi A} \vee B_{15}^{\varphi A} C_{15}^{\varphi A}) +$$
$$(B_{21}^{\varphi A} C_{21}^{\varphi A} \vee B_{22}^{\varphi A} C_{22}^{\varphi A}) + (B_{31}^{\varphi A} C_{31}^{\varphi A} \vee B_{32}^{\varphi A} C_{32}^{\varphi A} \vee B_{33}^{\varphi A} C_{33}^{\varphi A} \vee B_{34}^{\varphi A} C_{34}^{\varphi A} \vee B_{35}^{\varphi A} C_{35}^{\varphi A}) = \quad (4.5)$$
$$(0 \cdot 1 \vee 0 \cdot 2 \vee 0 \cdot 3 \vee 0 \cdot 4 \vee 1 \cdot 5) + (0 \cdot 1 \vee 1 \cdot 5) + (1 \cdot 1 \vee 0 \cdot 2 \vee 0 \cdot 3 \vee 0 \cdot 4 \vee 0 \cdot 5) =$$
$$5 + 5 + 1 = 11.$$

Крок 4. Визначення показника «Ступінь відповідальності». Показник ступінь відповідальності P_{CB}^{φ} для φ-го об'єкту визначається виразом (3.6). Наприклад, при $n_5 = 8 \quad (i = \overline{1,8})$, $n_{51} = 2$ $(j = \overline{1,2})$, $n_{52} = 2 \quad (j = \overline{1,2})$, $n_{53} = 3$ $(j = \overline{1,3})$, $n_{54} = 3$ $(j = \overline{1,3})$, $n_{55} = 2 \quad (j = \overline{1,2})$, $n_{56} = 2$ $(j = \overline{1,2})$, $n_{57} = 2 \quad (j = \overline{1,2})$, $n_{58} = 2 \quad (j = \overline{1,2})$ з урахуванням прикладу (2.23) значення:

$$C_{1j}^{\varphi R} = C_{5j}^{\varphi R} = C_{6j}^{\varphi R} = C_{7j}^{\varphi R} = C_{8j}^{\varphi R} = \begin{cases} 0 \ \textit{при} \ R_{11}^{\varphi} = R_{51}^{\varphi} = R_{61}^{\varphi} = R_{71}^{\varphi} = R_{81}^{\varphi} = \text{«}\textit{Так}\text{»} \\ 5 \ \textit{при} \ R_{12}^{\varphi} = R_{52}^{\varphi} = R_{62}^{\varphi} = R_{72}^{\varphi} = R_{82}^{\varphi} = \text{«}\textit{Ні}\text{»}; \end{cases}$$

$$C_{2j}^{\varphi R} = \begin{cases} -5 \ \textit{при} \ R_{21}^{\varphi} = \text{«}\textit{Так}\text{»} \\ 5 \ \textit{при} \ R_{22}^{\varphi} = \text{«}\textit{Ні}\text{»}; \end{cases}$$

$$C_{3j}^{\varphi R} = \begin{cases} -5 \ \textit{при} \ R_{31}^{\varphi} = \text{«}\textit{Так}\text{»} \\ 5 \ \textit{при} \ R_{32}^{\varphi} = \text{«}\textit{Ні}\text{»} \\ 1 \ \textit{при} \ R_{33}^{\varphi} = \text{«}\textit{Невідомо}\text{»}; \end{cases} \qquad C_{4j}^{\varphi R} = \begin{cases} 5 \ \textit{при} \ R_{41}^{\varphi} = \text{«}\textit{Так}\text{»} \\ -5 \ \textit{при} \ R_{42}^{\varphi} = \text{«}\textit{Ні}\text{»} \\ 1 \ \textit{при} \ R_{43}^{\varphi} = \text{«}\textit{Невідомо}\text{»}. \end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти $R_{11}^{\varphi} = R_{21}^{\varphi} = R_{31}^{\varphi} = R_{51}^{\varphi} = R_{61}^{\varphi} = R_{71}^{\varphi} = R_{81}^{\varphi}$=«Так», R_{42}^{φ} = «Ні», з підмножин $\mathbf{R_1^{\varphi}}$, $\mathbf{R_2^{\varphi}}$, $\mathbf{R_3^{\varphi}}$, $\mathbf{R_4^{\varphi}}$, $\mathbf{R_5^{\varphi}}$, $\mathbf{R_6^{\varphi}}$, $\mathbf{R_7^{\varphi}}$, $\mathbf{R_8^{\varphi}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(R_{11}^{\varphi}) = b(R_{21}^{\varphi}) = b(R_{31}^{\varphi}) = b(R_{42}^{\varphi}) = b(R_{51}^{\varphi}) = b(R_{61}^{\varphi}) = b(R_{71}^{\varphi}) = b(R_{81}^{\varphi}) =$ «*TRUE*». З урахуванням зазначеного $B_{11}^{\varphi R} = B_{21}^{\varphi R} = B_{31}^{\varphi R} = B_{42}^{\varphi R} = B_{51}^{\varphi R} = B_{61}^{\varphi R} = B_{71}^{\varphi R} = B_{81}^{\varphi R} = 1$, а $C_{11}^{\varphi R} = C_{51}^{\varphi R} = C_{61}^{\varphi R} = C_{71}^{\varphi R} = C_{81}^{\varphi R} = 0$, $C_{21}^{\varphi R} = C_{31}^{\varphi R} = C_{42}^{\varphi R} = -5$. Таким чином, вираз (3.6) матиме наступний вигляд: $P_{CB}^{\varphi} = \sum_{i=1}^{8} \bigvee_{j=1}^{n_{5i}} B_{ij}^{\varphi R} C_{ij}^{\varphi R} =$

$$(B_{11}^{\varphi R}C_{11}^{\varphi R} \vee B_{12}^{\varphi R}C_{12}^{\varphi R}) + (B_{21}^{\varphi R}C_{21}^{\varphi R} \vee B_{22}^{\varphi R}C_{22}^{\varphi R}) + (B_{31}^{\varphi R}C_{31}^{\varphi R} \vee B_{32}^{\varphi R}C_{32}^{\varphi R} \vee B_{33}^{\varphi R}C_{33}^{\varphi R}) +$$
$$(B_{41}^{\varphi R}C_{41}^{\varphi R} \vee B_{42}^{\varphi R}C_{42}^{\varphi R} \vee B_{43}^{\varphi R}C_{43}^{\varphi R}) + (B_{51}^{\varphi R}C_{51}^{\varphi R} \vee B_{52}^{\varphi R}C_{52}^{\varphi R}) + (B_{61}^{\varphi R}C_{61}^{\varphi R} \vee B_{62}^{\varphi R}C_{62}^{\varphi R}) +$$
$$(B_{71}^{\varphi R}C_{71}^{\varphi R} \vee B_{72}^{\varphi R}C_{72}^{\varphi R}) + (B_{81}^{\varphi R}C_{81}^{\varphi R} \vee B_{82}^{\varphi R}C_{82}^{\varphi R}) = (1\cdot 0 \vee 0\cdot 5) + (1\cdot(-5) \vee 0\cdot 5) +$$
$$(1\cdot(-5) \vee 0\cdot 5 \vee 0\cdot 1) + (0\cdot 5 \vee 1\cdot(-5) \vee 0\cdot 1) + (1\cdot 0 \vee 0\cdot 5) + (1\cdot 0 \vee 0\cdot 5) +$$
$$(1\cdot 0 \vee 0\cdot 5) + (1\cdot 0 \vee 0\cdot 5) = 0 - 5 - 5 - 5 + 0 + 0 + 0 + 0 = -15. \quad (4.6)$$

Крок 5. Визначення показника «Рецидив порушення». Показник рецидив порушення $P_{РЦП}^{\varphi}$ для φ-го об'єкту визначається виразом (3.7). Наприклад, при $n_6 = 1$ $(i = 1)$, $n_{61} = 2$ $(j = \overline{1,2})$, та при $n_{61} = 1$ $n_{611} = 0$ $(k = 0)$, а при $n_{61} = 2$ $n_{612} = 3$ $(k = \overline{1,3})$, $n_{6121} = 3$ $(e = \overline{1,3})$, $n_{6122} = 3$ $(e = \overline{1,3})$, $n_{6123} = 3$ $(e = \overline{1,3})$ з урахуванням прикладу до (2.33) значення:

$$C_{1j}^{\varphi I} = \begin{cases} 0 \ \textit{при} \ I_{11}^{\varphi} = \text{«}\textit{Так}\text{»} \\ 5 \ \textit{при} \ I_{12}^{\varphi} = \text{«}\textit{Ні}\text{»}; \end{cases} \qquad C_{122e}^{\varphi I} = C_{123e}^{\varphi I} = \begin{cases} 0 \ \textit{при} \ I_{1221}^{\varphi} = I_{1231}^{\varphi} = \text{«}\textit{Так}\text{»} \\ 5 \ \textit{при} \ I_{1222}^{\varphi} = I_{1232}^{\varphi} = \text{«}\textit{Ні}\text{»} \\ 1 \ \textit{при} \ I_{1223}^{\varphi} = I_{1233}^{\varphi} = \text{«}\textit{Невідомо}\text{»}. \end{cases}$$

$$C_{121e}^{\varphi I} = \begin{cases} 5 \ \textit{при} \ I_{1211}^{\varphi} = \text{«}\textit{Так}\text{»} \\ 0 \ \textit{при} \ I_{1212}^{\varphi} = \text{«}\textit{Ні}\text{»} \\ 1 \ \textit{при} \ I_{1213}^{\varphi} = \text{«}\textit{Невідомо}\text{»}; \end{cases}$$

В результаті поточного оцінювання, наприклад, компонента I_{11}^{φ} = «Так» з підмножини $\mathbf{I}_1^{\varphi}$ відповідно визначено істиною, а інші помилковими. В такому випадку значення функції є: $b(I_{11}^{\varphi}) = \text{«}TRUE\text{»}$. З урахуванням зазначеного $B_{11}^{\varphi I} = 1$, а $C_{11}^{\varphi I} = 0$. Таким чином, вираз (3.7) матиме наступний вигляд: $P_{РЦП}^{\varphi} = \bigvee_{i=1}^{1} \bigvee_{j=1}^{n_{6i}} B_{ij}^{\varphi I} C_{ij}^{\varphi I} =$

$$(B_{11}^{\varphi I}C_{11}^{\varphi I} \vee (B_{12}^{\varphi I}C_{12}^{\varphi I} + B_{1211}^{\varphi I}C_{1211}^{\varphi I} \vee B_{1212}^{\varphi I}C_{1212}^{\varphi I} \vee B_{1213}^{\varphi I}C_{1213}^{\varphi I} + B_{1221}^{\varphi I}C_{1221}^{\varphi I} \vee B_{1222}^{\varphi I}C_{1222}^{\varphi I} \vee$$
$$B_{1223}^{\varphi I}C_{1223}^{\varphi I} + B_{1231}^{\varphi I}C_{1231}^{\varphi I} \vee B_{1232}^{\varphi I}C_{1232}^{\varphi I} \vee B_{1233}^{\varphi I}C_{1233}^{\varphi I}) = (1\cdot 0 \vee 0\cdot 5) = 0. \quad (4.7)$$

Крок 6. Визначення показника «Рівень співпраці». Показник рівень співпраці $P_{РС}^{\varphi}$ для φ-го об'єкту визначається виразом (3.8). Наприклад, при $n_7 = 3$ $(i = \overline{1,3})$, $n_{71} = 5$ $(j = \overline{1,5})$, $n_{72} = 2$ $(j = \overline{1,2})$, $n_{73} = 2$ $(j = \overline{1,2})$ з урахуванням прикладу до (2.37) значення:

$$C_{1j}^{\varphi C}=\begin{cases}1\ при\ C_{11}^{\varphi}=[100\%;\ 75\%[\\ 2\ при\ C_{12}^{\varphi}=[75\%;\ 50\%[\\ 3\ при\ C_{13}^{\varphi}=[50\%;\ 25\%[\\ 4\ при\ C_{14}^{\varphi}=[25\%;\ 0\%[\\ 5\ при\ C_{15}^{\varphi}=\text{«}\varnothing\text{»};\end{cases}\qquad C_{2j}^{\varphi C}=\begin{cases}0\ при\ C_{21}^{\varphi}=\text{«}Так\text{»}\\ 5\ при\ C_{22}^{\varphi}=\text{«}Ні\text{»};\end{cases}$$

$$C_{3j}^{\varphi C}=\begin{cases}0\ при\ C_{31}^{\varphi}=\text{«}План\ по\ відновленню\text{»}\\ 5\ при\ C_{32}^{\varphi}=\text{«}Наказ\text{»}.\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти C_{15}^{φ} = [$\varnothing$], C_{22}^{φ} = «Ні», C_{32} = «Наказ» з підмножин $\mathbf{C_1^{\varphi}}$, $\mathbf{C_2^{\varphi}}$, $\mathbf{C_3^{\varphi}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(C_{15}^{\varphi})=b(C_{22}^{\varphi})=b(C_{32}^{\varphi})=$ «*TRUE*». З урахуванням зазначеного $B_{15}^{\varphi C}=B_{22}^{\varphi C}=B_{32}^{\varphi C}=1$, а $C_{15}^{\varphi C}=C_{22}^{\varphi C}=C_{32}^{\varphi C}=5$.

Таким чином, вираз (3.8) матиме наступний вигляд: $P_{PC}^{\varphi}=\sum_{i=1}^{3}\bigvee_{j=1}^{n_{7i}}B_{ij}^{\varphi C}C_{ij}^{\varphi C}=(B_{11}^{\varphi C}C_{11}^{\varphi C}\vee$

$$B_{12}^{\varphi C}C_{12}^{\varphi C}\vee B_{13}^{\varphi C}C_{13}^{\varphi C}\vee B_{14}^{\varphi C}C_{14}^{\varphi C}\vee B_{15}^{\varphi C}C_{15}^{\varphi C})+(B_{21}^{\varphi C}C_{21}^{\varphi C}\vee B_{22}^{\varphi C}C_{22}^{\varphi C})+$$
$$(B_{31}^{\varphi C}C_{31}^{\varphi C}\vee B_{32}^{\varphi C}C_{32}^{\varphi C})=(0\cdot1\vee0\cdot2\vee0\cdot3\vee0\cdot4\vee1\cdot5)+(0\cdot1\vee1\cdot5)+ \qquad (4.8)$$
$$(0\cdot1\vee1\cdot5)=5+5+5=15.$$

Крок 7. Визначення показника «Категорії даних». Показник категорії даних $P_{КД}^{\varphi}$ для φ-го об'єкту визначається виразом (3.9). Наприклад, при $n_8=3$ $(i=\overline{1,3})$, $n_{81}=2$ $(j=\overline{1,2})$, $n_{82}=2$ $(j=\overline{1,2})$, $n_{83}=2$ $(j=\overline{1,2})$ з урахуванням прикладу до (2.41) значення:

$$C_{1j}^{\varphi CA}=C_{2j}^{\varphi CA}=C_{3j}^{\varphi CA}=\begin{cases}5\ при\ CA_{11}^{\varphi}=CA_{21}^{\varphi}=CA_{31}^{\varphi}=\text{«}Так\text{»}\\ 0\ при\ CA_{12}^{\varphi}=CA_{22}^{\varphi}=CA_{32}^{\varphi}=\text{«}Ні\text{»}.\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти CA_{12}^{φ} = CA_{32}^{φ} =«Ні», CA_{21}^{φ} = «Так», з підмножин $\mathbf{CA_1^{\varphi}}$, $\mathbf{CA_2^{\varphi}}$, $\mathbf{CA_3^{\varphi}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(CA_{12}^{\varphi})=b(CA_{21}^{\varphi})=b(CA_{32}^{\varphi})=$ «*TRUE*». З урахуванням зазначеного $B_{12}^{\varphi CA}=B_{21}^{\varphi CA}=B_{32}^{\varphi CA}=1$, а $C_{12}^{\varphi CA}=C_{32}^{\varphi CA}=0$, $C_{21}^{\varphi CA}=5$. Таким чином, вираз (3.9) матиме наступний вигляд [81]:

$$P^{\varphi}_{КД} = \sum_{i=1}^{3}\bigvee_{j=1}^{n_{8i}} B^{\varphi CA}_{ij} C^{\varphi CA}_{ij} = (B^{\varphi CA}_{11} C^{\varphi CA}_{11} \vee B^{\varphi CA}_{12} C^{\varphi CA}_{12}) + (B^{\varphi CA}_{21} C^{\varphi CA}_{21} \vee B^{\varphi CA}_{22} C^{\varphi CA}_{22}) +$$
$$(B^{\varphi CA}_{31} C^{\varphi CA}_{31} \vee B^{\varphi CA}_{32} C^{\varphi CA}_{32}) = (0 \cdot 5 \vee 1 \cdot 0) + (1 \cdot 5 \vee 0 \cdot 0) + (0 \cdot 5 \vee 1 \cdot 0) = 0 + 5 + 0 = 5. \quad (4.9)$$

Крок 8. Визначення показника «Спосіб виявлення». Показник спосіб виявлення $P^{\varphi}_{СПВ}$ для φ-го об'єкту визначається виразом (3.10). Наприклад, при $n_9 = 1$ $(i = 1)$, $n_{91} = 4$ $(j = \overline{1,4})$, та при $n_{91} = 1$ $n_{911} = 1$ $(k = \overline{1,1})$, $n_{9111} = 3$ $(e = \overline{1,3})$, $n_{91112} = 1$ $(p = \overline{1,1})$, $n_{911121} = 3$ $(x = \overline{1,3})$, а при $n_{91} = 2, n_{91} = 3, n_{91} = 4, n_{912} = 0$ $(k = 0)$ з урахуванням прикладу до (2.53) значення:

$$C^{\varphi M}_{1j} = \begin{cases} 0 \text{ при } M^{\varphi}_{11} = \text{«Суб'єкт порушник»} \\ 5 \text{ при } M^{\varphi}_{12} = \text{«Інформатор»} \\ 5 \text{ при } M^{\varphi}_{13} = \text{«Заголовки ЗМІ»} \\ 3 \text{ при } M^{\varphi}_{14} = \text{«Інше»}; \end{cases} \qquad C^{\varphi M}_{111e} = C^{\varphi M}_{11121x} = \begin{cases} 0 \text{ при } M^{\varphi}_{1111} = M^{\varphi}_{111211} = \text{«Так»} \\ 2 \text{ при } M^{\varphi}_{1112} = M^{\varphi}_{111212} = \text{«Ні»} \\ 1 \text{ при } M^{\varphi}_{1113} = M^{\varphi}_{111213} = \text{«Невідомо».} \end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти M^{φ}_{14}=«Інше» з підмножини $\mathbf{M}^{\boldsymbol{\varphi}}_{\mathbf{1}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(M^{\varphi}_{14}) = \text{«}TRUE\text{»}$. З урахуванням зазначеного $B^{\varphi M}_{14} = 1$, а $C^{\varphi M}_{14} = 3$. Таким чином, вираз (3.10) матиме наступний вигляд:

$$P^{\varphi}_{СПВ} = \sum_{i=1}^{1}\bigvee_{j=1}^{n_{9i}} B^{\varphi M}_{ij} C^{\varphi M}_{ij} = (B^{\varphi M}_{11} C^{\varphi M}_{11} + (B^{\varphi M}_{1111} C^{\varphi M}_{1111} \vee B^{\varphi M}_{1112} C^{\varphi M}_{1112} \vee B^{\varphi M}_{1113} C^{\varphi M}_{1113}) +$$
$$(B^{\varphi M}_{111211} C^{\varphi M}_{111211} \vee B^{\varphi M}_{111212} C^{\varphi M}_{111212} \vee B^{\varphi M}_{111213} C^{\varphi M}_{111213})) \vee B^{\varphi M}_{12} C^{\varphi M}_{12} \vee B^{\varphi M}_{13} C^{\varphi M}_{13} \vee B^{\varphi M}_{14} C^{\varphi M}_{14}) = \quad (4.10)$$
$$= (0 \cdot 0 + (0 \cdot 0 + 0 \cdot 2 + 0 \cdot 1) + (0 \cdot 0 + 0 \cdot 2 + 0 \cdot 1)) \vee 0 \cdot 5 \vee 0 \cdot 5 \vee 1 \cdot 3 = 3.$$

Крок 9. Визначення показника «Відповідність заходам». Показник відповідність заходам $P^{\varphi}_{ВЗ}$ для φ-го об'єкту визначається виразом (3.11). Наприклад, при $n_{10} = 1$ $(i = 1)$, $n_{101} = 2$ $(j = \overline{1,2})$, та при $n_{102} = 2$ $n_{1011} = 0$ $(k = 0)$, а при $n_{101} = 1$ $n_{1011} = 1$ $(k = \overline{1,1})$, $n_{10111} = 3$ $(e = \overline{1,3})$ з урахуванням прикладу до (2.61) значення:

$$C_{1j}^{\varphi ME}=\begin{cases}5\ \ при\ ME_{11}^{\varphi}=\text{«}Так\text{»}\\ 0\ \ при\ ME_{12}^{\varphi}=\text{«}Ні\text{»};\end{cases}\qquad C_{111e}^{\varphi ME}=\begin{cases}0\ \ при\ ME_{1111}^{\varphi}=\text{«}Так\text{»}\\ 5\ \ при\ ME_{1112}^{\varphi}=\text{«}Ні\text{»}\\ 1\ \ при\ ME_{1113}^{\varphi}=\text{«}Невідомо\text{»}.\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти $ME_{11}^{\varphi}=\text{«}Так\text{»}$ з підмножини $\mathbf{ME_1^{\varphi}}$ та компоненти $ME_{1112}^{\varphi}=\text{«}Ні\text{»}$ з підмножини $\mathbf{ME_{111}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(ME_{11}^{\varphi})=b(ME_{1112}^{\varphi})=\text{«}TRUE\text{»}$. З урахуванням зазначеного $B_{11}^{\varphi ME}=B_{1112}^{\varphi ME}=1$, а $C_{11}^{\varphi ME}=C_{1112}^{\varphi ME}=5$. Таким чином, вираз (3.11) матиме наступний вигляд:

$$P_{B3}^{\varphi}=\sum_{i=1}^{1}\bigvee_{j=1}^{n_{10i}}B_{ij}^{\varphi ME}C_{ij}^{\varphi ME}=((B_{11}^{\varphi ME}C_{11}^{\varphi ME}+(B_{1111}^{\varphi ME}C_{1111}^{\varphi ME}\vee B_{1112}^{\varphi ME}C_{1112}^{\varphi ME}\vee B_{1113}^{\varphi M}C_{1113}^{\varphi ME}))$$
$$\vee B_{12}^{\varphi ME}C_{12}^{\varphi ME})=(1\cdot 5+(0\cdot 0\vee 1\cdot 5\vee 0\cdot 1))\vee 0\cdot 5=5+5=10. \qquad (4.11)$$

Крок 10. Визначення показника «Дотримання кодексів». Показник дотримання кодексів $P_{ДК}^{\varphi}$ для φ-го об'єкту визначається виразом (3.12). Наприклад, при $n_{11}=2$ $(i=\overline{1,2})$, а саме, при $n_{11}=1$ $n_{111}=$ визначення наявності Кодексу Поведінки, а при $n_{11}=2$ $n_{112}=2$ $(j=\overline{1,2})$, $n_{1111}=1$ $(k=\overline{1,1})$, $n_{11111}=3$ $(e=\overline{1,3})$ з урахуванням прикладу до (2.69) значення:

$C_{11}^{\varphi AD}=B_{81}^{\varphi R}C_{81}^{\varphi R}\vee B_{82}^{\varphi R}C_{82}^{\varphi R}$ *при* $AD_{11}^{\varphi}=\text{«}Так\text{»}$
(Цей бал виставлено на Етапі 3 Кроку 4);

$$C_{2j}^{\varphi AD}=\begin{cases}0\ \ при\ AD_{21}^{\varphi}=\text{«}Так\text{»}\\ 0\ \ при\ AD_{22}^{\varphi}=\text{«}Ні\text{»};\end{cases}$$

$$C_{211e}^{\varphi AD}=\begin{cases}0\ \ при\ AD_{2111}^{\varphi}=\text{«}Так\text{»}\\ 5\ \ при\ AD_{2112}^{\varphi}=\text{«}Ні\text{»}\\ 1\ \ при\ AD_{2113}^{\varphi}=\text{«}Невідомо\text{»}.\end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти $AD_{11}^{\varphi}=\text{«}Так\text{»}$ з підмножини $\mathbf{AD_1^{\varphi}}$, $AD_{21}^{\varphi}=\text{«}Так\text{»}$ з підмножини $\mathbf{AD_2^{\varphi}}$, та компоненти $AD_{2111}^{\varphi}=\text{«}Так\text{»}$ з підмножини $\mathbf{AD_{211}}$ відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(AD_{11}^{\varphi})=b(AD_{21}^{\varphi})=b(AD_{2111}^{\varphi})=\text{«}TRUE\text{»}$. З урахуванням зазначеного $B_{11}^{\varphi AD}=B_{21}^{\varphi AD}=B_{2111}^{\varphi AD}=1$, а

$C_{21}^{\varphi AD} = C_{2111}^{\varphi AD} = 0$. Таким чином, вираз (3.12) матиме наступний вигляд:

$$P_{ДК}^{\varphi} = \sum_{i=1}^{2} \bigvee_{j=1}^{n_{11i}} B_{ij}^{\varphi AD} C_{ij}^{\varphi AD} = B_{11}^{\varphi AD} C_{11}^{\varphi AD} + (B_{21}^{\varphi AD} C_{21}^{\varphi AD} + B_{2111}^{\varphi AD} C_{2111}^{\varphi AD} \vee B_{2112}^{\varphi AD} C_{2112}^{\varphi AD} \vee B_{2113}^{\varphi AD} C_{2113}^{\varphi AD}) \vee B_{22}^{\varphi AD} C_{22}^{\varphi AD}) == 1 \cdot 0 + (1 \cdot 0 + 1 \cdot 0 \vee 0 \cdot 5 \vee 0 \cdot 1) \vee 0 \cdot 0 = 0. \quad (4.12)$$

Крок 11. Визначення показника «Визначаючий чинник». Показник визначаючий чинник $P_{ВЧ}^{\varphi}$ для φ-го об'єкту визначається виразом (3.13). Наприклад, при $n_{12} = 2 \quad (i = \overline{1,2})$, $n_{121} = 3 \; (j = \overline{1,3})$, $n_{1211} = 2 \quad (k = \overline{1,2})$, $n_{12111} = 5 \; (e = \overline{1,5})$ з урахуванням прикладу до (2.77) значення:

$$C_{1j}^{\varphi F} = \begin{cases} 5 \;\; при \; F_{11}^{\varphi} = «Так» \\ 0 \;\; при \; F_{12}^{\varphi} = «Ні» \\ 1 \;\; при \; F_{13}^{\varphi} = «Невідомо»; \end{cases} \qquad C_{2j}^{\varphi F} = \begin{cases} 0 \;\; при \; F_{21}^{\varphi} = «Так» \\ 5 \;\; при \; F_{22}^{\varphi} = «Ні» \\ 1 \;\; при \; F_{23}^{\varphi} = «Невідомо»; \end{cases}$$

$$C_{111e}^{\varphi F} = \begin{cases} 5 \;\; при \; F_{1111}^{\varphi} =]\infty; \; €1.000.000[\\ 4 \;\; при \; F_{1112}^{\varphi} = [€1.000.000; \; €500.000[\\ 3 \;\; при \; F_{1113}^{\varphi} = [€500.000; \; €100.000[\\ 2 \;\; при \; F_{1114}^{\varphi} = [€100.000€; \; 0[\\ 1 \;\; при \; F_{1115}^{\varphi} = [\varnothing] \\ 0 \;\; при \; F_{1116}^{\varphi} = «Невідомо»; \end{cases} \qquad C_{211e}^{\varphi F} = \begin{cases} 1 \;\; при \; F_{2111}^{\varphi} =]\infty; \; €1.000.000[\\ 2 \;\; при \; F_{2112}^{\varphi} = [€1.000.000; \; €500.000[\\ 3 \;\; при \; F_{2113}^{\varphi} = [€500.000; \; €100.000[\\ 4 \;\; при \; F_{2114}^{\varphi} = [€100.000€; \; 0[\\ 5 \;\; при \; F_{2115}^{\varphi} = [\varnothing] \\ 0 \;\; при \; F_{2116}^{\varphi} = «Невідомо». \end{cases}$$

В результаті поточного оцінювання, наприклад, компоненти $F_{11}^{\varphi} = «Так»$ з підмножини $\mathbf{F_1^{\varphi}}$ та компоненти $F_{1111}^{\varphi} =]\infty; \; €1.000.000[$ з підмножини $\mathbf{F_{111}}$, та компоненти $F_{21}^{\varphi} = «Так»$ з підмножини $\mathbf{F_2^{\varphi}}$ та компоненти $F_{2111}^{\varphi} =]\infty; \; €1.000.000[$ з підмножини $\mathbf{F_{211}}$, відповідно визначено істинними, а інші помилковими. В такому випадку значення функції є: $b(F_{11}^{\varphi}) = b(F_{1111}^{\varphi}) = b(F_{21}^{\varphi}) = b(F_{2111}^{\varphi}) = «TRUE»$. З урахуванням зазначеного $B_{11}^{\varphi F} = B_{1111}^{\varphi F} = B_{21}^{\varphi F} = B_{2111}^{\varphi F} = 1$, а $C_{11}^{\varphi F} = C_{1111}^{\varphi F} = 5$, $C_{21}^{\varphi F} = 0$, $C_{2111}^{\varphi F} = 5$. Таким чином, вираз (3.13) матиме наступний вигляд: $P_{ВЧ}^{\varphi} = \sum_{i=1}^{2} \bigvee_{j=1}^{n_{12i}} B_{ij}^{\varphi F} C_{ij}^{\varphi F} =$

$$((B_{11}^{\varphi F} C_{11}^{\varphi F} + (B_{1111}^{\varphi F} C_{1111}^{\varphi F} \vee B_{1112}^{\varphi F} C_{1112}^{\varphi F} \vee B_{1113}^{\varphi F} C_{1113}^{\varphi F} \vee B_{1114}^{\varphi F} C_{1114}^{\varphi F} \vee B_{1115}^{\varphi F} C_{1115}^{\varphi F} \vee B_{1116}^{\varphi F} C_{1116}^{\varphi F})) \vee B_{12}^{\varphi F} C_{12}^{\varphi F} \vee B_{13}^{\varphi F} C_{13}^{\varphi F}) + ((B_{21}^{\varphi F} C_{21}^{\varphi F} + (B_{2111}^{\varphi F} C_{2111}^{\varphi F} \vee B_{2112}^{\varphi F} C_{2112}^{\varphi F} \vee B_{2113}^{\varphi F} C_{2113}^{\varphi F} \vee B_{2114}^{\varphi F} C_{2114}^{\varphi F} \vee$$

$$B_{2115}^{\varphi F}C_{2115}^{\varphi F} \vee B_{2116}^{\varphi F}C_{2116}^{\varphi F})) \vee B_{22}^{\varphi F}C_{22}^{\varphi F} \vee B_{22}^{\varphi F}C_{22}^{\varphi F}) = ((1\cdot 5 + (1\cdot 5 \vee 0\cdot 4 \vee 0\cdot 3 \vee 0\cdot 2 \vee 0\cdot 1 \vee 0\cdot 0)) \vee 0\cdot 0 \vee 0\cdot 1) + ((1\cdot 0 + (1\cdot 1 \vee 0\cdot 2 \vee 0\cdot 3 \vee 0\cdot 4 \vee 0\cdot 5 \vee 0\cdot 0)) \vee 0\cdot 5 \vee 0\cdot 1) = 11. \quad (4.13)$$

Звернемо увагу, що в процесі оцінювання (кроки 1÷11) вибір певних характеристик порушення засновується на конкретних оцінках діяльності підприємства, які в результаті сформують значення показників $P_{СП}^{\varphi}$, $P_{ХП}^{\varphi}$, $P_{ЗШ}^{\varphi}$, $P_{СВ}^{\varphi}$, $P_{РЦП}^{\varphi}$, $P_{РС}^{\varphi}$, $P_{КД}^{\varphi}$, $P_{СПВ}^{\varphi}$, $P_{ВЗ}^{\varphi}$, $P_{ДК}^{\varphi}$ та $P_{ВЧ}^{\varphi}$ які з наведених прикладів відповідно приймають значення 18, 9, 11, -15, 0, 15, 5, 3, 10, 0 та 11 що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства.

Етап 4. Фіналізована процедура обробки експертних даних

Крок 1. Вибір рекомендацій на основі суджень експерта. Вибір рекомендацій отримується з множини **RE** та підмножини $\mathbf{RE_i}$, відповідно до формули (3.16). Наприклад, при $n_{13} = 11$ $(i = \overline{1,11})$, $n_{131} = 4$ $(j = \overline{1,4})$, $n_{132} = 3$ $(j = \overline{1,3})$, $n_{133} = 3$ $(j = \overline{1,3})$, $n_{134} = 8$ $(j = \overline{1,8})$, $n_{135} = 4$ $(j = \overline{1,4})$, $n_{136} = 3$ $(j = \overline{1,3})$, $n_{137} = 3$ $(j = \overline{1,3})$, $n_{138} = 3$ $(j = \overline{1,3})$, $n_{139} = 2$ $(j = \overline{1,2})$, $n_{1310} = 3$ $(j = \overline{1,3})$, $n_{1311} = 4$ $(j = \overline{1,4})$ та враховуючи всі вище перераховані приклади, формулу (3.16) можна представити як: $\mathbf{RE^{\varphi}} = \{\bigcup_{i=1}^{11} \mathbf{RE_i^{\varphi}}\} = \{\bigcup_{i=1}^{11}\{\bigcup_{j=1}^{n_{13i}} RE_{ij}^{\varphi}\}\} = \{\{RE_{11}^{\varphi}, RE_{12}^{\varphi}, RE_{13}^{\varphi}, RE_{14}^{\varphi}\}, \{RE_{21}^{\varphi}, RE_{22}^{\varphi}, RE_{23}^{\varphi}\},$

$$\{RE_{31}^{\varphi}, RE_{32}^{\varphi}, RE_{33}^{\varphi}\}, \{RE_{41}^{\varphi}, RE_{42}^{\varphi}, RE_{43}^{\varphi}, RE_{44}^{\varphi}, RE_{45}^{\varphi}, RE_{46}^{\varphi}, RE_{47}^{\varphi}, RE_{48}^{\varphi}\},$$
$$\{RE_{51}^{\varphi}, RE_{52}^{\varphi}, RE_{53}^{\varphi}, RE_{54}^{\varphi}\}, \{RE_{61}^{\varphi}, RE_{62}^{\varphi}, RE_{63}^{\varphi}\}, \{RE_{71}^{\varphi}, RE_{72}^{\varphi}, RE_{73}^{\varphi}\}, \{RE_{81}^{\varphi}, RE_{82}^{\varphi}, \quad (4.14)$$
$$RE_{83}^{\varphi}\}, \{RE_{91}^{\varphi}, RE_{92}^{\varphi}\}, \{RE_{101}^{\varphi}, RE_{102}^{\varphi}, RE_{103}^{\varphi}\}, \{RE_{111}^{\varphi}, RE_{112}^{\varphi}, RE_{113}^{\varphi}, RE_{114}^{\varphi}\}\},$$

де описано всі рекомендації (див. (2.81), підрозділ 2.2.).

У цьому випадку, всі зазначені рекомендації використовуються відповідно для кожного свого етапу та мають на меті покращити діяльність підприємства для уникнення повторної появи порушення. Всі рекомендації виставляються тільки для Етапу 3, відповідно до суджень експерта та своєї приналежності до певної категорії [81].

Крок 2. Підрахунок набраних балів відповідно до суджень експерта. Для виконання даного кроку необхідно використати значення показників, отриманих

на Етапі 3 на основі виразів: (4.3-4.13). Для підрахунку набраної кількості балів з усіх етапів, необхідно просумувати значення їх ідентифікаторів відповідно до (3.17):

$$\sum_{i=1}^{11} P_i^{\varphi} = 18+9+11-15+0+15+5+3+10+0+11 = 67 \quad (4.15)$$

Максимальна сума для всіх кроків Етапу 3 складає 160 балів. Обчислимо коефіцієнт обчисленої кількості отриманих балів (total marks coefficient) TMC^{φ} для всіх 11 кроків Етапу 3 відповідно до формули (3.18):

$$TMC^{\varphi} = \frac{\sum_{i=1}^{11} P_i^{\varphi}}{160} = \frac{67}{160} = 0{,}41875. \quad (4.16)$$

Крок 3. Обчислення максимально-наближеного штрафу для підприємства. Для розрахунку максимального збитку для підприємства MF^{φ} скористаємося формулою (3.19). Наприклад, при використанні $T^{\varphi} = 3\,000\,000\,000\,€$ та $P_{СП}^{\varphi} = 0{,}04$ (дивись (4.1) та (4.2) відповідно) матимемо наступний вигляд виразу (3.19):

$$MF^{\varphi} = T^{\varphi} \times P_{СП}^{\varphi} = 3\,000\,000\,000\,€ \times 0{,}04 = 120\,000\,000\,€. \quad (4.17)$$

Для обчислення МНШ AF^{φ} скористаємося формулою (3.20). Наприклад, використовуючи дані із виразів (4.16) та (4.17), маємо наступне обчислення:

$$AF^{\varphi} = MF^{\varphi} \times TMC^{\varphi} = 120\,000\,000\,€ \times 0{,}41875 = 50\,250\,000\,€,$$

де $AF^{\varphi} = 50\,250\,000\,€$ – обчислений максимально-наближений штраф для підприємства враховуючи всі, вище перераховані приклади [81, 82].

Верифікація розробленого методу оцінювання негативних наслідків від порушення конфіденційності персональних даних

Для проведення верифікації розробленого методу було обрано випадки з наступними умовами та отримано результати (табл. 4.1.):

1. $\mathbf{T^{\varphi}} = 120000\,€$, $L_{11}^{\varphi} = \{"Ст.83,п.4,пп.а"\}$, N_{13}^{φ} = «Конфіденційна», N_{23}^{φ} =]Місяць; 6 Місяців]; N_{31}^{φ} =]0; 1000]; N_{42}^{φ} = «Низький», CH_{13}^{φ} = «Середній»; CH_{22}^{φ} = «Ні»; CH_{32}^{φ} = «Застосування», A_{12}^{φ} = «Значна»; A_{22}^{φ} = «Ні»; A_{34}^{φ} = [€100.000€; 0[, R_{11}^{φ} =

$R_{21}^{\varphi} = R_{31}^{\varphi} = R_{51}^{\varphi} = R_{81}^{\varphi} =$ «Так»; $R_{42}^{\varphi} = R_{62}^{\varphi} = R_{72}^{\varphi} =$ «Ні»; $I_{11}^{\varphi} =$ «Так»; $C_{11}^{\varphi} =$ [100%; 75%[, $C_{21}^{\varphi} =$ «Так», $C_{31}^{\varphi} =$ «План по відновленню», $CA_{21}^{\varphi} =$ «Так», $CA_{12}^{\varphi} = CA_{32}^{\varphi} =$ «Ні», $M_{12}^{\varphi} =$ «Інформатор»; $ME_{12}^{\varphi} =$ «Ні», $AD_{22}^{\varphi} =$ «Ні», $F_{12}^{\varphi} =$ «Ні», $F_{21}^{\varphi} =$ «Так», $F_{2116}^{\varphi} =$ «Невідомо».

2. $\mathbf{T}^{\varphi} = 120000\,€$, $L_{11}^{\varphi} = \{"Ст.83,п.4,пп.a"\}$, $L_{21}^{\varphi} = \{"Ст.83,п.5,пп.a"\}$, $L_{22}^{\varphi} = \{"Ст.83,п.4,пп.b"\}$, $N_{13}^{\varphi} =$ «Конфіденційна», $N_{23}^{\varphi} =$]Місяць; 6 Місяців]; $N_{31}^{\varphi} =$]0; 1000]; $N_{42}^{\varphi} =$ «Низький», $CH_{13}^{\varphi} =$ «Середній»; $CH_{22}^{\varphi} =$ «Ні»; $CH_{32}^{\varphi} =$ «Застосування», $A_{12}^{\varphi} =$ «Значна», $A_{22}^{\varphi} =$ «Ні», $A_{34}^{\varphi} =$ [€100.000€; 0[, $R_{11}^{\varphi} = R_{21}^{\varphi} = R_{31}^{\varphi} = R_{51}^{\varphi} = R_{81}^{\varphi} =$ «Так», $R_{42}^{\varphi} = R_{62}^{\varphi} = R_{72}^{\varphi} =$ «Ні»; $I_{11}^{\varphi} =$ «Так», $C_{11}^{\varphi} =$ [100%; 75%[, $C_{21}^{\varphi} =$ «Так», $C_{31}^{\varphi} =$ «План по відновленню», $CA_{21}^{\varphi} =$ «Так», $CA_{12}^{\varphi} = CA_{32}^{\varphi} =$ «Ні», $M_{12}^{\varphi} =$ «Інформатор»; $ME_{12}^{\varphi} =$ «Ні», $AD_{22}^{\varphi} =$ «Ні», $F_{12}^{\varphi} =$ «Ні», $F_{21}^{\varphi} =$ «Так», $F_{2116}^{\varphi} =$ «Невідомо».

3. $\mathbf{T}^{\varphi} = 120000\,€$, $L_{11}^{\varphi} = \{"Ст.83,п.4,пп.a"\}$, $L_{21}^{\varphi} = \{"Ст.83,п.5,пп.a"\}$, $L_{22}^{\varphi} = \{"Ст.83,п.4,пп.b"\}$, $N_{13}^{\varphi} =$ «Конфіденційна», $N_{25}^{\varphi} =$] Рік; ∞[, $N_{33}^{\varphi} =$]50000; 100000]; $N_{34}^{\varphi} =$]100000; 1000000], $N_{44}^{\varphi} =$ «Високий», $CH_{13}^{\varphi} =$ «Середній»; $CH_{22}^{\varphi} =$ «Ні»; $CH_{32}^{\varphi} =$ «Застосування», $A_{14}^{\varphi} =$ «Незначна», $A_{22}^{\varphi} =$ «Ні»; $A_{34}^{\varphi} =$ [€100.000€; 0[, $R_{11}^{\varphi} = R_{21}^{\varphi} = R_{51}^{\varphi} = R_{81}^{\varphi} =$ «Так»; $R_{32}^{\varphi} = R_{62}^{\varphi} = R_{72}^{\varphi} =$ «Ні», $R_{43}^{\varphi} =$ «Невідомо», $I_{12}^{\varphi} =$ «Ні», $I_{1221}^{\varphi} =$ «Так»; $I_{1212}^{\varphi} = I_{1232}^{\varphi} =$ «Ні»; $C_{11}^{\varphi} =$ [100%; 75%[, $C_{21}^{\varphi} =$ «Так», $C_{31}^{\varphi} =$ «План по відновленню», $CA_{11}^{\varphi} = CA_{21}^{\varphi} =$ «Так», $CA_{32}^{\varphi} =$ «Ні», $M_{11}^{\varphi} =$ «Суб’єкт порушник», $M_{111}^{\varphi} =$ «"Суб'єкт порушник" повідомив наглядовий орган протягом 72 годин після виникнення інциденту» відповідно до статті 33(1)», $M_{1111}^{\varphi} =$ «Так»; $ME_{12}^{\varphi} =$ «Ні», $AD_{22}^{\varphi} =$ «Ні», $F_{11}^{\varphi} =$ «Так», $F_{1114}^{\varphi} =$ [€100000; €0[; $F_{21}^{\varphi} =$ «Так», $F_{2116}^{\varphi} =$ «Невідомо».

4. $\mathbf{T}^{\varphi} = 160000\,€$, $L_{11}^{\varphi} = \{"Ст.83,п.4,пп.a"\}$, $L_{21}^{\varphi} = \{"Ст.83,п.5,пп.a"\}$, $L_{22}^{\varphi} = \{"Ст.83,п.4,пп.b"\}$, $N_{13}^{\varphi} =$ «Конфіденційна», $N_{25}^{\varphi} =$] Рік; ∞[, $N_{33}^{\varphi} =$]50000; 100000]; $N_{34}^{\varphi} =$]100000; 1000000], $N_{44}^{\varphi} =$ «Високий», $CH_{13}^{\varphi} =$ «Середній»; $CH_{22}^{\varphi} =$ «Ні»; $CH_{32}^{\varphi} =$ «Застосування», $A_{14}^{\varphi} =$ «Незначна», $A_{22}^{\varphi} =$ «Ні»; $A_{34}^{\varphi} =$ [€100.000€; 0[, $R_{11}^{\varphi} = R_{21}^{\varphi} =$

R_{51}^{φ} = R_{81}^{φ} = «Так»; R_{32}^{φ} = R_{62}^{φ} = R_{72}^{φ} = «Ні», R_{43}^{φ} = «Невідомо», I_{12}^{φ} = «Ні», I_{1221}^{φ} = «Так»; I_{1212}^{φ} = I_{1232}^{φ} = «Ні»; C_{11}^{φ} = [100%; 75%[, C_{21}^{φ} = «Так», C_{31}^{φ} = «План по відновленню», CA_{11}^{φ} = CA_{21}^{φ} = «Так», CA_{32}^{φ} = «Ні», M_{11}^{φ} = «Суб'єкт порушник», M_{111}^{φ} = «"Суб'єкт порушник" повідомив наглядовий орган протягом 72 годин після виникнення інциденту» відповідно до статті 33(1)», M_{1111}^{φ} = «Так»; ME_{12}^{φ} = «Ні», AD_{22}^{φ} = «Ні», F_{11}^{φ} = «Так», F_{1114}^{φ} = [€100000; €0[; F_{21}^{φ} = «Так», F_{2116}^{φ} = «Невідомо».

5. $\mathbf{T}^{\varphi} = 160000\,€$, $L_{11}^{\varphi} = \{"Ст.83,п.4,пп.a"\}$, $L_{21}^{\varphi} = \{"Ст.83,п.5,пп.a"\}$, $L_{22}^{\varphi} = \{"Ст.83,п.4,пп.b"\}$, N_{13}^{φ} = «Конфіденційна», N_{25}^{φ} =] Рік; ∞[, N_{33}^{φ} =]50000; 100000]; N_{34}^{φ} =]100000; 1000000], N_{44}^{φ} = «Високий», CH_{13}^{φ} = «Середній»; CH_{22}^{φ} = «Ні»; CH_{32}^{φ} = «Застосування», A_{14}^{φ} = «Незначна», A_{22}^{φ} = «Ні»; A_{34}^{φ} = [€100.000€; 0[, R_{11}^{φ} = R_{21}^{φ} = R_{51}^{φ} = R_{81}^{φ} = «Так»; R_{32}^{φ} = R_{62}^{φ} = R_{72}^{φ} = «Ні», R_{43}^{φ} = «Невідомо», I_{12}^{φ} = «Ні», I_{1221}^{φ} = «Так»; I_{1212}^{φ} = I_{1232}^{φ} = «Ні»; C_{11}^{φ} = [100%; 75%[, C_{21}^{φ} = «Так», C_{31}^{φ} = «План по відновленню», CA_{11}^{φ} = CA_{21}^{φ} = «Так», CA_{32}^{φ} = «Ні», M_{13}^{φ} = «Заголовки ЗМІ», ME_{12}^{φ} = «Ні», AD_{21}^{φ} = «Так», AD_{2112}^{φ} = «Ні»; F_{11}^{φ} = «Так», F_{1114}^{φ} = [€100000; €0[; F_{21}^{φ} = «Так», F_{2116}^{φ} = «Невідомо».

Таблиця 4.1.

Результат верифікації розробленого методу

Вип адок	$P_{СП}^{\varphi}$	$P_{ХП}^{\varphi}$	$P_{ЗШ}^{\varphi}$	$P_{СВ}^{\varphi}$	$P_{РЦП}^{\varphi}$	$P_{РС}^{\varphi}$	$P_{КД}^{\varphi}$	$P_{СПВ}^{\varphi}$	$P_{ВЗ}^{\varphi}$	$P_{ДК}^{\varphi}$	$P_{ВЧ}^{\varphi}$	MF^{φ}	AF^{φ}
	($\sum$ *балів* / $MF_{P_i^{\varphi}}^{\varphi}$, € / $AF_{P_i^{\varphi}}^{\varphi}$, €)												
1	9 135 300	8 120 225	11 165 225	-5 0 600	0 0 300	1 15 225	5 75 225	5 75 75	0 0 150	0 0 75	0 0 300	2400	510
2	9 270 600	8 240 450	11 330 450	-5 0 1200	0 0 600	1 30 450	5 150 450	5 150 150	0 0 300	0 0 150	0 0 600	4800	1020
3	15 450 600	8 240 450	13 390 450	10 300 1200	100 300 600	1 30 450	10 300 450	0 0 150	0 0 300	0 0 150	7 210 600	4800	2220
4	15 600 800	8 320 600	13 520 600	10 400 1600	100 400 800	1 40 600	10 400 600	0 0 200	0 0 400	0 0 200	7 280 800	6400	2960
5	15 600 800	8 320 600	13 520 600	10 400 1600	100 400 800	1 40 600	10 400 600	5 200 200	0 0 400	5 200 200	7 280 800	6400	3360

Проведено дослідження роботи розробленого методу оцінювання негативних наслідків від порушення конфіденційності персональних даних, із подальшою верифікацією його працездатності. Результати моделювання показали високу чутливість методу до зміни вихідних параметрів, зокрема – рівня конфіденційності, періоду зберігання, виду інциденту, наявності реагування та ступеня шкоди.

Аналіз таблиці кейсів свідчить, що навіть за схожих технічних характеристик витоку, значний вплив на фінальні показники мають якісні фактори. Наприклад, у кейсах 4 і 5, незважаючи на однакові показники обсягу та тривалості витоку, відсутність повідомлення наглядового органу у п’ятому випадку призвела до збільшення підсумкових фінансових втрат (3360 € проти 2960 €). Такий результат демонструє здатність методу інтегрувати вимоги GDPR, зокрема щодо своєчасного інформування органів нагляду.

Також простежується прогресивне зростання санкцій та фінансових втрат зі збільшенням чутливості персональних даних та часу їх зберігання. Наприклад, кейс 1, який включає обмежену кількість інцидентів і мінімальний вплив, сформував суму втрат 2400 €, тоді як кейси 4 та 5 – досягли втрат у 6400 €, з різним рівнем штрафів залежно від реакції організації. Це підтверджує, що метод адекватно масштабує оцінку збитків залежно від тяжкості інциденту, кількості уразливих факторів та відповідності діям суб'єкта законодавчим вимогам.

Додатково встановлено, що метод враховує джерело загрози: у випадках, коли витік даних ініційовано внутрішнім суб’єктом (працівником), автоматично підвищується коефіцієнт ризику, що дозволяє використовувати метод для оцінювання внутрішніх загроз. За допомогою бальної шкали та прив’язки до грошових еквівалентів метод дозволяє обґрунтувати можливі фінансові наслідки у форматі, придатному для бізнес-рішень і відповідності принципам прозорості, передбаченим GDPR.

Отримані результати свідчать про коректність функціонування розробленого методу у різних контекстах витоку персональних даних, його

здатність враховувати множинні параметри ризику та забезпечувати адаптивну оцінку шкоди. Метод придатний до масштабування та може бути реалізований як елемент автоматизованої системи управління інформаційними ризиками.

Для реалізації розробленого методу необхідно розробити автоматизовану систему оцінювання потенційних фінансових наслідків від витоку ПД, що дозволить організаціям ефективно впроваджувати вимоги GDPR забезпечуючи високий рівень захисту даних.

4.2. Експериментальне дослідження методу оцінювання безпеки персональних даних в процесі обробки в автоматизованих системах

Розроблений в 3.2. метод оцінювання безпеки персональних даних [68] відповідає національним та світовим практикам управління інформаційною безпекою. Проте ефективність та придатність цього методу до практичного застосування в умовах українського правового, організаційного та технічного середовища потребує верифікації та підтвердження шляхом дослідження. Результати дослідження дозволять перевірити стабільність методу при зміні вхідних умов, а також виявити його межі застосовності. Це, в свою чергу, є передумовою для його вдосконалення, розширення або інтеграції в існуючі системи управління інформаційною безпекою.

Етап 1. Визначаємо документи у яких наявні ПД та коефіцієнт їх важливості, відповідно до табл.2.2: паспорт (A_1), $K_{vd1}=0,9$; військовий квиток (A_2), $K_{vd2}=0,8$; свідоцтво про народження (A_3), $K_{vd3}=0,7$; свідоцтво про шлюб (A_6), $K_{vd6}=0,5$; трудова книжка (A_7), $K_{vd7}=0,5$. Сумарна величина коефіцієнтів важливості визначається за формулою (3.21).

$$K_{vd}=K_{vd1}+K_{vd2}+K_{vd3}+K_{vd6}+K_{vd7}=3,4. \quad (4.18)$$

Нехай під загрозою знаходяться документи A_1, A_3 та A_6, тоді за формулою (3.21): $K_{vdr}=K_{vd1}+K_{vd3}+K_{vd6}=2,1$. Наступним кроком відбувається визначення середовища обробки ПД, що містяться у вказаних документах, відповідно до таблиці 2.3: Word (B_1) $K_{vp1}=0,3$; Excel (B_2) $K_{vp2}=0,4$; Access (B_3) $K_{vp3}=0,5$;

«Працівники» (B_5) $K_{vp5}=0,7$; «IT-Enterprise» (B_7) $K_{vp7}=0,9$. Нехай ПД обробляються ПЗ B_2 та B_5. Аналогічно, за формулою (3.21), визначаються коефіцієнти K_v та K_{vr} для ПЗ обробки ПД. Таким чином, значення $K_{vp}=2,8$ та $K_{vpr}=1,1$. Визначення максимально можливого розрахункового значення ризику R_{max} визначається за формулою (3.22):

$$R_{max}=\frac{K_{vdr}+K_{vpr}}{K_{vd}+K_{vp}}=\frac{2,1+1,1}{3,4+2,8}=0,52 \qquad (4.19)$$

Проте, для оцінки ризику захисту ПД, необхідно дослідити використані в АС механізми безпеки ПД, існуючі загрози захисту ПД та визначити відповідний їм рівень реалізації.

Етап 2. На даному етапі проводиться аналіз функціонуючих механізмів безпеки. Кожен із запропонованих механізмів безпеки в моделі забезпечує корегування визначеного максимально можливого розрахункового значення ризику на коефіцієнт 0,2. Нехай в АС наявні 3 механізми безпеки (D_i, i=1÷3), тоді сумарний коефіцієнт відповідно до формули (3.23) $K_m=3\times 0,2=0,6$.

Етап 3. Передбачається ідентифікація можливих загроз захисту ПД при обробці БПД в АС. Перелік цих загроз (**F**) визначається запропонованим методом аналізу і оцінки ризиків ПД в БПД. Нехай, в прикладі визначено загрози з «низькими» та «середніми» рівнями, то відповідно до формули (2.82) $P_{riv\_zag}=0,6$, тоді згідно з (3.24) [68]:

$$R_{zag_{corr}}=P_{riv\_zag}\times R_{max}=0,6\times 0,52=0,31 \qquad (4.20)$$

Після розрахунку $R_{zag_{corr}}$, визначимо розрахунковий інтервал – в межах якого і знаходиться реальний ризик захисту ПД. Весь інтервал $I\in(I_{min},I_{max})$ згідно таблиці 2.4 поділено на підінтервали [0÷0,1], [0,1÷0,3], [0,3÷0,6], [0,6÷0,8], [0,8÷1].

Етап 4. Визначення величини можливого збитку від витоку ПД (чи БПД в АС) може визначатися як кількісними, так і якісними показниками. Оскільки $R_{zag_{corr}}=0,31$, то згідно до розробленої моделі аналізу і оцінки ризиків ПД в БПД,

а саме таблиці 2.4, наведено шкали показників величин можливих збитків: розрахунковий інтервал ризику можливого витоку ПД – [0,31÷0,6]; грошовий еквівалент ризику можливих збитків – (1000÷10000 $); бальна оцінка ризику втрати ПД – 3 бали.

Етап 5. Визначимо корекцію ймовірності з врахуванням механізмів захисту (R_{C_corr}) за формулою (3.25). У даному випадку R_{C_corr}, де $I \in (I_{min}, I_{max})$, $I \in (0,31 \div 0,6)$: $R_{C\_corr} = (0,31 + (0,6 - 0,31) \times (1 - 0,6)) = 0,426$.

Даний інтервал витоку ПД визначається збитками в грошовому еквіваленті на рівні $G \in (G_{min}, G_{max})$ $G \in (1000 \div 10000\ \$)$. Таким чином ймовірні збитки в грошах, визначаються за формулою (3.26):

$$R_g = 1000 + (10000 - 1000) \times 0,426 = 4834\ \$ \qquad (4.21)$$

Етап 6. Після проведення аналізу та оцінки ризиків ПД в БПД, можна сформувати кінцеві висновки про стан рівня захищеності ПД в конкретній АС. А отже, можна надати рекомендації щодо підвищення цього стану, а саме через впровадження тих чи інших механізмів безпеки, що запропоновані в таблиці 2.6. Оскільки було визначено ризик витоку ПД у 3 бали, то згідно до таблиці 2.6, в АС необхідно – використати ТЗІ/КЗІ (технічний та/або криптографічний ЗІ). Таким чином проведено оцінку ризиків захисту ПД у БПД в АС на конкретному прикладі.

Верифікація методу. Для проведення верифікації розробленого методу було обрано 2 випадки з наступними умовами [68]:

1) ПД (A_i) обробляються ПЗ B_2 та B_5 при $K_{vd} = 3,4$; $K_{vp} = 2,8$; $K_{vpr} = 1,1$; $K_m = 0,6$, $P_{riv\_zag} = 0,6$, отримані результати приведені у таблиці 4.2.

2) ПД (A_i) обробляються ПЗ B_2, B_5 та B_7 при $K_{vd} = 3,4$; $K_{vp} = 2,8$; $K_{vpr} = 1,1$; $K_m = 0,6$, $P_{riv\_zag} = 1$, отримані результати приведені у таблиці 4.3.

Таблиця 4.2

Результати верифікації 1-го випадку

Документи	K_{vdr}	R_{max}	$R_{zag_{corr}}$	Інтервал	Бали	Грошовий еквівалент	R_{C_corr}	R_g
A_6	0,5	0,26	0,15	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
…	…	…	…	…	…	…	…	…
A_1	0,9	0,32	0,19	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
A_1, A_6	1,4	0,40	0,24	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
…	…	…	…	…	…	…	…	…
A_1, A_2	1,7	0,45	0,27	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
A_2, A_3, A_6	2	0,50	0,30	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
…	…	…	…	…	…	…	…	…
A_1, A_2, A_3	2,4	0,56	0,34	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
A_2, A_3, A_6, A_7	2,5	0,58	0,35	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
…	…	…	…	…	…	…	…	…
A_1, A_2, A_3, A_6	2,9	0,65	0,39	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
…	…	…	…	…	…	…	…	…
A_1, A_2, A_3, A_6, A_7	3,4	0,73	0,44	0,31 ÷ 0,6	3	1000-10000$	0,426	4834

Таблиця 4.3

Результати верифікації 2-го випадку

Документи	K_{vdr}	R_{max}	$R_{zag_{corr}}$	Інтервал	Бали	Грошовий еквівалент	R_{C_corr}	R_g
A_6	0,5	0,40	0,40	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
…	…	…	…	…	…	…	…	…
A_1	0,9	0,47	0,47	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
A_1, A_6	1,4	0,55	0,55	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
…	…	…	…	…	…	…	…	…
A_1, A_2	1,7	0,60	0,60	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
A_2, A_3, A_6	2	0,65	0,65	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
…	…	…	…	…	…	…	…	…
A_1, A_2, A_3	2,4	0,71	0,71	0,61 ÷ 0,8	4	10000-100000$	0,686	71740
A_2, A_3, A_6, A_7	2,5	0,73	0,73	0,61 ÷ 0,8	4	10000-100000$	0,686	71740
…	…	…	…	…	…	…	…	…
A_1, A_2, A_3, A_6	2,9	0,79	0,79	0,61 ÷ 0,8	4	10000-100000$	0,686	71740
…	…	…	…	…	…	…	…	…
A_1, A_2, A_3, A_6, A_7	3,4	0,87	0,87	0,81 ÷ 1	5	100000-1000000$	0,426	897400

Метод було апробовано на двох тестових випадках, що охоплювали різні комбінації типів документів, програмного забезпечення для обробки персональних даних, кількості реалізованих механізмів захисту та рівнів загроз. Аналіз результатів, представлених у таблицях 4.2 та 4.3, дозволяє зробити такі ключові висновки:

Метод демонструє стабільність при зміні вхідних параметрів. У кожному з варіантів простежується логічна послідовність росту ризику в міру зменшення рівня захисту та збільшення вагомості оброблюваних даних. Наприклад, у другому випадку при зростанні сумарного коефіцієнта вагомості документів та використанні менш надійного програмного середовища, значення ризику суттєво перевищує відповідні показники першого варіанту.

Метод коректно визначає інтервали ризику та пов’язані з ними збитки. У першому випадку значення ризику в більшості комбінацій залишаються в межах інтервалу [0,11 ÷ 0,3], що відповідає 2 бальній оцінці та незначним грошовим втратам (100–1000 $). У другому випадку при менш сприятливих умовах обробки, ризик послідовно зростає — від середнього (3 бали, до 10 000 $) до високого (4–5 балів, понад 100 000 $).

Виявлено критичні порогові значення. Як видно з таблиці 4.3, при подальшому підвищенні сумарного коефіцієнта вагомості (до 3,4) та відповідного збільшення ймовірності реалізації загроз, значення ризику переходить в інтервал [0,81 ÷ 1], що відповідає критичному рівню втрат (5 балів, понад 100 000 $). Це дозволяє встановлювати граничні допустимі значення для ризику ПД в АС і формувати вимоги до обов’язкового впровадження КЗІ/ТЗІ.

4.3. Експериментальне дослідження методу оцінювання рівня критичності у разі витоку персональних даних

Розробка методу оцінювання рівня критичності інцидентів витоку персональних даних [80] є лише першим кроком на шляху до його практичного застосування. Для підтвердження ефективності та доцільності використання запропонованого підходу необхідно здійснити його дослідження, що дозволяє

виявити сильні сторони методу, перевірити його здатність адекватно реагувати на різноманітні сценарії витоків, а також оцінити його чутливість до різних вхідних параметрів. Оскільки критичність витоку персональних даних залежить від багатьох чинників – таких як тип даних, обсяг, контекст витоку, потенційні наслідки для суб'єктів даних та організації – важливо переконатися, що метод враховує ці аспекти належним чином і дозволяє отримати об'єктивну та обґрунтовану оцінку. Дослідження методу також необхідне для верифікації його застосовності в реальних умовах, виявлення обмежень, а також для формування рекомендацій щодо подальшого вдосконалення. Розглянемо роботу механізмів кореляції подій та оцінювання сумарного та середнього рівнів критичності ситуації, що склалась під впливом декількох ІПКС на прикладі [80].

Нехай **A, B, C, D** та **E** – ідентифікатори інцидентів, де **A** – Зміна кліматичних умов в серверній, В – Мережева атака відмова в обслуговувані, **C** – Крадіжка обладнання та носіїв інформації, **D** – Злам мережі порушником, **E** – Повінь. Спочатку необхідно визначити множини оціночних параметрів, які відповідають кожному з них, для того, щоб виявити залежність між цими ІПКС.

Так, зміна кліматичних умов в серверній, характеризується такою множиною оціночних параметрів: $\mathbf{L_A} = \{ TR - L_1; DVF - L_2; OS - L_4; OLED - L_5; DDI - L_{10}; CRT - L_{11}; CRP - L_{12} \}$. Аналогічно для мережевої атаки відмова в обслуговувані: $\mathbf{L_B} = \{ TR - L_1; DVF - L_2; OS - L_4; OLED - L_5; F - L_9; DDI - L_{10}; CRT - L_{11}; CRP - L_{12}; DVChS - L_{15} \}$. Для крадіжка обладнання і носіїв інформації: $\mathbf{L_C} = \{ DVF - L_2; OS - L_4; OLED - L_5; F - L_9; DDI - L_{10}; DVChS - L_{15} \}$. Злам мережі порушником характеризується множиною $\mathbf{L_D} = \{ TR - L_1; DVF - L_2; OS - L_4; F - L_9; CRT - L_{11}; CRP - L_{12}; DVChS - L_{15} \}$. І останній ІПКС - повінь: $\mathbf{L_E} = \{ TR - L_1; DVF - L_2; GS - L_3; OLED - L_5; RTLH - L_7; F - L_9; DDI - L_{10}; RTLH - L_7; CRP - L_{12} \}$.

Під час експериментального дослідження були промодельовані ІПКС і проведена їх оцінка в чіткій і нечіткій формі, що наведені в таблиці 4.4.

Таблиця 4.4.

Результати оцінювання ІПКС

ІПКС	Рівень критичності	НЧ
A	60 балів або 0,6	0/0,4; 1/0,6; 0/0,8
B	80 балів або 0,8	0/0,6; 1/0,8; 0/1
C	30 балів або 0,3	0/0,1;1/0,3;0/0,5
D	40 балів або 0,4	0/0,2; 1/0,4; 0/0,6
E	50 балів або 0,5	0/0,3; 1/0,5; 0/0,7

Припустимо, що в якості основного ІПКС експертом була обрана крадіжка обладнання і носіїв інформації, оскільки основний акцент в діяльності організації робиться на забезпеченні конфіденційності інформації. Далі визначаємо коефіцієнт кореляції між подіями, причому С – основний ІПКС, A,B,D,E – залежні. Тоді: $\underset{\sim}{LCS}_C = \underset{\sim}{LCS}_{осн} = \underset{\sim}{LCS}_1$, $\underset{\sim}{LCS}_A = \underset{\sim}{LCS}_{зал_2} = \underset{\sim}{LCS}_2$, $\underset{\sim}{LCS}_B = \underset{\sim}{LCS}_{зал_3} = \underset{\sim}{LCS}_3$, $\underset{\sim}{LCS}_D = \underset{\sim}{LCS}_{зал_4} = \underset{\sim}{LCS}_4$, $\underset{\sim}{LCS}_E = \underset{\sim}{LCS}_{зал_5} = \underset{\sim}{LCS}_5$. Розрахуємо коефіцієнти кореляції для обраних залежних подій, використовуючи вираз:

$$K_{12} = K_{CA} = K_{IKS_{осн} IKS_{зал_2}} = \frac{|(\mathbf{L_{осн}} \cap \mathbf{L_{зал_2}})|}{|\mathbf{L_{зал_2}}|} = = \frac{|(\mathbf{L_C} \cap \mathbf{L_D})|}{|\mathbf{L_D}|} = \frac{4}{7},$$

$$K_{13} = K_{CB} = K_{IKS_{осн} IKS_{зал_3}} = \frac{|(\mathbf{L_C} \cap \mathbf{L_B})|}{|\mathbf{L_B}|} = \frac{6}{9} = \frac{2}{3},$$

$$K_{14} = K_{CD} = K_{IKS_{осн} IKS_{зал_4}} = \frac{|(\mathbf{L_C} \cap \mathbf{L_A})|}{|\mathbf{L_A}|} = \frac{4}{7},$$

$$K_{15} = K_{CE} = K_{IKS_{осн} IKS_{зал_5}} = \frac{|(\mathbf{L_C} \cap \mathbf{L_E})|}{|\mathbf{L_E}|} = \frac{3}{8}.$$

Таким чином, розраховані всі коефіцієнти кореляції для даного набору з 5-ти ІПКС. Розрахуємо середній рівень критичності без врахування взаємозалежностей між окремими ІПКС, скориставшись формулою:

$$\underset{\sim}{LCS}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \underset{\sim}{LCS}_2 + \underset{\sim}{LCS}_3 + \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_5) = \text{ (1/5)*({0/0,1; 1/0,3; 0/0,5} +}$$

{0/0,2; 1/0,6; 0/0,8} + {0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/0,3; 0/0,7; 0/0,9; 0/0,5; 1/0,9; 0/1,1; 0/0,7; 0/1,1; 0/1,3}+{0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/0,7; 1/0,9; 0/1,1}+{0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,3; 0/1,5; 0/1,7; 0/1,5; 1/1,7; 0/1,9; 0/1,7; 0/1,9; 0/2,1}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,5; 1/1,7; 0/1,9}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,5; 1/1,7; 0/1,9}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,7; 0/1,9; 0/2,1; 0/1,9; 1/2,1; 0/2,3; 0/2,1; 0/2,3; 0/2,5}+ {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,9; 1/2,1; 0/2,3}+ {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/2,2; 0/2,4; 0/2,6; 0/2,4; 1/2,6; 0/2,8; 0/2,6; 0/2,8; 0/3}) = (1/5)({0/2,4; 1/2,6; 0/2,8}) = {0/0,48; 1/0,52; 0/0,56} або після дефазифікації $\underset{\sim}{LCS}_{сер} = 0{,}52$ або *52* бали за *100*-бальною шкалою.

Для того, щоб визначити середнє значення рівня критичності щодо окремого аспекту, зазвичай по якійсь окремій найважливішій характеристиці потрібно застосувати механізм кореляції. Надалі будемо проводити розрахунки для спрощення обчислень використовуючи апарат звичайної (чіткої) арифметики. Визначимо середній рівень критичності поточної ситуації за виразом:

$$\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \sum_{i=2}^{5} K_{IKS_{осн} IKS_{заг_i}} * \underset{\sim}{LCS}_i) = (1/5)* (0{,}3 + (4/7)*0{,}6) + (2/3)*0{,}8 + (4/7)*0{,}4 + (3/8)*0{,}5) = 0{,}32$$

або *32* бали за *100*-бальною шкалою.

Як бачимо, середнє значення рівня критичності з врахуванням кореляції між інцидентами менше ніж без врахування, що пояснюється виділенням конкретного аспекту щодо оцінки впливу, за умов експерименту – збереження конфіденційності інформаційних ресурсів. Таким чином, той вплив, що породжує порушення інших характеристик, в даних розрахунках не враховано. Для перевірки адекватності запропонованого механізму перевіримо коректність результатів при подачі у вигляді вхідних даних рівнів критичності всіх виявлених інцидентів, що становлять 0 і 1 [80] (табл. 4.5 та табл. 4.6).

Таблиця 4.5

Результати оцінювання ІПКС

ІПКС	Рівень критичності	НЧ
A	0	0/0; 1/0; 0/0,2
B	0	0/0; 1/0; 0/0,2
C	0	0/0; 1/0; 0/0,2
D	0	0/0; 1/0; 0/0,2
E	0	0/0; 1/0; 0/0,2

Очевидно, що коли рівень критичності всіх ІПКС буде 0 балів, то $\underset{\sim}{LCS}_{сер} = \underset{\sim}{LCS}^{K}_{сер} = 0$.

Таблиця 4.6

Результати оцінювання ІПКС

ІПКС	Рівень критичності	НЧ
A	100 балів або 1	0/0,8; 1/1; 0/1
B	100 балів або 1	0/0,8; 1/1; 0/1
C	100 балів або 1	0/0,8; 1/1; 0/1
D	100 балів або 1	0/0,8; 1/1; 0/1
E	100 балів або 1	0/0,8; 1/1; 0/1

Розрахуємо середній рівень критичності ситуації без врахування показників кореляції інцидентів в випадку коли всі ІПКС мають максимальну критичність.

$\underset{\sim}{LCS}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \underset{\sim}{LCS}_2 + \underset{\sim}{LCS}_3 + \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_5) = 1/5(1+1+1+1+1) = 1$ або *100* балів.

З врахування кореляційної взаємозалежності інцидентів згідно з формулою:

$\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \sum_{i=2}^{5} K_{IKS_{осн} IKS_{заг_i}} * \underset{\sim}{LCS}_i) = (1/5)* (1 + (4/7)*1) + (2/3)*1 + (4/7)*1 + (3/8)*1) = 0,64$ або *64* бали за *100*-бальною шкалою. Як видно, отримані результати цілком коректні і не виходять за область допустимих значень рівня критичності $[0;\ 1]$. Проаналізуємо коректність застосування механізму визначення сумарного

рівня критичності ситуації в залежності від врахування взаємної кореляції інцидентів.

Розрахуємо сумарний рівень критичності без врахування взаємозалежностей між окремими ІПКС, скориставшись формулою:

$$\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}_i \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}_i) = 0{,}5 + 0{,}3\ ((1\text{-}0{,}6)(1\text{-}0{,}8)(1\text{-}0{,}4)(1\text{-}0{,}5))$$

$+ 0{,}6\ ((1\text{-}0{,}8)(1\text{-}0{,}4)(1\text{-}0{,}5)) + 0{,}8((1\text{-}0{,}4)(1\text{-}0{,}5)) + 0{,}4\ (1\text{-}0{,}5) = 0{,}5 + 0{,}0072 + 0{,}036 + 0{,}24 + 0{,}2 = 0{,}9832$ або *98* балів за *100*-бальною шкалою.

Застосуємо механізм кореляції інцидентів, щоб визначити сумарний рівень критичності ситуації, що склалася внаслідок їх комплексного впливу. Визначимо сумарний рівень критичності поточної ситуації, причому коефіцієнти кореляції застосуємо такі ж як в попередньому прикладі, тобто: $K_{12} = \frac{4}{7}$, $K_{13} = \frac{2}{3}$, $K_{14} = \frac{4}{7}$, $K_{15} = \frac{3}{8}$, а вхідні дані з табл. 4.4. Відповідно $\underset{\sim}{LCS}_2^K = K_{12} * \underset{\sim}{LCS}_2$, $\underset{\sim}{LCS}_3^K = K_{13} * \underset{\sim}{LCS}_3$, $\underset{\sim}{LCS}_4^K = K_{14} * \underset{\sim}{LCS}_4$, $\underset{\sim}{LCS}_5^K = K_{15} * \underset{\sim}{LCS}_5$ і $\underset{\sim}{LCS}_1^K = \underset{\sim}{LCS}_1$. Отже,

$$\underset{\sim}{LCS}_{сум}^K = \underset{\sim}{LCS}_5^K + \sum_{i=1}^{4} \underset{\sim}{LCS}_i^K \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}_i^K) = (3/8)0{,}5 + 0{,}3((1\text{-}(4/7)0{,}6)(1\text{-}(2/3)0{,}8)(1\text{-}$$

$(4/7)0{,}4)(1\text{-}(3/8)0{,}5)) + (4/7)0{,}6\ ((1\text{-}(2/3)0{,}8)(1\text{-}(4/7)0{,}4)(1\text{-}(3/8)0{,}5)) + (2/3)0{,}8((1\text{-}(4/7)0{,}4)(1\text{-}(3/8)0{,}5)) + (4/7)0{,}4(1\text{-}(3/8)0{,}5) = 0{,}1875 + 0{,}0577 + 0{,}1003 + 0{,}3343 + 0{,}1857 = 0{,}8655$ або *87* балів за *100*-бальною шкалою. Як бачимо, сумарне значення рівня критичності з врахуванням кореляції між інцидентами менше ніж без врахування, що також пояснюється виділенням конкретного аспекту щодо оцінки впливу, за умов експерименту – збереження конфіденційності інформаційних ресурсів. Таким чином, той вплив, що породжує порушення інших характеристик, в даних розрахунках не враховано. Для перевірки адекватності запропонованого методу перевіримо коректність результатів при подачі у вигляді вхідних даних рівнів критичності всіх виявлених інцидентів, що становлять 0 і 1 (табл. 4.5 та табл. 4.6 відповідно). Очевидно, що коли рівень критичності всіх

ІПКС буде 0 балів, то $\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}^{K}_{сум} = 0$.

Розглянемо ситуацію, яка виникає під впливом інцидентів з максимальною критичністю. Розрахуємо сумарний рівень критичності ситуації без врахування показників кореляції інцидентів в такому випадку:

$$\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}_i \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}_i) = 1 + 1\ ((1\text{-}1)(1\text{-}1)(1\text{-}1)(1\text{-}1)) + 1((1\text{-}1)(1\text{-}1)(1\text{-}1)) + 0{,}8((1\text{-}1)(1\text{-}1)) + 1(1\text{-}1) = 1$$

або *100* балів. З врахування кореляційної взаємозалежності інцидентів згідно з формулою:

$$\underset{\sim}{LCS}^{K}_{сум} = \underset{\sim}{LCS}^{K}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}^{K}_i \prod_{i=2}^{5} (1 - \underset{\sim}{LCS}^{K}_i) = (3/8) + (1\text{-}(4/7))(1\text{-}(2/3))(1\text{-}(4/7))(1\text{-}(3/8)) + (4/7)(1\text{-}(2/3))(1\text{-}(4/7))(1\text{-}(3/8)) + (2/3)(1\text{-}(4/7))(1\text{-}(3/8)) + (4/7)(1\text{-}(3/8)) = 0{,}375 + 0{,}038265 + 0{,}05102 + 0{,}178571 + 0{,}357143 = 1$$

або *100* балів за *100*-бальною шкалою. Як видно отримані результати, так само як і при визначені середнього рівня критичності, цілком коректні і не виходять за область допустимих значень [0; 1], що підтверджує адекватність розроблених механізмів. У результаті проведеного дослідження методу оцінювання рівня критичності інцидентів витоку персональних даних встановлено його обґрунтованість, коректність та практичну придатність. Основна увага в експериментальному аналізі була приділена перевірці здатності методу враховувати взаємозв'язки між інцидентами порушення конфіденційності та його поведінці при зміні вхідних параметрів [80].

Проведені обчислення підтвердили, що середній рівень критичності, розрахований без урахування кореляцій між інцидентами, є завищеним порівняно з результатом, отриманим з урахуванням кореляційної взаємозалежності. Це демонструє важливість урахування взаємного впливу інцидентів, особливо при оцінюванні ситуації з фокусом на окремий аспект, такий як конфіденційність даних. Сумарний рівень критичності також має нижчі значення при врахуванні кореляцій, що свідчить про гнучкість та адаптивність методу до специфіки впливу різних інцидентів. Це дозволяє уникати переоцінки критичності ситуації у разі дублювання ефектів чи взаємного послаблення впливу інцидентів.

Метод адекватно реагує на граничні випадки: при подачі нульових або максимальних значень критичності усіх інцидентів результати залишаються в межах допустимого діапазону [0; 1] і відображають логічні очікування (0 балів – повна відсутність загрози, 100 балів – критична ситуація). Реалізовані математичні механізми – як у нечіткій, так і в чіткій формі – забезпечують точність оцінювання, демонструючи правильну роботу під час агрегації, дефазифікації та врахування кореляційних коефіцієнтів. Таким чином, обчислювальні експерименти підтвердили працездатність і обґрунтованість розробленого методу. Його можна застосовувати як основу для прийняття рішень щодо реагування на інциденти порушення конфіденційності, з можливістю подальшого вдосконалення через урахування додаткових факторів або вагомості характеристик.

4.4. Розробка алгоритмічного та програмного забезпечення системи оцінки негативних наслідків втрати персональних даних

Розробка алгоритмічного забезпечення є ключовим етапом реалізації системи оцінки негативних наслідків втрати персональних даних, оскільки саме алгоритмічне наповнення визначає функціональну поведінку кожного з компонентів, що були попередньо сформовані на етапі побудови структурної моделі. Структурна модель системи задає загальну архітектуру та взаємозв’язки між її функціональними блоками, однак для перетворення цієї архітектури на працююче рішення необхідно формалізувати послідовність дій у вигляді алгоритмів, які реалізують логіку обробки інцидентів порушення конфіденційності. Розроблені алгоритми повинні враховувати специфіку аналізу персональних даних, відповідність статтям GDPR, правила оцінки штрафних санкцій, а також механізми формування звітності. Такий підхід забезпечує однозначне та систематичне перетворення вхідних даних користувача у формалізовану оцінку критичності інциденту, що є основою для прийняття рішень у сфері інформаційної безпеки.

Для детального представлення функціонування структурної схеми системи

(рис. 3.4) було розроблено алгоритми роботи кожного з її блоків [105, 106]. У стисненому вигляді послідовність дій системи представлена на рисунку 4.1. Перший етап – «Ідентифікація порушення» – передбачає введення базової інформації про підприємство, в якому стався інцидент.

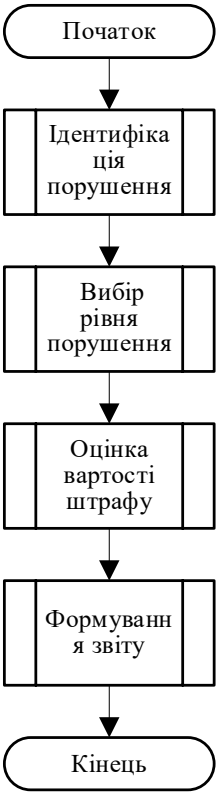


Рис. 4.1. Алгоритм послідовного виконання основних етапів програмної системи оцінки негативних наслідків від витоку персональних даних

Другий етап – «Вибір рівня порушення» – передбачає визначення порушеної статті Регламенту GDPR, на основі чого автоматично встановлюється відповідний рівень порушення.

Третій етап – «Оцінка вартості штрафу» – реалізується як послідовність питань та варіантів відповідей, що моделюють характеристики конкретного інциденту (рисунок 4.2). Цей блок складається з одинадцяти підпроцесів, кожен з яких охоплює окремий аспект оцінки. Кожен підпроцес включає у себе питання, топологію логіки переходів між ними та механізми запису результатів у файли для подальшого опрацювання. Наприклад, перший підпроцес – «Питання пункту (а)» – показано на рисунку 4.4.

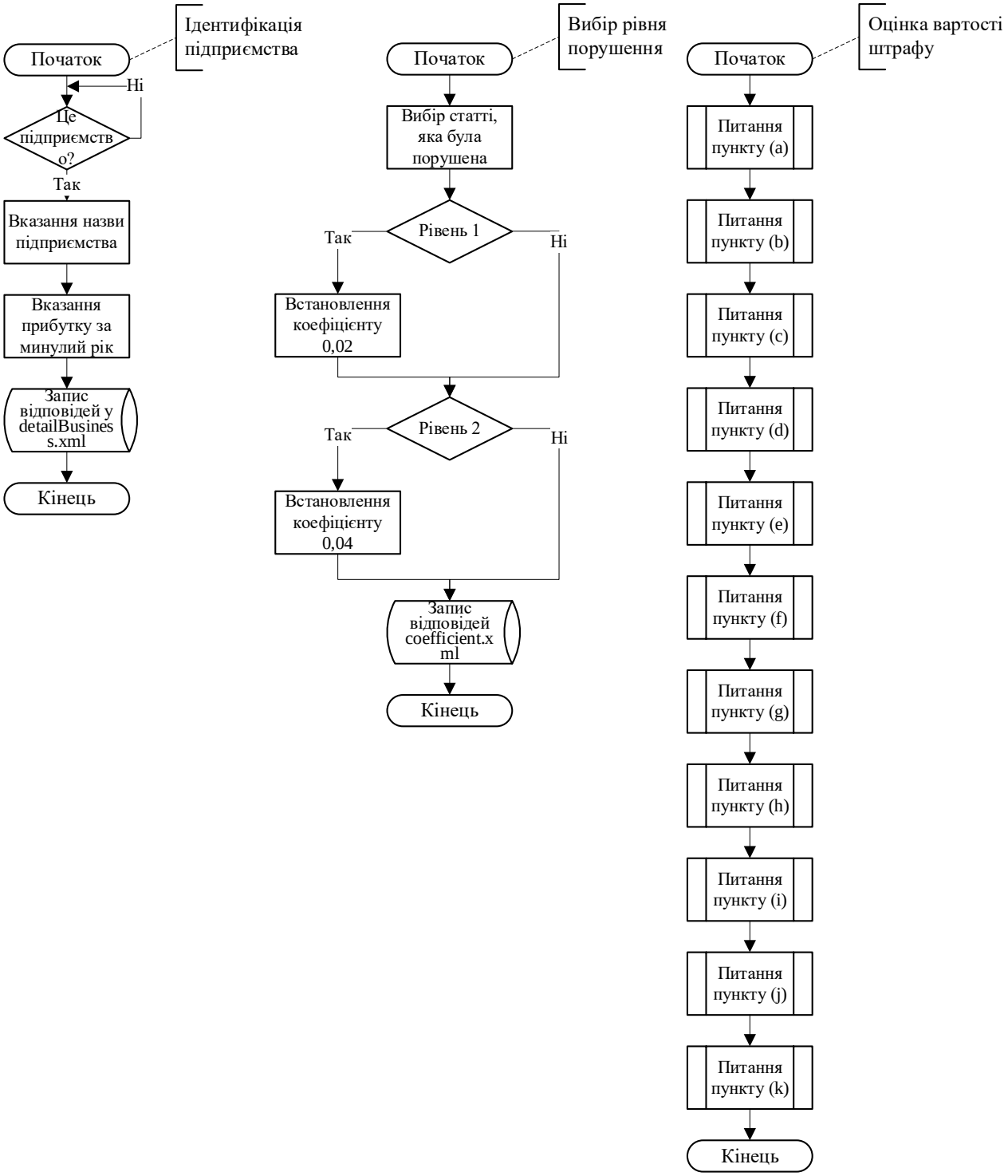


Рис. 4.2. Підпроцеси перших трьох пунктів програмної системи

Четвертий етап – «Формування звіту» – виконує узагальнення введеної користувачем інформації, а також результатів оцінювання. Система враховує відповідні критерії та нараховані бали, на основі чого розраховується орієнтовна сума штрафу, що може бути накладена на підприємство за результатами

порушення. Крім того, для кожного пункту надаються рекомендації, що дозволяє виявити недоліки в інформаційній системі підприємства та мінімізувати ризики їх повторення в майбутньому (рисунок 4.3).

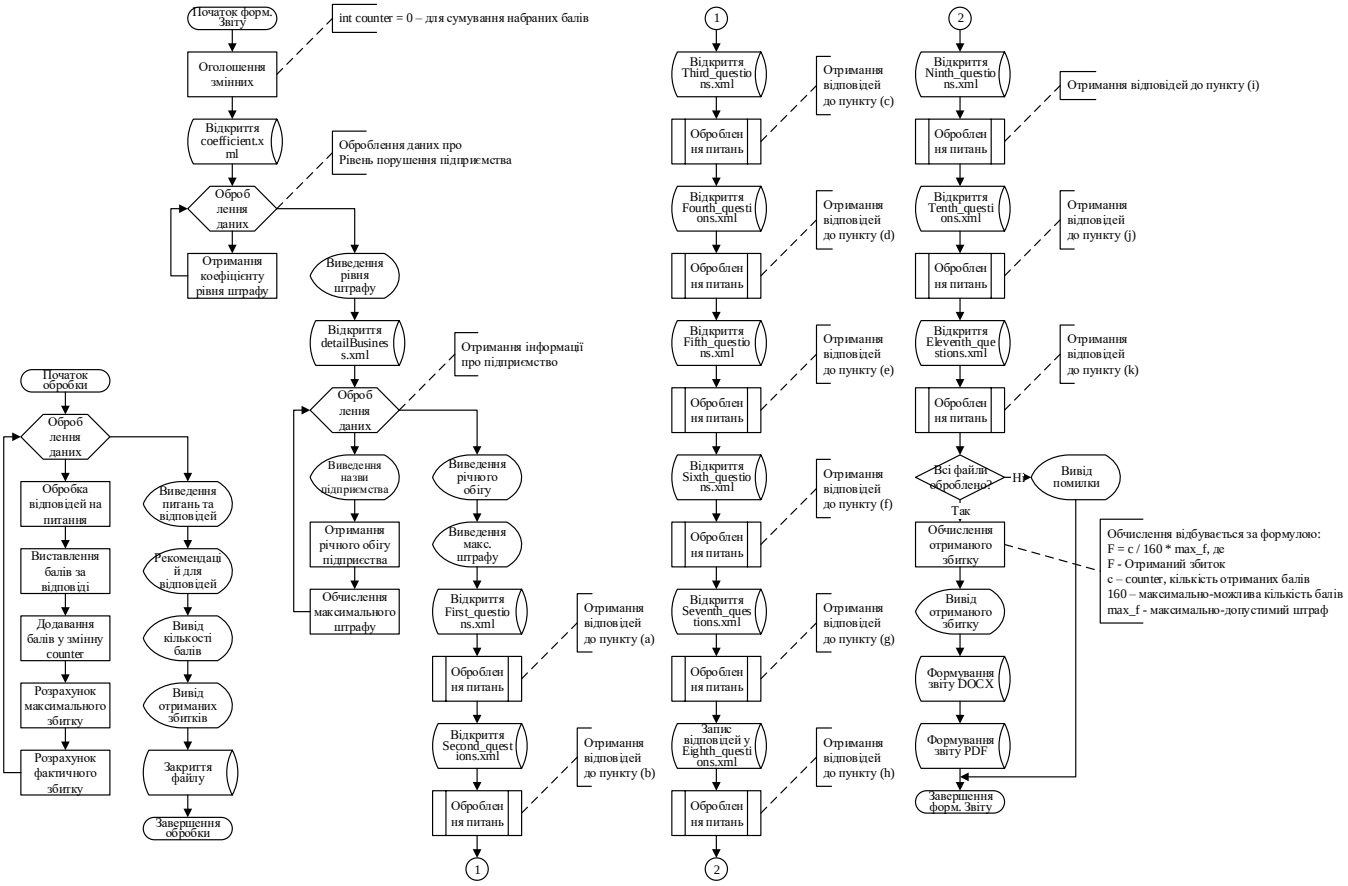


Рис. 4.3. Підпроцес формування звіту

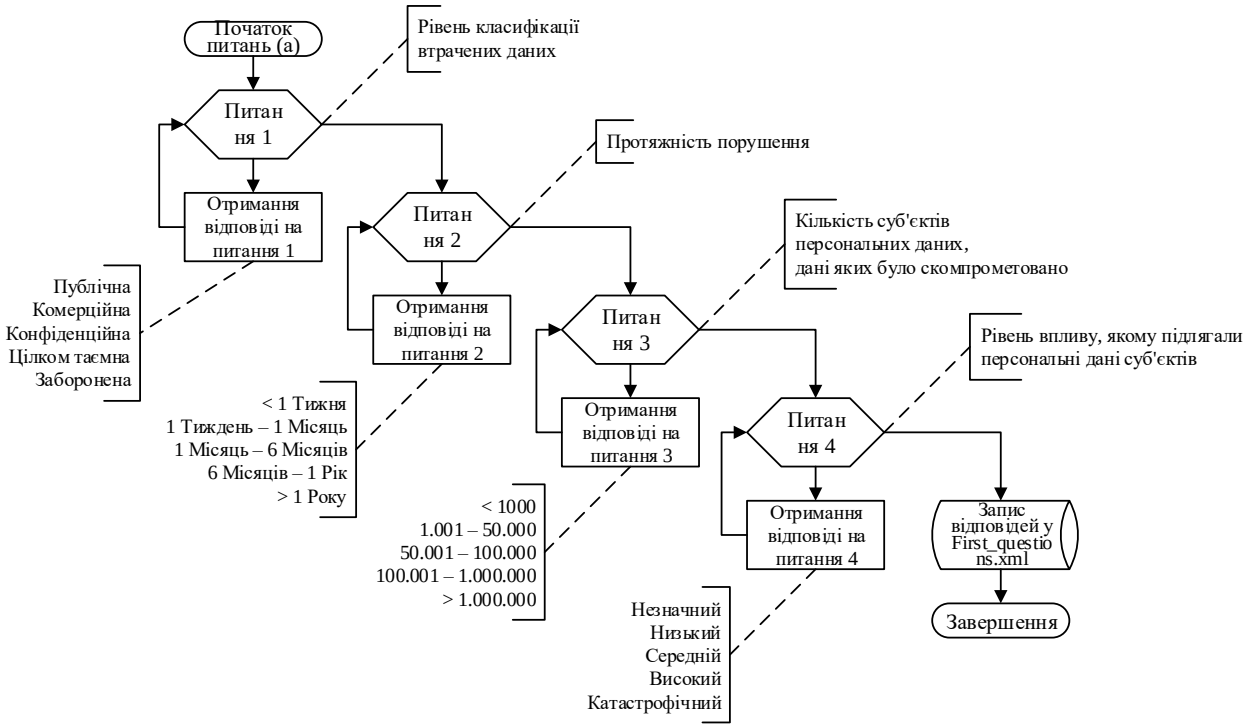


Рис. 4.4. Структура блоку питань розділу (а) у межах підпроцесу «Оцінка вартості штрафу»

Здійснено розробку алгоритмічного забезпечення системи оцінки негативних наслідків втрати персональних даних, що базується на вимогах Регламенту GDPR. Побудовані алгоритми забезпечують формалізовану реалізацію логіки роботи функціональних блоків системи, відповідно до попередньо визначеної структурної моделі. Деталізовано етапи функціонування системи, включаючи ідентифікацію порушення, визначення рівня порушення, оцінку потенційного штрафу на основі набору питань та відповідей, а також формування підсумкового звіту з рекомендаціями.

Створено інтегровану базу даних параметрів інцидентів та оціночних характеристик, яка дозволяє здійснювати збір, обробку, збереження та повторне використання даних для оцінювання шкоди. База даних підтримує ієрархічну структуру оцінювання [108] за напрямами відповідності GDPR, що дозволяє швидко і надійно формувати вхідні дані для експертного аналізу.

Для реалізації програмної системи автоматизованого оцінювання негативних наслідків від порушень у сфері захисту персональних даних

використано мову програмування C#, що є технічно обґрунтованим та доцільним з огляду на функціональні, архітектурні та експлуатаційні вимоги до розробленого рішення. C# забезпечує високу продуктивність і стабільність при реалізації настільних і серверних додатків, що є важливим для створення надійної системи, яка моделює інциденти порушення конфіденційності та виконує складні логічні обчислення для оцінювання штрафних санкцій згідно з положеннями GDPR [109, 110]. Платформа .NET, в рамках якої працює мова C#, пропонує широкий спектр бібліотек і засобів для роботи з файлами, включаючи можливості формування звітів у форматах DOCX та PDF. Це дозволяє легко інтегрувати функціональність генерації документації без необхідності стороннього програмного забезпечення.

C# є об'єктно-орієнтованою мовою з чіткою типізацією, що забезпечує зручність побудови модульної архітектури системи. Це важливо для реалізації незалежних логічних блоків: ідентифікації інциденту, визначення порушених статей GDPR, розрахунку штрафів, генерації рекомендацій тощо. Така структура підвищує масштабованість та спрощує супровід системи. Крім того, завдяки гнучким інтерфейсним можливостям C# (наприклад, за допомогою Windows Forms або WPF), можливо створити зручний та інтуїтивно зрозумілий графічний інтерфейс для користувача, що особливо важливо при розробці системи, призначеної для широкого кола підприємств, які не завжди мають висококваліфікований IT-персонал. Таким чином, вибір C# як мови реалізації дозволяє повною мірою забезпечити виконання усіх функціональних вимог системи – від моделювання сценаріїв витоку до отримання персоналізованих рекомендацій – з дотриманням високих стандартів продуктивності, безпеки та якості коду.

4.5. Експериментальне дослідження системи оцінки негативних наслідків втрати персональних даних

Для проведення експериментального дослідження функціонування розробленої програмної системи оцінювання негативних наслідків витоку персональних даних

використано дані про порушення, зафіксоване у компанії Google (див. п. 4.1).

На першому етапі роботи з програмою після її запуску користувачеві пропонується перейти до розділу «Вибір рівня порушення» (рис. 4.5). У цьому вікні необхідно обрати одну або кілька статей, що були порушені, після чого натискається кнопка «Підтвердження». Обрані параметри автоматично зберігаються у файл для подальшого аналізу. З урахуванням кейсу компанії Google, інтерфейс модуля представлений на рис. 4.6.

Далі користувач переходить до блоку «Ідентифікація підприємства», де вводить базову інформацію про організацію: її назву, ідентифікатор та річний дохід. На основі цих даних система автоматично обчислює потенційний максимальний штраф. Для завершення введення даних необхідно натиснути кнопку «Підтвердження» (рис. 4.7).

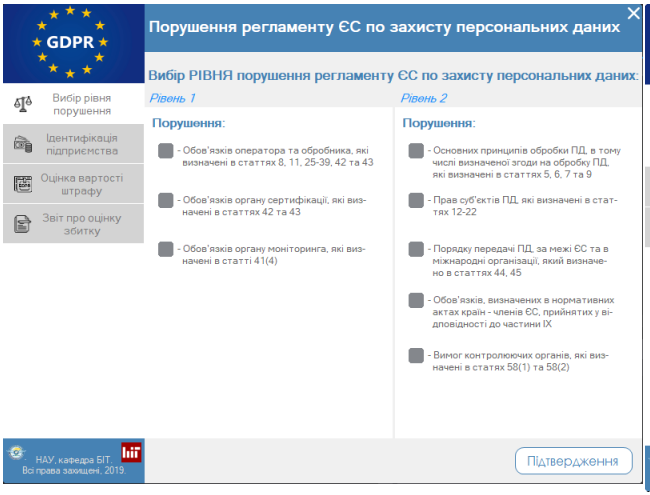


Рис. 4.5. Початкова сторінка системи

Рис. 4.6. Вибір статей порушених компанією

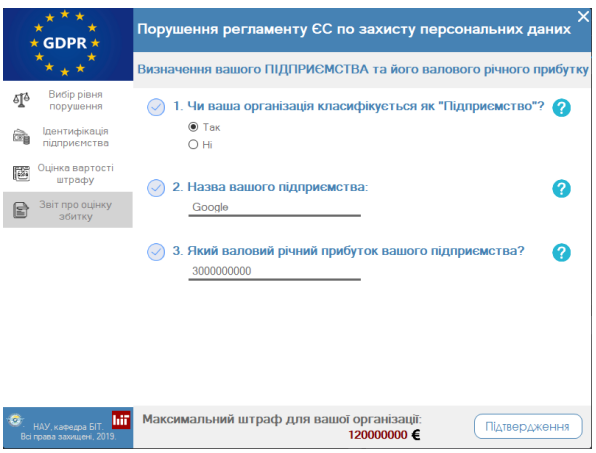


Рис. 4.7. Процес ідентифікації підприємства

Після завершення етапів вибору рівня порушення та внесення інформації про підприємство, користувач переходить до розділу «Оцінка вартості штрафу». На цьому кроці система пропонує відповісти на низку запитань, що деталізують обставини інциденту, з метою коригування суми можливого штрафу. Спершу, у блоці (a), користувач надає відповіді, які відображають обставини, подібні до випадку з компанією Google, і підтверджує введену інформацію за допомогою кнопки «Підтвердження» (рис. 4.8). Далі, у пункті (b), потрібно вказати ступінь залученості керівництва до процесу реагування на інцидент, оцінити рівень дотримання галузевих стандартів, а також підтвердити, чи були вжиті заходи для покращення інформаційної безпеки відповідно до рекомендованих практик. Після заповнення цього блоку користувач знову натискає «Підтвердження» і переходить до наступного пункту (c) (рис. 4.9) [106, 107].

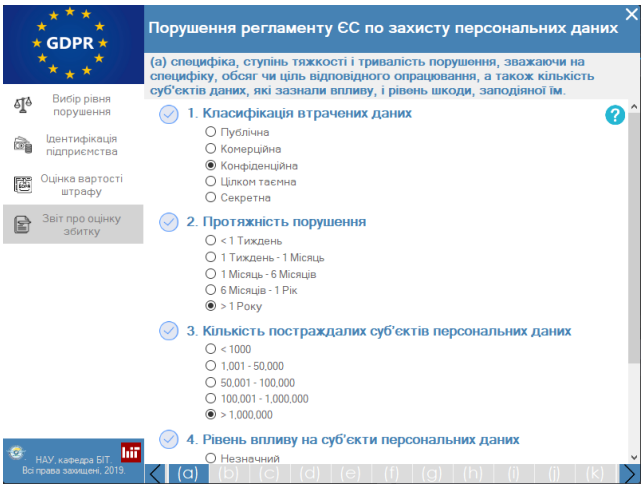


Рис. 4.8. Відповіді на питання

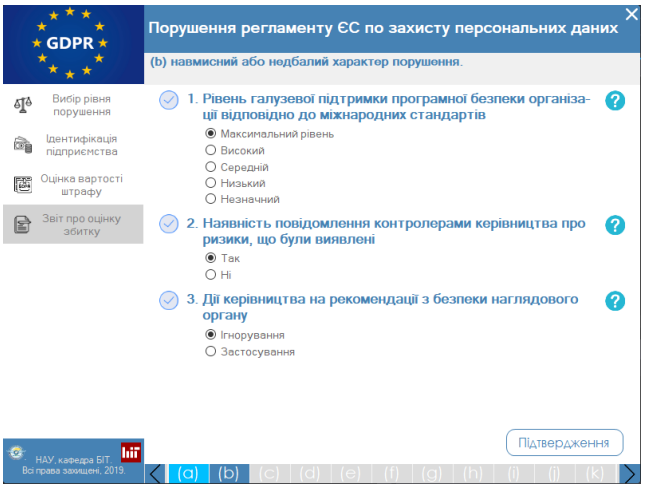


Рис. 4.9. Відповіді на питання

Принцип подальшої роботи програмної системи на Етапі 3 наведено в Додатку А.

Після одержання відповідей на всі одинадцять питань, користувачу відкривається доступ до перегляду звіту. Саме тому, далі натискаємо «Звіт про оцінку збитку», в результаті чого отримуємо детальну оцінку про порушення компанії Google з наближеним штрафом у розмірі 50 млн. €, як і було виставлено наглядовим органом Франції (CNIL) (Рис. 4.10.):

Рис. 4.10. Отриманий звіт із прогнозованою шкодою для компанії

Рис. 4.11. Аналіз результатів опрацювання пункту (a)

Під час аналізу сформованого звіту за пунктом (a) (див. рис. 4.11), можна побачити, що для кожного запитання наведено індивідуальні рекомендації, дотримання яких сприятиме зменшенню ризику повторення подібного інциденту в майбутньому. У звіті також вказано кількість нарахованих балів, а також оцінено фактичні та потенційні збитки, що стосуються цього пункту.

За аналогією побудовано аналітичні звіти і для пунктів від (b) до (k), що дозволяє оцінити кожен з них окремо та своєчасно вжити запобіжних заходів. Усі відповідні матеріали наведені в Додатку А.

З метою зручності користувача передбачено два формати для збереження звітів – DOCX і PDF. Це забезпечує можливість оперативної передачі матеріалів керівництву (з унеможливленням редагування, оскільки інформація представлена у графічному вигляді) і дає змогу швидко підготувати друковану версію документа (рис. 4.12 та 4.13).

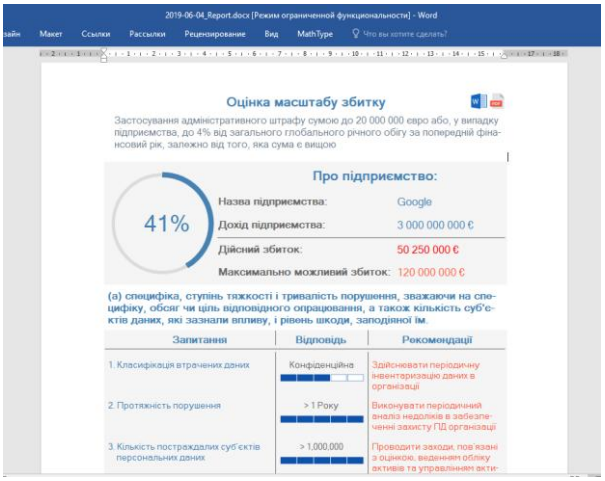


Рис. 4.12. Створення звітного файлу у форматі DOCX

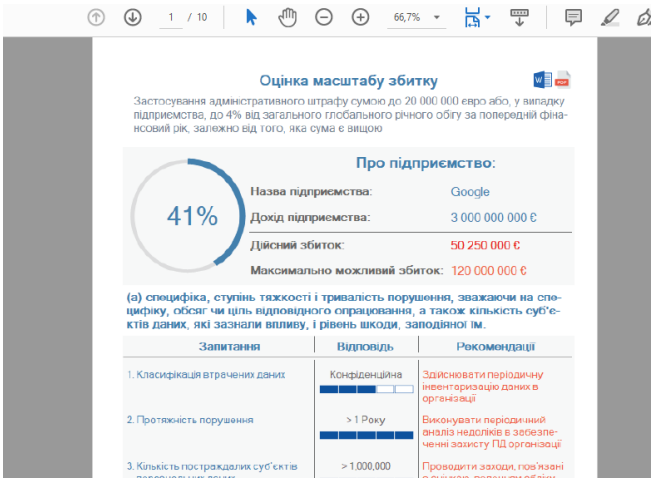
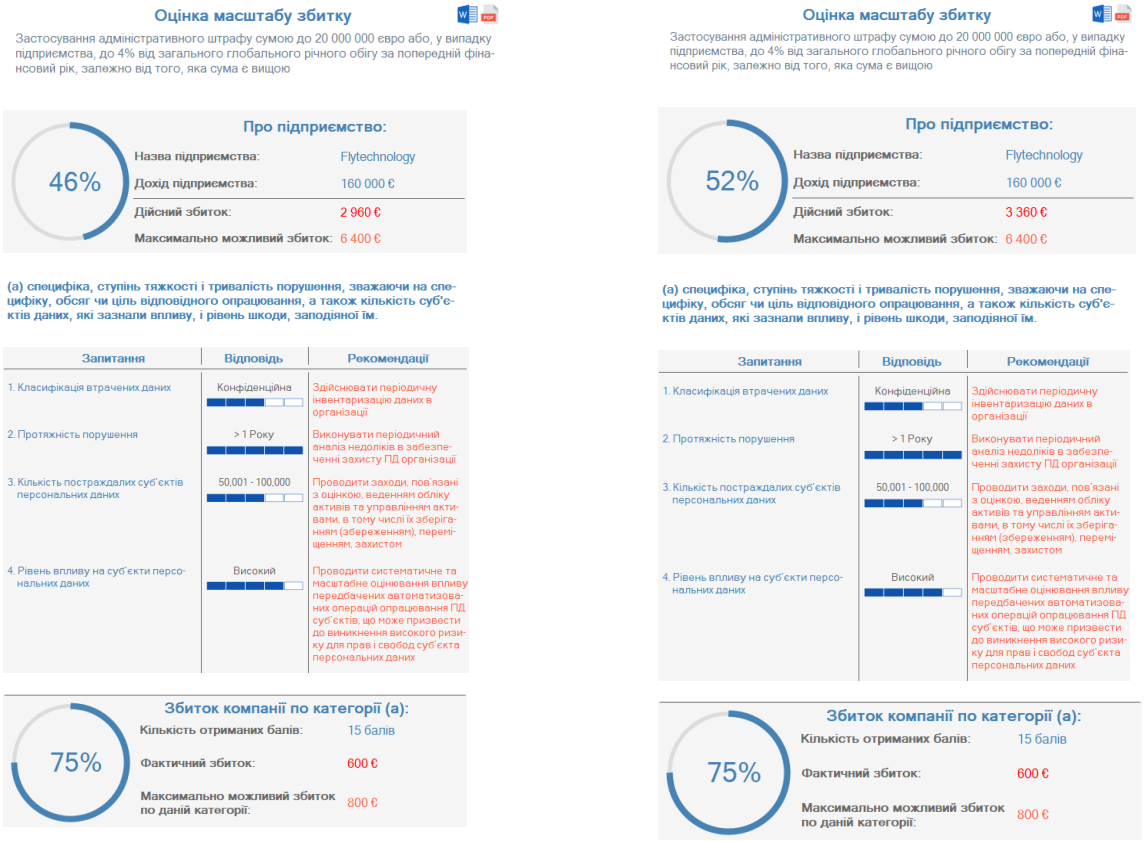


Рис. 4.13. Створення звітного файлу у форматі PDF

Проведена верифікація системи (рис. 4.14) на основі п’яти кейсів показала високу чутливість до зміни вихідних параметрів, що дозволило ідентифікувати критичні зони витоків персональних даних та здійснити оцінку максимального фінансового збитку. В усіх випадках система коректно реагувала на рівень конфіденційності та період зберігання персональних даних. Випадки з вищим рівнем чутливості даних та тривалістю зберігання >1 року генерували суттєво вищі грошові штрафи. Це підтверджує здатність системи інтегрувати ризики згідно положень GDPR.

Дані свідчать, що на фінальний розмір збитків впливає не лише кількість та види документів чи тривалість витоку, а й якісні характеристики – наявність плану реагування, повідомлення наглядового органу, ступінь шкоди, реакція компанії. Наприклад, у кейсах 4 і 5, попри однакові технічні характеристики інциденту, наявність або відсутність повідомлення суттєво змінює підсумковий розмір санкцій. Система дозволяє врахувати, чи витік ініційовано внутрішнім суб'єктом (наприклад, працівником), що автоматично впливає на зростання коефіцієнта ризику. Це робить систему релевантною у ситуаціях, коли необхідна оцінка внутрішніх загроз. Завдяки використанню шкали балів та відповідних грошових еквівалентів, верифікаційна таблиця продемонструвала прогресивне зростання фінансових втрат із нарощуванням кількості інцидентів, їх тяжкості та ігноруванням протоколів безпеки.

а) б) в)



г) д)

Рис. 4.14. Результат верифікації розробленої системи

Отримані результати підтверджують, що розроблена система добре масштабується і може бути реалізована у вигляді автоматизованої системи, надаючи релевантні результати для бізнесу, що відповідає вимогам GDPR щодо прозорості обробки та оцінки наслідків витоків ПД [111-113].

Порівняння власної розробки з уже існуючими методами, моделями та системами є важливим і необхідним кроком для об'єктивної оцінки її ефективності, унікальності та практичної цінності. Такий аналіз дозволяє виявити сильні та слабкі сторони запропонованого рішення, а також визначити його відповідність сучасним вимогам, зокрема вимогам Регламенту GDPR. У підрозділі 1.3 проведено детальний огляд та порівняння існуючих підходів, що слугувало основою для формування критеріїв оцінки та вибору ключових параметрів системи. Це дозволяє не лише підтвердити доцільність розробки нової системи, а й обґрунтувати її переваги над аналогами, що підвищує довіру до результатів дослідження та сприяє більш ефективному впровадженню розробленого рішення на практиці.

Таблиця 4.7.

Порівняльна таблиця оцінювання методів, моделей та систем

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	Репутаційні	Фінансові	Захист персональних даних	Інформаційна/кібербезпека	Спеціалізовані/галузеві	Експертні/опитувальні дані	Структурні/технічні дані
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
FAIR	–	+	–	+	+	+	–	–	+	+	+	–	+	+	–
NIST SP 800-30 / RMF	–	+	–	+	–	+	+	+	-	+	+	+	–	+	+
NIST Privacy Framework / PRAM	+	–	+	+	–	+	+	–	+–	–	–	+	–	–	+
ISO 27005	–	+	–	+	–	+	+	–	–	+	–	+	–	–	+
ISO 31000	–	–	–	+	–	+	+	–	+–	+–	–	+	–	–	+
OWASP Risk Rating	–	+	–	+	+	+	–	–	+	+	–	+	–	+	–

Продовження табл.4.7.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
DPIA (GDPR)	+	+	+	+	–	+	+	–	–	+	–	+	–	–	+
CRAMM	–	+	–	+	–	+	+	–	–	–	–	+	–	–	+
OCTAVE	+–	–	–	+	+	+	+	–	+–	+–	–	+	–	–	+
EBIOS (Risk Manager)	+	+	+	+	+	+	+	–	–	–	–	+	–	–	+
MEHARI	–	+	–	+	–	+	+	–	+–	+–	–	+	–	–	+
Ponemon Cost Model	–	–	–	+	+	+	–	+	+	+	+	–	–	+	–
CyberVaR (CVaR)	–	+	–	+	+	–	–	+	+	+	+	–	–	+	–
Quantitative Assessment of Cybersecurity Risks	+–	–	+	+	+	+	–	+	+	+	+	–	–	+	–
Модель оцінювання наслідків витоку державної таємниці	–	–	–	+	+	–	+	–	+	–	–	+	–	–	+
Модель оцінки параметрів безпеки у соцмережах	+–	–	+	–	+	–	+	–	+	–	–	–	+	+	–
Модель підвищення захищеності ПД у ДН ЗСУ	+–	+	+	+	+	+	+	–	+	–	–	+	+	+	+
Модель розрахунку цінності інформації установи	+–	–	–	+	+	+	+	–	+	+	–	–	+	+	–
Система оцінки негативних наслідків втрати ПД	+	+	+	+	–	+	–	–	+	+	+	+	+	+	+

Розроблена система вирізняється тим, що є спеціалізованою, структурованою і безпосередньо орієнтованою на вимоги Регламенту GDPR, що значно підвищує її практичну цінність для організацій, які обробляють персональні дані в європейському або суміжному правовому полі. Її основна перевага полягає в тому, що вона побудована безпосередньо на положеннях GDPR, який встановлює систему штрафів за порушення правил захисту персональних даних, а отже дозволяє здійснювати кількісну оцінку збитків з урахуванням юридичних наслідків. Це дозволяє здійснювати формалізоване, логічно обґрунтоване обчислення штрафів і рівнів загроз, що не просто імітує загальну оцінку ризику, а дає змогу побачити грошовий еквівалент порушення з урахуванням регуляторної логіки.

Унікальною є також можливість інтегрувати модель у процеси Data Protection Impact Assessment (DPIA), що робить її особливо корисною для

компаній, які впроваджують нові проєкти чи технології. На відміну від більшості моделей, які або абстрактно моделюють загрози, або працюють лише з фінансовими наслідками, ця система дозволяє відображати конкретні ризики через юридично значимі параметри, підвищуючи як точність, так і обґрунтованість рішень.

Крім того, система є кількісною та якісною водночас, тобто поєднує обчислювані метрики (оцінка штрафів у грошовому вираженні) з логічною структурою класифікації порушень. Такий підхід дозволяє не лише оцінити поточний стан захищеності, а й побудувати сценарії розвитку подій, у т.ч. прогнозувати гірший випадок з урахуванням регуляторних санкцій.

Ще однією важливою перевагою є адаптація системи до українського контексту при одночасному збереженні відповідності GDPR. Це робить її особливо ефективною для державних органів, українських компаній з іноземними партнерами або тих, хто надає послуги громадянам ЄС.

Таким чином, розроблена система поєднує:

– пряме юридичне відображення вимог GDPR;

– кількісну оцінку можливих санкцій;

– гнучку параметризацію під конкретні організаційні умови;

– можливість застосування як для аналізу інцидентів, так і для превентивного планування.

4.6. Висновки до розділу 4

У розділі було експериментально підтверджено ефективність запропонованих методів та системи оцінювання наслідків витоку персональних даних. Здійснено апробацію запропонованих математичних методів, алгоритмів і програмного забезпечення у контексті національного законодавства та європейських вимог до захисту ПД – зокрема, Регламенту GDPR.

Проведене експериментальне дослідження методу оцінювання негативних наслідків від порушення конфіденційності персональних даних підтвердило його

здатність точно враховувати як кількісні, так і якісні характеристики інциденту. Метод забезпечує кількісну оцінку штрафних наслідків, адаптовану до вимог GDPR, шляхом аналізу таких чинників, як тип ПД, обсяг впливу, реакція компанії, а також джерело загрози. Дослідження показало, що: наявність або відсутність повідомлення наглядовому органу здатна змінювати підсумкову оцінку збитків у 2–3 рази; метод стабільно реагує на зміну вагомості документів та параметрів захисту; верифікація на реальних сценаріях засвідчила логічне зростання суми санкцій при погіршенні рівня безпеки чи поведінкових реакцій організації. Це дозволяє визнати метод адекватним і чутливим інструментом оцінювання санкцій у разі витоку ПД.

Експериментальне дослідження методу оцінювання безпеки персональних даних, засвідчило, що запропонований метод коректно оцінює ризик витоку персональних даних з урахуванням множини технічних і організаційних параметрів. Метод дозволяє не тільки кількісно інтерпретувати ризик у вигляді балів, а й відповідати грошовим інтервалам збитків. Проведено апробацію на тестових випадках, що охоплювали різні комбінації типів документів, програмного забезпечення для обробки персональних даних, кількості реалізованих механізмів захисту та рівнів загроз, що дозволило зробити наступні висновки: метод демонструє стабільність при зміні вхідних параметрів, у кожному з варіантів простежується логічна послідовність росту ризику в міру зменшення рівня захисту та збільшення вагомості оброблюваних даних; метод коректно визначає інтервали ризику та пов’язані з ними збитки; виявлено критичні порогові значення, що дозволило встановлювати граничні допустимі значення для ризику ПД в АС і формувати вимоги до обов’язкового впровадження КЗІ/ТЗІ.

Результати дослідження підтвердили здатність методу оцінювання рівня критичності у разі витоку персональних даних адекватно оцінювати рівень критичності інцидентів за допомогою чітких і нечітких методів, а також ураховувати кореляційні зв’язки між подіями, що дозволяє уникнути дублювання впливу інцидентів і надмірної оцінки. Введення механізму кореляції дозволяє

отримати об'єктивні оцінки навіть у складних ситуаціях з кількома джерелами загроз. Підтверджено чутливість методу до зміни вхідних параметрів і адекватність при крайових значеннях. Таким чином, запропонований підхід забезпечує точні, логічні й адаптивні результати критичності при мультиінцидентному аналізі.

Розроблене алгоритмічне та програмне забезпечення реалізує усі компоненти структурної моделі системи оцінки негативних наслідків втрати персональних даних відповідно до положень Регламенту GDPR. Це забезпечує формалізоване обчислення максимально наближеного розміру збитків на основі комплексного аналізу факторів інциденту, включаючи рівень порушення, тип персональних даних, контекст події та рівень відповідальності підприємства. Розробка реалізована мовою C#, що забезпечує високий рівень продуктивності та модульність. Створено інтегровану базу даних параметрів інцидентів та оціночних характеристик, яка дозволяє здійснювати збір, обробку, збереження та повторне використання даних для оцінювання шкоди.

Експериментальне дослідження програмної реалізації запропонованої системи на прикладі кейсів, включаючи інцидент з Google, показала її високу ефективність і достовірність результатів. Зокрема: система коректно реагує на критичні вхідні параметри (тривалість зберігання, рівень конфіденційності, джерело витоку); встановлено пряму залежність між якісними характеристиками порушення (план реагування, повідомлення органу) та величиною збитків; при моделюванні відсутності реагування або коли загроза походила від внутрішнього суб’єкта, грошові штрафи були суттєво вищими. Результати системи узгоджуються з фактичними значеннями штрафів, що було накладено контролюючими органами ЄС, що свідчить про її відповідність практичним регуляторним підходам. Таким чином, система не лише формалізує оцінку, а й підтримує прийняття рішень, автоматизуючи складні логічні зв’язки між характеристиками інциденту, джерелами загроз, діями компанії та очікуваними фінансовими наслідками.

Проведене порівняння розробленої системи з існуючими методами, моделями та системами оцінювання негативних наслідків втрати персональних даних дозволяє зробити висновок, що розроблена система вигідно вирізняється серед типових міжнародних підходів (FAIR, NIST, OWASP, MEHARI тощо) за такими ключовими критеріями: повна відповідність GDPR; наявність реалізації у вигляді ПЗ; підтримка як експертних, так і структурно-фактичних джерел даних; одночасне врахування фінансових, репутаційних та організаційних втрат; універсальність для оцінки в державному, корпоративному та галузевому середовищі. Ці ознаки засвідчують унікальність і вищу практичну придатність системи у порівнянні з наявними засобами, що часто або орієнтовані лише на кіберризики, або не мають повноцінної реалізації у вигляді адаптивного інструменту.

ВИСНОВКИ

Результатом виконаної роботи є вирішення важливої науково-прикладної проблеми, пов’язаної з розробкою методів і моделей оцінки негативних наслідків від витоку персональних даних, яка обумовлена зростанням кіберзагроз, посиленням регуляторних вимог (зокрема Регламенту GDPR), а також необхідністю забезпечення ефективного управління інформаційною безпекою і мінімізації фінансових втрат організацій.

У процесі виконання дисертаційної роботи отримані наступні результати:

1. Проведено комплексний аналіз вітчизняних та міжнародних моделей, методів та систем у сфері захисту персональних даних, їх відповідність нормативно-правовій базі України та ЄС (зокрема, GDPR), що дозволило сформулювати вимоги до створення нових 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.

2. Розроблено теоретико-множинну та кортежну моделі параметрів персональних даних, що дозволило відповідно формалізувати і моделювати вплив кожного із параметрів, що впливають на оцінювання збитку від втрати персональних даних відповідно до Регламенту GDPR та визначити множини вхідних та вихідних параметрів для формалізації процесу оцінювання ризику втрати персональних даних з урахуванням національного нормативно-правового забезпечення, які в подальшому будуть використані для розробки відповідних методів оцінювання безпеки персональних даних на основі кортежної моделі відповідно до вимог українського законодавства та механізмів розрахунку негативних наслідків на основі теоретико-множинної GDPR-моделі параметрів персональних даних.

3. Розроблено метод оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR

та метод оцінювання безпеки персональних даних, що дозволило відповідно визначати величину максимального та фактичного збитків для організації у разі порушення конфіденційності персональних даних і надавати рекомендації щодо вибору політики їх безпеки відповідно до вимог Регламенту GDPR та надавати рекомендації щодо вибору політики безпеки персональних даних і послуг безпеки відповідно до функціонального профілю захищеності та визначати величину можливої шкоди у разі втрати таких персональних даних з урахуванням національного нормативно-правового забезпечення.

4. Розроблено структурну модель системи оцінювання негативних наслідків від витоку персональних даних, яка за рахунок використання методу оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR та 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.

5. Розроблено алгоритмічне забезпечення, яке реалізує структурну модель системи оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR. Це забезпечує формалізоване обчислення максимально наближеного розміру збитків на основі комплексного аналізу чинників інциденту, включаючи рівень порушення, тип персональних даних, контекст події та рівень відповідальності підприємства. Створено інтегровану базу даних параметрів інцидентів та оціночних характеристик, яка дозволяє здійснювати збір, обробку, збереження та повторне використання даних для оцінювання шкоди. База даних підтримує ієрархічну структуру оцінювання за напрямами відповідності GDPR, що дозволяє швидко і надійно формувати вхідні дані для експертного аналізу. Проведено експериментальне дослідження для перевірки адекватності розроблених підходів.

Отримані результати підтвердили, що розроблена система надає релевантні результати, що відповідають вимогам GDPR щодо прозорості обробки та оцінки наслідків витоків персональних даних. Проведені дослідження підтвердили достовірність теоретичних положень та практичних розробок дисертаційного дослідження, а також впровадження і успішне практичне використання зазначених розробок підтвердили достовірність теоретичних гіпотез і висновків дисертаційної роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шаховал О., Лозова І., Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. *Захист інформації*. 2016. Т. 18, № 1. С. 57–65. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_1_9

2. 10 найпотужніших кібератак та витоків даних за всю історію. GigaTrans - Інтернет для Вашого офісу. URL: https://gigatrans.ua/ua/news/10-naypotuzhn-shih-k-beratak-ta-vitok-v-danih-za-vsyu-stor-yu?utm_source

3. New ransomware, old techniques: Petya adds worm capabilities | Microsoft Security Blog. Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc

4. Солонина Є. Злив персональних даних українців: що сталося і як захиститися. Радіо Свобода. URL: https://www.radiosvoboda.org/a/zlyv-danyx-i-diya/30610626.html

5. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. Analysis of modern cloud services to ensure cybersecurity. *6th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES* 2022, Vol. 207, pp. 110 - 117. (*Scopus*). URL: https://doi.org/10.1016/j.procs.2022.09.043

6. Гізун А., Лозова І. Аналіз дефініцій поняття кризова ситуація та основних аспектів концепції управління безперервністю бізнесу. *Безпека інформації*. 2016. Т. 22, № 1. С. 99-108. URL: http://nbuv.gov.ua/UJRN/bezin_2016_22_1_17.

7. Різак М. В. Правове регулювання відносин щодо персональних даних в Україні : монографія. Харків: Панов, 2016. 464 с.

8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

9. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

10. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

11. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент Європ. Союзу від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

12. 7eminar. Штрафи, заборони, права: які зміни несе новий закон про персональні дані. 7eminar. URL: https://7eminar.ua/news/7121-strafi-zaboroni-prava-yaki-zmini-nese-novii-zakon-pro-personalni

13. Аналіз законодавства про захист персональних даних України. Звіт. / підгот. АС “Саєнко Харенко” / Міністерство Цифрової Трансформації України. URL: http://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_ Finalnyy-zvit.pdf.

14. Правовий механізм захисту персональних даних: монографія / В. Брижко ; за ред. М. Швеця та Р. Калюжного. К. : Парлам. вид-во, 2003. 120 с.

15. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI: станом на 8 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

16. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.

17. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII: станом на 18 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

18. Олександр Шевчук. Відповідальність і санкції за порушення загального регламенту про захист даних (GDPR). URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/gdprvidpovidalnist-i-sanktsii-3.pdf

19. Волосецький В.О. Іноземний досвід правового регулювання захисту персональних даних. Міжнародний науковий журнал. URL: https://www.internauka.com/uploads/public/14815322304340.pdf.

20. Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних комунікацій (Директива про право на недоторканість особистого життя та комунікації) електронні засоби зв'язку) : Директива Європ. Союзу від 12.07.2002 № 2002/58/ЄС: станом на 25 листоп. 2009 р. URL: https://zakon.rada.gov.ua/laws/show/994_b34#Text

21. Directive - 2016/680 - EN - Law Enforcement Directive; LED - EUR-Lex. EUR-Lex – Access to European Union law – choose your language. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

22. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 432 с. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

23. Overview of The Privacy Act of 1974 (2020 Edition). Department of Justice | Homepage | United States Department of Justice. URL: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

24. Health Insurance Portability and Accountability Act of 1996. ASPE. URL: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

25. Children's Online Privacy Protection Rule ("COPPA"). Federal Trade Commission. URL: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

26. Personal Information Protection and Electronic Documents Act. Justice Laws Website - Site Web de la lÃ©gislation (Justice). URL: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

27. The Privacy Act - Office of the Privacy Commissioner of Canada. Commissariat à la protection de la vie privée du Canada / Office of the Privacy Commissioner. URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/

28. V. Hrebenuik , Y. Dreis, A. Hrebenuik, I. Lozova. Definitions in the field of personal data protection: a comparative analysis of the legislation of Ukraine and European Union. Technologie, procesy i systemy produkcyjne: Monografia. Tom3. Akademia Techniczno Humanistyczna w Bielsku-Bialej, 2020. pp. 141 - 146. URL: https://engineerxxi.ubb.edu.pl/fcp/eHFNIBD8dJBYXMwoXQH5hbEpmfHIGFBcNBi4oGgh0VWFeUxRUPBYvEkFWQQMOZm96Dzc1IikcFEpjZXQLC3QZ/_users/code_0DQNBBTkZMh4KLBYRAGomPA9qIDw/publikacje/2020/engineerxxi_2020_vol3_13.pdf

29. Брижко В.М., Радянська А.І., Швець М.Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. К.: Тріумф, 2006. 256 с.

30. Людмила Присяжна. Рада схвалила законопроєкт про захист персональних даних | Think brave. Think brave | Останні новини бізнесу України. URL: https://biz.ligazakon.net/news/232077_rada-skhvalila-zakonoprokt-pro-zakhist-personalnikh-danikh

31. Проект Закону України від 25.10.2022 р. N 8153 «Про захист персональних даних». URL: https://ips.ligazakon.net/document/view/JI08275I?an=1

32. Гуржій Т. О. Петрицький. А. Л. Правовий захист персональних даних: монографія. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.

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

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

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

36. NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

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

38. 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.

39. 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.

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

41. 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

42. 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

43. 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

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

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

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

47. «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.

48. 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

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

50. 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%20ransomware%20to%20insider%20attacks

51. 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

52. 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

53. 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

54. 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

55. 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

56. 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

57. 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.

58. Корченко О., Дрейс Ю., Лозова І., Педченко Є. Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*. 2020. Т. 22, № 2. С. 120-141. URL: https://doi.org/10.18372/2410-7840.22.14871

59. Y. Dreis, I. Lozova, A. Biskupskyi, Y. Pedchenko, Y. Ivanchenko. GDPR-model of parameters for estimating losses from loss of personal data. Przetwarzanie, transmisja i bezpieczeństwo informacji: Monografia. Tom 2. Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2019. pp. 127 - 138. URL: https://www.researchgate.net/profile/Yurii-Dreis-2/publication/387069634_GDPR-MODEL_OF_PARAMETERS_FOR_ESTIMATING_LOSSES_FROM_LOSS_OF_PERSONAL_DATA_MODEL_PARAMETROW_GDPR_DO_SZACOWANIA_STRAT_Z_UTRATY_DANYCH_OSOBOWYCH/links/675edfb7da24c8537c76497f/GDPR-MODEL-OF-PARAMETERS-FOR-ESTIMATING-LOSSES-FROM-LOSS-OF-PERSONAL-DATA-MODEL-PARAMETROW-GDPR-DO-SZACOWANIA-STRAT-Z-UTRATY-DANYCH-OSOBOWYCH.pdf

60. Дрейс Ю.О., Лозова І.Л., Ковальов Д.А. Структурно-параметрична GDPR-модель оцінки негативних наслідків від витоку персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали VI міжнарод. наук.-практ. конф., 19 – 22 лютого 2020 р. Київ: Вид-во Європейського університету, 2020. – С. 39-41. URL: https://www.researchgate.net/publication/389811894_STRUKTURNO-PARAMETRICNA_GDPR-MODEL_OCINKI_NEGATIVNIH_NASLIDKIV_VID_VITOKU_PERSONALNIH_DANIH

61. Дрейс Ю.О., Лозова І.Л. Розробка GDPR-моделі параметрів оцінювання наслідків витоку персональних даних. *Комп'ютерні технології: інновації, проблеми, рішення*: Матеріали II Всеукраїнської науково-технічної конференції, м. Житомир, 14-15 листопада 2019 р. Житомир, Житомирська політехніка, 2019. С. 78-79. URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/tezy-dopovidej-kt2019_os.pdf

62. Лозова І., Педченко Є., Баланда А. Теоретико-множинне представлення параметру «Рівень порушення» для кортежної GDPR-моделі, *ITSec-2020: Безпека інформаційних технологій*: Матеріали X міжнар. наук.-техніч. конф., м. Київ, 19-24 березня 2020 року. Київ, 2020. С. 47-49.

63. Лозова І. Теоретико-множинне представлення окремих параметрів для кортежної GDPR-моделі. *Безпека ресурсів інформаційних систем*: збірник тез І Міжнародної науково-практичної конференції, м. Чернігів, 16-17 квітня 2020 р., Чернігів: НУЧП, 2020. С. 110-116. URL: https://stu.cn.ua/wp-content/uploads/2021/04/bris-t.pdf

64. Дрейс Ю., Скворцов С., Лозова І., Біскупський А. Множинна інтерпретація параметрів «Зниження шкоди» та «Ступінь відповідальності» для кортежної GDPR-моделі. *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2020)*: Матеріали 12-ої Всеукр. науково-практ. конф., м. Миколаїв, 24-26 черв. 2020 р. Миколаїв, 2020. С. 21-24. URL: https://www.researchgate.net/publication/389848384_MNOZINNA_INTERPR

ETACIA_PARAMETRIV_ZNIZENNA_SKODI_TA_STUPIN_VIDPOVIDALNOSTI_DLA_KORTEZNOI_GDPR-MODELI

65. The Penetration Testing Execution Standard Documentation / The PTES Team, 2017, 229 p. URL: https://buildmedia.readthedocs.org/ media/pdf/pentest-standard/latest/pentest-standard.pdf

66. ISO/IEC 31010:2009 Risk Management. Risk assessment techniques. Geneva: 2009, №1, 176 p.

67. Про затвердження документів у сфері захисту персональних даних / Уповноважений ВР з прав людини; Наказ, Порядок, Форма типового документа [...] від 08.01.2014 р. №1/02-14/ URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

68. Корченко О., Дрейс Ю., Лозова І. Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. *Захист інформації*. 2016. Т. 18, № 1. С. 39-47. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_1_7

69. Дрейс Ю.О., Лозова І.Л. Формування параметрів оцінювання негативних наслідків витоку персональних даних в автоматизованих системах. *ITSec: Безпека інформаційних технологій*: Матеріали VIII міжнародної науково-технічної конференції, м.Київ,16-18 травня 2018 р. Київ, 2018. С.14-15.

70. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університ*у. 2013. Вип. 6-3 (1). С. 90–94.

71. Роз'яснення до Типового порядку обробки персональних даних Уповноважений ВР з прав людини від 08.01.2014. URL: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text

72. Обуховська Т. І. Класифікація персональних даних та режиму доступу до них. *Вісник Національної академії державного управління*. 2013. № 1. С. 97–104.

73. Кардаш А. В. Інформація про особу та персональні дані: окремі аспекти співвідношення. *Форум права*: електрон. наук. фахове вид. 2017. № 4. С. 87–92. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_4_15.pdf

74. Корченко О.Г., Архипов О.Є., Дрейс Ю.О. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія. К.: Наук.-вид. центр НА СБ України, 2014. 332 с. ISBN 978-617-7092-26-0

75. Дрейс Ю.О. Базові параметри представлення ризику захисту персональних даних в державних АС. *Інформаційна безпека держави, суспільства та особистості*: Збірник тез доповідей всеукраїнської науково-практичної конференції, 16 квітня 2015 р., м. Кіровоград: КНТУ, 2015. С.118.

76. Дрейс Ю.О. Заходи захисту персональних даних в інформаційних (автоматизованих) системах. *Перспективні напрями захисту інформації*: Матеріали І всеукраїнської науково-практичної конференції, 7-9 вересня 2015 р. Одеса: ОНАЗ ім. О.С. Попова, 2015. С.29-32.

77. Корченко А., Козачок В., Гізун А. Метод оцінки рівня критичності для систем управління кризовими ситуаціями. *Захист інформації*, 2015, Т.17, №1, С. 86-98.

78. Карпінський М., Корченко А., Гізун А. Метод виявлення інцидентів/потенційних кризових ситуацій. *Захист інформації,* 2015, Т.17, №2, С.124-130.

79. Карпінський М., Корченко А., Гізун А. Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, 2015. №.1 (29), С. 76-85.

80. Гізун А., Лозова І., Трикуш О. Застосування механізму кореляції інцидентів/потенційних кризових ситуацій для оцінювання рівня критичності поточної ситуації в інформаційній сфері. *Безпека інформації*. 2017. Т. 23, № 3. С. 215-221. URL: http://nbuv.gov.ua/UJRN/bezin_2017_23_3_10

81. Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л., Педченко Є.М. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Захист інформації.* 2023. Т. 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232.

82. Pedchenko Y., Karpinski M., Lozova I., Kotyk O., Petrovska M. Damage assessment from the personal data loss. Problems of scientific, technical and legal support for cybersecurity in the modern world : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 34-46. DOI: 10.24917/9788668020861 URL: https://bazawiedzy.uken.krakow.pl/info/article/UKENca47634692fd430697964f5fa8af695f/

83. Лозова І.Л., Корченко О.Г., Котик О.В. Оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали X Міжнарод. наук.-практ. конф., Київ, 25 квітня 2024 р. / Редкол.: О. І. Тимошенко та ін. Київ: Вид-во Європейського університету, 2024. С. 74-78. URL: https://e-u.edu.ua/userfiles/files/135/2024-zbirnik_h_mizhnarodna-_konf_aktualni_pitannya_zabezpechennya_kiberbezpeki_ta_zahistu_informacii.pdf

84. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., Balagura, D. Development of the sociocyberphysical systems` multi-contour security methodology. *Eastern-European Journal of Enterprise Technologies*. 2024. Vol. 1, no. 9 (127). P. 34–51. (*Scopus*) URL: https://doi.org/10.15587/1729-4061.2024.298844

85. Yevseiev, S., Dzheniuk, N., Tolkachov, M., Milov, O., Voitko, T., Prygara, M. et al. Development of a multi-loop security system of information interactions in socio-cyberphysical systems. *Eastern-European Journal of Enterprise Technologies*, 2023, 5 (9 (125)), P.53–74. https://doi.org/10.15587/1729-4061.2023.289467

86. Dzheniuk, N., Yevseiev, S., Lazurenko, B., Serkov, O., Kasilov, O. A method of protecting information in cyber-physical space. *Advanced Information Systems*, 2023, 7 (4), P.80–85. https://doi.org/10.20998/2522-9052.2023.4.11

87. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. Development of the automated decision-making system synthesis method in the management of information security channels. *Eastern-European Journal of Enterprise Technologies*, 2023, 6 (9 (126)), P. 39–49. https://doi.org/10.15587/1729-4061.2023.293511

88. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. https://doi.org/10.15587/978-617-7319-31-2

89. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. https://doi.org/10.15587/978-617-7319-57-2

90. Yevseiev, S., Hryhorii, K., Liekariev, Y. Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies*, 2016, 6 (4 (84)), P. 11–23. https://doi.org/10.15587/1729-4061.2016.86175

91. Yevseiev, S., Korol, O., Kots, H. Construction of hybrid security systems based on the crypto-code structures and flawed codes. *Eastern-European Journal of Enterprise Technologies*, 2017, 4 (9 (88)), P. 4–21. https://doi.org/10.15587/1729-4061.2017.108461

92. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et al. Practical implementation of the Niederreiter modified crypto code system on truncated elliptic codes. *Eastern-European Journal of Enterprise Technologies*, 2018, 6 (4 (96)), P. 24–31. https://doi.org/10.15587/1729-4061.2018.150903

93. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et al. Development of Niederreiter hybrid crypto-code structure on

flawed codes. *Eastern-European Journal of Enterprise Technologies*, 2019, 1 (9 (97)), P. 27–38. https://doi.org/10.15587/1729-4061.2019.156620

94. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S. et al. Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. *Eastern-European Journal of Enterprise Technologies*, 2021, 1 (2 (109)), P.14–23. https://doi.org/10.15587/1729-4061.2021.225346

95. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. *Eastern-European Journal of Enterprise Technologies*, 2021, 2 (9 (110)), P. 6–15. https://doi.org/10.15587/1729-4061.2021.229221

96. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, 3021, 3 (9 (111)), P. 63–83. https://doi.org/10.15587/1729-4061.2021.233533

97. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., Manzhul, I. Modeling the protection of personal data from trust and the amount of information on social networks. *EUREKA: Physics and Engineering*, 2021 1, P. 24–31. https://doi.org/10.21303/2461-4262.2021.001615

98. Cybersecurity classifier. Available at: https://skl.sspu.sumy.ua/

99. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H. et al. Development of an improved SSL/TLS protocol using post-quantum algorithms. *Eastern-European Journal of Enterprise Technologies*, 2023, 3 (9 (123)), P. 33–48. https://doi.org/10.15587/1729-4061.2023.281795

100. Milevsky, S. Development of threat classifier in socio-cyber-physical systems. *Ukrainian Scientific Journal of Information Security*, 2023, 29 (3). https://doi.org/10.18372/2225-5036.29.18070

101. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I. et al. Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. *Eastern-European Journal of Enterprise Technologies*, 2021, 5 (9 (113)), P. 30–47. https://doi.org/10.15587/1729-4061.2021.241638

102. Ranjitha, C. R., Thomas, J., Chithra, K. R. A brief study on LDPC codes. *International Journal of Engineering Research and General Science*, 2016, 4, (2), P. 612–618. Available at: http://pnrsolution.org/Datacenter/Vol4/Issue2/85.pdf

103. Корченко О.Г., Лозова І.Л. Структурна модель системи оцінки негативних наслідків втрати персональних даних. *Наукові записки ДУІКТ*. 2024. №2 (6). С. 165-170. URL: https://doi.org/10.31673/2786-8362.2024.028264

104. Лозова І., Корченко О. Розробка моделі системи оцінки негативних наслідків втрати персональних даних. *ITSec: Безпека інформаційних технологій*: Матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С.124-125. URL: https://drive.google.com/file/d/1Nt2w9E-N97TAIdAGqWKbaXsqASyP-4tt/view

105. Корченко О.Г., Лозова І.Л., Дрейс Ю.О., Хохлачова Ю.Є. Алгоритмічне забезпечення системи оцінки негативних наслідків від втрати персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали VII міжнарод. наук.-практ. конф., 24-27 лютого 2021 р. Київ: Вид-во Європейського університету, 2021. С.40-42. URL: https://www.researchgate.net/publication/389848654_ALGORITMICNE_ZABEZPECENNA_SISTEMI_OCINKI_NEGATIVNIH_NASLIDKIV_VID_VTRATI_PERSONALNIH_DANIH

106. Комп'ютерна програма «Програмний модуль оцінки негативних наслідків від витоку персональних даних»: а. с. 96927 Україна/ Ю. Дрейс., І. Лозова, Є. Педченко. Заявл. 27.03.2020 ; опубл. 29.05.2020, Бюл. № 58. URL: https://sis.nipo.gov.ua/uk/search/detail/1625864/

107. Дрейс Ю.О., Лозова І.Л., Педченко Є.М. Оцінювання негативних наслідків від витоку персональних даних. ITSec: Безпека інформаційних

технологій: Матеріали IX міжнародної науково-технічної конференції, м. Київ, 22-27 березня 2019 р. Київ, 2019. С.41-42.

108. Gnatyuk, S., Berdibayev, R., Azarov, I., Baisholan, N., Lozova I. Modern Types of Databases for SIEM System Development. *CEUR Workshop Proceedings*, 2021, 3187, pp. 127-138. (*Scopus*). URL: https://ceur-ws.org/Vol-3187/paper12.pdf

109. C# Guide - .NET managed language. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/dotnet/csharp/

110. Learn C# (C Sharp) | Codecademy. Codecademy. URL: https://www.codecademy.com/learn/learn-c-sharp

111. Яворська І.М., Стахура С.А. Штрафні санкції, як основна форма відповідальності за порушення Загального Регламенту захисту персональних даних в ЄС. Том 2 № 80 (2023): Науковий вісник Ужгородського національного університету. Серія: Право. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/59040/1/297104-Текст%20статті-685651-1-10-20240120.pdf

112. Духовна О. Вчимося на помилках: найбільші штрафи за порушення норм GDPR. Юридична газета online. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vchimosya-na-pomilkah-naybilshi-shtrafi-za-porushennya-norm-gdpr.html

113. Найбільші штрафи за порушення GDPR в 2023 році. URL: https://bsoprivacygroup.com/naibilshi-shtrafy-za-porushennia-gdpr-v-2023-rotsi/

ДОДАТОК А

Експериментальне дослідження функціонування розробленої програмної системи оцінювання негативних наслідків витоку персональних даних

У блоці питань розділу (c) користувач повинен зазначити дії, які були здійснені відповідальною особою для зменшення негативних наслідків інциденту, що зачепив персональні дані суб'єктів. Після вибору відповідей потрібно натиснути кнопку «Підтвердження» та перейти до наступного блоку — пункту (d) (див. Рис. А.1).

Під час заповнення пункту (d) користувач оцінює рівень відповідальності відповідальної особи згідно з наявними технічними та організаційними заходами, впровадженими на підприємстві. Після цього слід підтвердити введені дані та перейти до пункту (e) (Рис. А.2).

У пункті (e) потрібно вказати, чи є даний інцидент першим на підприємстві, чи подібні випадки вже траплялися. Натиснувши «Підтвердження», користувач переходить до розділу (f) (Рис. А.3).

На етапі заповнення пункту (f) користувач обирає рівень взаємодії компанії з відповідним наглядовим органом країни-члена ЄС, де було зафіксовано порушення. Після підтвердження, система переходить до пункту (g) (Рис. А.4).

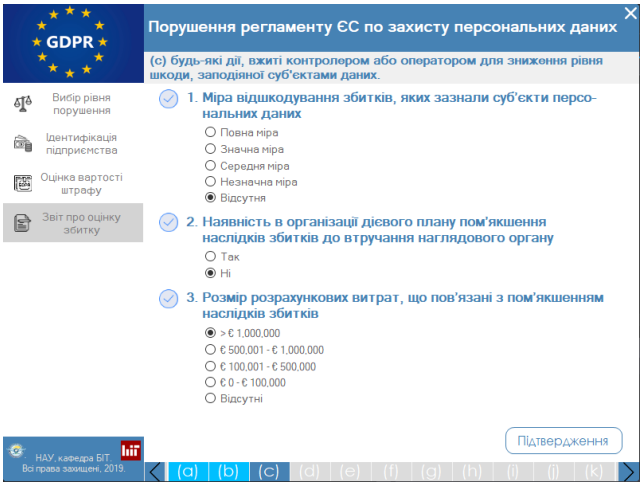


Рис. А.1. Оцінка параметрів пункту (c) на основі порушення компанії

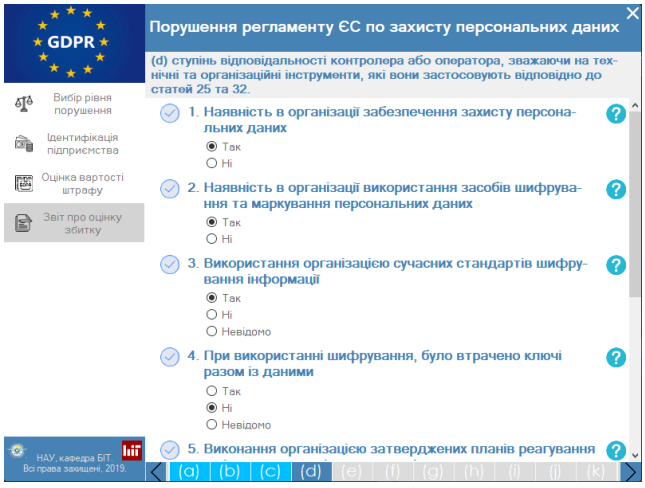


Рис. А.2. Оцінка параметрів пункту (d) на основі порушення компанії

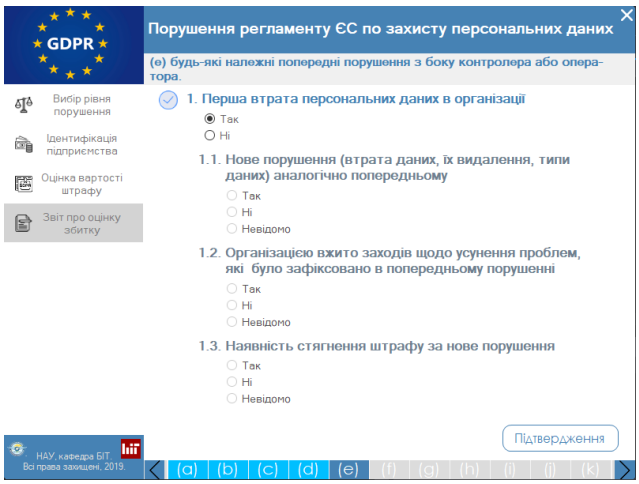


Рис. А.3. Оцінка параметрів пункту (e) на основі порушення компанії

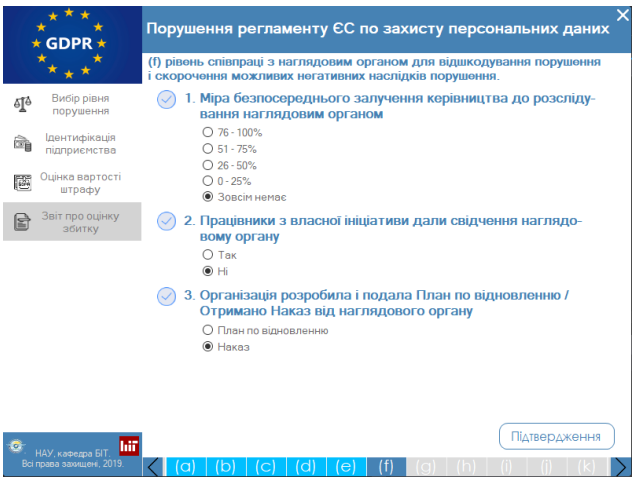


Рис. А.4. Оцінка параметрів пункту (f) на основі порушення компанії

У процесі заповнення блоку питань розділу (g) користувач має вказати типи персональних даних, які постраждали внаслідок інциденту. Після внесення відповідної інформації потрібно натиснути кнопку «Підтвердження», щоб перейти до наступного розділу (h) (див. Рис. А.5).

На етапі відповіді на питання пункту (h) користувачу слід зазначити, ким саме було проінформовано наглядовий орган про факт порушення, а також упродовж якого часу це було здійснено. Після введення даних натискається кнопка «Підтвердження», яка забезпечує перехід до блоку (i) (Рис. А.6).

Рис. А.5. Оцінка параметрів пункту (g) на основі порушення компанії

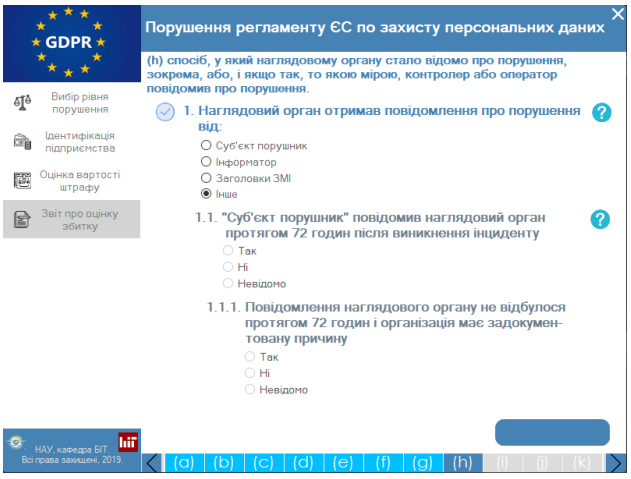


Рис. А.6. Оцінка параметрів пункту (h) на основі порушення компанії

Під час відповіді на запитання блоку (i), уповноважений співробітник має вказати, чи були реалізовані заходи впливу, передбачені статтею 58(2) Регламенту GDPR. Після надання відповіді слід натиснути кнопку «Підтвердження» для переходу до наступного пункту (j) (див. Рис. А.7).

У межах пункту (j) користувачеві необхідно зазначити, чи існує можливість проходження сертифікації даних у державі, на території якої стався інцидент. Після цього потрібно натиснути кнопку «Підтвердження» для продовження роботи з останнім блоком питань — пунктом (k) (Рис. А.8).

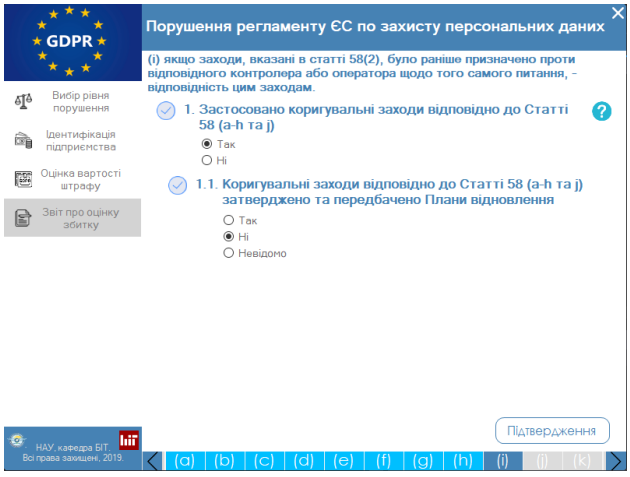


Рис. А.7. Оцінка параметрів пункту (i) на основі порушення компанії

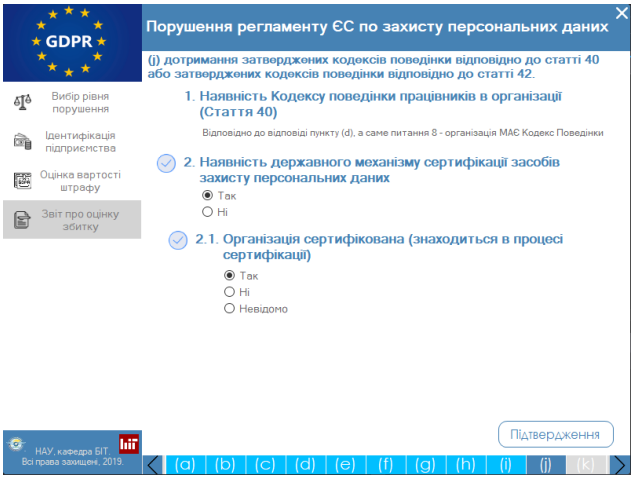


Рис. А.8. Оцінка параметрів пункту (j) на основі порушення компанії

На фінальному етапі, під час опрацювання пункту (k), уповноважений працівник має зазначити, чи мала місце фінансова вигода або збитки внаслідок витоку персональних даних. У разі стверджувальної відповіді необхідно вказати конкретний розмір відповідних сум. Завершивши внесення відповідей, слід натиснути кнопку «Підтвердження», після чого перейти до формування звіту, натиснувши на головному екрані опцію «Звіт про оцінку збитку» (див. Рис. А.9).

Рис. А.9. Оцінка параметрів пункту (k) на основі порушення компанії

Результати опрацюванням даних:

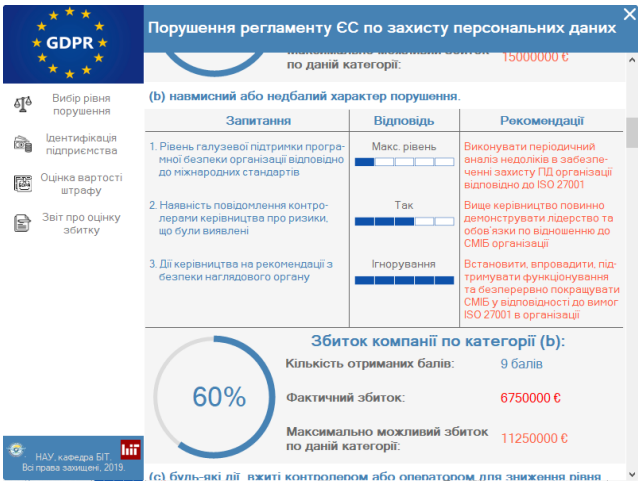


Рис. А.10. Аналіз результатів опрацювання пункту (b)

Рис. А.11. Аналіз результатів опрацювання пункту (c)

Рис. А.12 Аналіз результатів опрацювання пункту (d)

Рис. А.13. Аналіз результатів опрацювання пункту (d) (продовження)

Рис. А.14 Аналіз результатів опрацювання пункту (e)

Рис. А.15. Аналіз результатів опрацювання пункту (f)

Рис. А.16. Аналіз результатів опрацювання пункту (g)

Рис. А.17. Аналіз результатів опрацювання пункту (h)

Рис. А.18. Аналіз результатів опрацювання пункту (i)

Рис. А.19. Аналіз результатів опрацювання пункту (j)

Рис. А.20. Аналіз результатів опрацювання пункту (k)

ДОДАТОК Б

Фрагмент лістингу програми

```
using System;
using System.Collections.Generic;
using System.Drawing;
using System.Data;
using System.Windows.Forms;
using System.Drawing.Imaging;
using System.IO;
using iTextSharp.text;
using iTextSharp.text.pdf;
using Xceed.Words.NET;

namespace GDPR_fines.Report
{
   public partial class Report : UserControl
   {
      public Report()
      {
         InitializeComponent();

         func_start();
      }
private void func_start()
      {
         // Коефіцієнт збитку 2 чи 4
         string coef = Coefficient();

         // Назва підприємства та його статок за минулий рік
         string NameCompany = Identification(1);
         string Profit = Identification(2);

         lbNameCompany.Text = NameCompany;

         List<string> ii = new List<string>();
         for (int i = Profit.Length - 1, j = 0; i >= 0; i--)
         {
            if (j == 3)
            {
               ii.Insert(0, " ");
               ii.Insert(0, (Profit[i].ToString()));
               j = 0;
            }
            else
            {
               ii.Insert(0, (Profit[i].ToString()));
            }
            j++;
         }
```

```
string iii = "";
foreach (string number in ii)
   iii += number;
lbProfit.Text = iii + " €";

// Обчислення максимальної суми збитку компанії
float temp1 = Convert.ToSingle(Profit);
float temp2 = Convert.ToInt32(coef);
bool ident = false;

float temp3 = Convert.ToSingle(Math.Abs(temp1 * (temp2 / 100)));
maxProfit = Math.Round(temp3, 2);

Circular.MaxValue = Convert.ToInt32(circular_func_value(temp3));

string ttemp3 = Math.Round(temp3, 2).ToString();
List<string> mProfitT = new List<string>();
for (int i = 0; i < ttemp3.Length; i++)
{
   if (ttemp3[i].ToString() == ",")
   {
      ident = true;
      break;
   }
   else
      ident = false;
}

if (ident == true)
{
   for (int i = ttemp3.Length - 1, j = 0, k = 0; i >= 0; i--)
   {
      if (k == 1)
      {
         if (j == 3)
         {
            mProfitT.Insert(0, " ");
            mProfitT.Insert(0, (ttemp3[i].ToString()));
            j++;
         }
         else
         {
            mProfitT.Insert(0, (ttemp3[i].ToString()));
         }
         j++;
      }
      else
      {
         if (ttemp3[i].ToString() == ",")
         {
```

```
                    mProfitT.Insert(0, (ttemp3[i].ToString()));
                  k++;
                }
              else
                    mProfitT.Insert(0, (ttemp3[i].ToString()));
            }
          }
        }
        else
        {
          for (int i = ttemp3.Length - 1, j = 0; i >= 0; i--)
          {
            if (j == 3)
            {
              mProfitT.Insert(0, " ");
              mProfitT.Insert(0, (ttemp3[i].ToString()));
              j = 0;
            }
            else
            {
              mProfitT.Insert(0, (ttemp3[i].ToString()));
            }
            j++;
          }
        }

        ttemp3 = "";
        foreach (string number in mProfitT)
          ttemp3 += number;
        lbMaxFines.Text = (ttemp3).ToString() + " €";

        // Додавання даних в таблицю
        Add();
      }
// Коефіцієнт збитку 2 чи 4
      private string Coefficient()
      {
        string coef = "";

        DataSet ds = new DataSet();
        try
        {
          ds.ReadXml(pathCoefficient);
        }
        catch { }

        try
        {
          foreach (DataRow item in ds.Tables["Data_Coefficient"].Rows)
          {
            coef = (item["Number_Coefficient"]).ToString();              }
```

```
            if (coef == "2")
            {
                lbCoefficient.Text = "Застосування адміністративного штрафу сумою до 10 000 000 євро або, у випадку\nпідприємства, до 2% від загального глобального річного обігу за попередній фіна-\nнсовий рік, залежно від того, яка сума є вищою";
            }
            if (coef == "4")
            {
                lbCoefficient.Text = "Застосування адміністративного штрафу сумою до 20 000 000 євро або, у випадку\nпідприємства, до 4% від загального глобального річного обігу за попередній фіна-\nнсовий рік, залежно від того, яка сума є вищою";
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show("Error: " + ex.ToString(), "Error");
        }

        return coef;
    }
// Назва підприємства та його статок за минулий рік
    private string Identification(int digit) // 1 - Назва компанії, 2 - Статок компанії
    {
        string NameCompany = "";

        DataSet ds = new DataSet();
        ds.ReadXml(pathDetailBusiness);

        try
        {
            foreach (DataRow item in ds.Tables["Detail_Business"].Rows)
            {
                if (digit == 1)
                {
                    if ((item["Confirm_Company"]).ToString() == "Так")
                        NameCompany = (item["Name_Company"]).ToString();
                    if ((item["Confirm_Company"]).ToString() == "Ні")
                        NameCompany = "Не організація";
                }
                if (digit == 2)
                {
                    if ((item["Confirm_Company"]).ToString() == "Так")
                        NameCompany = (item["Profit_Company"]).ToString();
                }
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show("Проблема " + ex.ToString(), "Проблема завантаження файлу");
}
```

```
            return NameCompany;
        }
private void Add()
        {
            int data = 0;

            string temp1 = "";

            double calculate1 = 0;
            double calculate2 = 0;
            double calculate3 = 0;
            double calculate4 = 0;
            double calculate5 = 0;
            double calculate6 = 0;
            double calculate7 = 0;
            double calculate8 = 0;
            double calculate9 = 0;
            double calculate10 = 0;
            double calculate11 = 0;

            // Статя 83(2а)
            temp1 = FiQ(1); data = Convert.ToInt32(temp1);
            temp1 = FiQ(2); data += Convert.ToInt32(temp1);
            temp1 = FiQ(3); data += Convert.ToInt32(temp1);
            temp1 = FiQ(4); data += Convert.ToInt32(temp1);

            int mark1 = 20;
            Counter += data;

            calculate1 = CalculateData(mark1);
            Circular1_a.MaxValue =
Convert.ToInt32(circular_func_value(Convert.ToSingle(calculate1)));

            if (calculate1 > 0)
               lbMaxFines1.Text = calculate1.ToString() + " €";
            else
               lbMaxFines1.Text = "0" + " €";

            calculate1 = CalculateData(data);
            Circular1_a.Value = Convert.ToInt32(circular_func_value(Convert.ToSingle(calculate1)));

            if (calculate1 > 1)
               lbFine1.Text = calculate1.ToString() + " €";
            else
               lbFine1.Text = "0" + " €";

            lbCountMark1.Text = Counter.ToString() + " балів"; … }}}
```

ДОДАТОК В

Акти впровадження наукових досліджень дисертаційної роботи

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ЕН-ЛАЙН»
(ТОВ "ЕН-ЛАЙН")

вул. Грушевського Михайла, 28/2, н.п. №43, м. Київ, 01021
тел.: +38 (044) 228-52-22, e-mail: info@nline.net.ua
UA 583006140000026008500512203
в АТ "КРЕДІ АГРІКОЛЬ БАНК"
Код установи банку 300614
Код ЄДРПОУ 31626810

ЗАТВЕРДЖУЮ
Директор товариства з обмеженою
відповідальністю «ЕН-ЛАЙН»
_____ Юрій ВАРЕНИЦЯ
(підпис)
"19" травня 2025 року
М.П.

АКТ

Комісія у складі
голови – директор, Варениця Юрій Васильович;
членів комісії: – заступник директора, Тимченко Євгеній Олександрович
– головний адміністратор системи, Якименко Микола Юрійович

цим Актом засвідчує, що результати дисертаційного дослідження старшого викладача кафедри кібербезпеки Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут».

Лозової Ірини Леонідівни

на тему: "Моделі та методи оцінювання негативних наслідків від витоку персональних даних"
на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»
впроваджені в діяльності товариства з обмеженою відповідальністю «ЕН-ЛАЙН».

У межах діяльності ТОВ «ЕН-ЛАЙН» було впроваджено прикладне програмне забезпечення, розроблене на основі результатів дисертаційної роботи Лозової Ірини Леонідівни. Зазначене програмне забезпечення реалізує алгоритми автоматизованої системи оцінювання негативних наслідків витоку персональних даних та дозволяє моделювати інциденти, визначати ймовірні штрафні санкції відповідно до вимог GDPR, а також генерувати персоналізовані рекомендації щодо підвищення рівня інформаційної безпеки організації. Впровадження програмного продукту дозволило підприємству підвищити якість оцінки ризиків, скоротити час аналізу інцидентів, забезпечити відповідність діяльності чинним європейським стандартам у сфері захисту персональних даних, а також покращити процес ухвалення управлінських рішень у сфері кібербезпеки. Практичне використання розробки підтвердило її ефективність як інструмента підтримки безпеки даних, управління інцидентами та зниження потенційних фінансових і репутаційних втрат.

Голова комісії	Директор	_____ (підпис)	Юрій ВАРЕНИЦЯ
Члени комісії	Заступник директора	_____ (підпис)	Євгеній ТИМЧЕНКО
	Головний адміністратор системи	_____ (підпис)	Микола ЯКИМЕНКО

FLY TECHNOLOGY

ТОВ «ФЛАЙ ТЕХНОЛОДЖИ УА»
Україна, 04050, м. Київ,вул. Глибочицька, 44
ЄДРПОУ 45106491

ЗАТВЕРДЖУЮ
Директор ТОВ «ФЛАЙ ТЕХНОЛОДЖИ УА»
Олександр КАЗЬМІН
"12" травня 2025 року
М.П.

АКТ

Комісія у складі:

- голови – директора Казьміна Олександра Олеговича;
- членів комісії:
  – в.о. фінансового директора, Кравченко Юлії Володимирівни
  – в.о. начальника відділу продажу, Кулика Дмитра Олександровича

цим Актом засвідчує, що результати дисертаційного дослідження старшого викладача кафедри кібербезпеки Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» **Лозової Ірини Леонідівни** на тему: **"Моделі та методи оцінювання негативних наслідків від витоку персональних даних" на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»** впроваджені в діяльності ТОВ «ФЛАЙ ТЕХНОЛОДЖИ УА».

У межах інформаційно-аналітичної підтримки внутрішніх процесів з управління ризиками конфіденційності персональних даних в ТОВ «ФЛАЙ ТЕХНОЛОДЖИ УА» було впроваджено прикладне програмне забезпечення, створене на основі результатів дисертаційної роботи Лозової Ірини Леонідівни. Практичне застосування зазначеного програмного продукту в межах компанії дало змогу автоматизувати процес оцінювання ризиків витоку персональних даних, суттєво скоротити час обробки інцидентів, підвищити точність і прозорість ухвалення управлінських рішень у сфері кіберзахисту, а також забезпечити відповідність політик безпеки підприємства сучасним європейським вимогам. Отримані результати впровадження підтверджують ефективність і прикладну цінність дисертаційного дослідження Лозової Ірини Леонідівни.

Голова комісії Директор _____ Олександр КАЗЬМІН

Члени комісії В.о. фінансового директора _____ Юлія КРАВЧЕНКО

В.о. начальника відділу продажів _____ Дмитро КУЛИК

ТОВ "СІТОН ДІДЖИТАЛ"
вул. Гарматна, 4, 4-й поверх, офіс 4,
Київ, Україна, 03067
+380 44 239 99 99
info@seeton.digital

ЗАТВЕРДЖУЮ
Директор товариства з обмеженою відповідальністю «СІТОН ДІДЖИТАЛ»
Дмитро НІКІТЮК
(підпис)
"02" червня 2025 року
М.П.

АКТ

Комісія у складі:
голови – директор, Нікітюк Дмитро Вікторович;
членів комісії: – керівник відділу систем інформаційної безпеки, Педченко Євгеній Максимович
– заступник керівника відділу систем інформаційної безпеки, Коровайченко Юрій Юрійович

цим Актом засвідчує, що результати дисертаційного дослідження старшого викладача кафедри кібербезпеки Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут».

Лозової Ірини Леонідівни

на тему: "Моделі та методи оцінювання негативних наслідків від витоку персональних даних" на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»
впроваджені в діяльності **товариства з обмеженою відповідальністю «СІТОН ДІДЖИТАЛ».**

Зокрема, під час створення спеціалізованого програмного забезпечення для оцінювання рівня критичності інцидентів витоку персональних даних, орієнтованого на застосування в державних та приватних організаціях України, використано результати дисертаційної роботи Лозової Ірини Леонідівни, які включають формалізовану структурну модель автоматизованої системи підтримки прийняття рішень щодо оцінювання інцидентів, алгоритмічне забезпечення обчислення збитків, а також інтегровану базу даних інцидентів і відповідних оціночних характеристик. Зазначені наукові напрацювання стали основою для практичного впровадження механізмів автоматизованого аналізу негативних наслідків витоку персональних даних для підтримки інформаційної безпеки та управління ризиками в інформаційних системах.

Голова комісії	Директор	(підпис) Дмитро НІКІТЮК
Члени комісії	Керівник відділу систем інформаційної безпеки	(підпис) Євгеній ПЕДЧЕНКО
	Заступник керівника відділу систем інформаційної безпеки	(підпис) Юрій КОРОВАЙЧЕНКО

ДОДАТОК Г

Список опублікованих праць за темою дисертації

1. Шаховал О., Лозова І., Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. *Захист інформації*. 2016. Т. 18, № 1. С. 57–65. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_1_9

2. Гізун А., Лозова І. Аналіз дефініцій поняття кризова ситуація та основних аспектів концепції управління безперервністю бізнесу. *Безпека інформації*. 2016. Т. 22, № 1. С. 99-108. URL: http://nbuv.gov.ua/UJRN/bezin_2016_22_1_17.

3. Корченко О., Дрейс Ю., Лозова І. Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. *Захист інформації*. 2016. Т. 18, № 1. С. 39-47. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_1_7

4. Гізун А., Лозова І., Трикуш О. Застосування механізму кореляції інцидентів/потенційних кризових ситуацій для оцінювання рівня критичності поточної ситуації в інформаційній сфері. *Безпека інформації*. 2017. Т. 23, № 3. С. 215-221. URL: http://nbuv.gov.ua/UJRN/bezin_2017_23_3_10

5. О. Корченко, Ю.Дрейс, І.Лозова, Є. Педченко. Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*. 2020. Т. 22, № 2. С. 120-141. URL: https://doi.org/10.18372/2410-7840.22.14871

6. Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л., Педченко Є.М. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Захист інформації.* 2023. Т. 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232.

7. Корченко О.Г., Лозова І.Л. Структурна модель системи оцінки негативних наслідків втрати персональних даних. *Наукові записки ДУІКТ*. 2024. №2 (6). С. 165-170. URL: https://doi.org/10.31673/2786-8362.2024.028264

8. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., Balagura, D. Development of the sociocyberphysical systems` multi-contour security methodology. *Eastern-European Journal of Enterprise Technologies*. 2024. Vol. 1, no. 9 (127). P. 34–51. (*Scopus*) URL: https://doi.org/10.15587/1729-4061.2024.298844

9. Pedchenko Y., Karpinski M., Lozova I., Kotyk O., Petrovska M. Damage assessment from the personal data loss. Problems of scientific, technical and legal support for cybersecurity in the modern world : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 34-46. DOI: 10.24917/9788668020861 URL: https://bazawiedzy.uken.krakow.pl/info/article/UKENca47634692fd430697964f5fa8af695f/

10. V. Hrebenuik , Y. Dreis, A. Hrebenuik, I. Lozova. Definitions in the field of personal data protection: a comparative analysis of the legislation of Ukraine and European Union. Technologie, procesy i systemy produkcyjne: Monografia. Tom3. Akademia Techniczno Humanistyczna w Bielsku-Bialej, 2020. pp. 141 - 146. URL: https://engineerxxi.ubb.edu.pl/fcp/eHFNIBD8dJBYXMwoXQH5hbEpmfHIGFBcNBi4oGgh0VWFeUxRUPBYvEkFWQQMOZm96Dzc1IikcFEpjZXQLC3QZ/_users/code_0DQNBBTkZMh4KLBYRAGomPA9qIDw/publikacje/2020/engineerxxi_2020_vol3_13.pdf

11. Y. Dreis, I. Lozova, A. Biskupskyi, Y. Pedchenko, Y. Ivanchenko. GDPR-model of parameters for estimating losses from loss of personal data. Przetwarzanie, transmisja i bezpieczeństwo informacji: Monografia. Tom 2. Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2019. pp. 127 - 138. URL: https://www.researchgate.net/profile/Yurii-Dreis-2/publication/387069634_GDPR-MODEL_OF_PARAMETERS_FOR_ESTIMATING_LOSSES_FROM_LOSS_OF_PERSONAL_DATA_MODEL_PARAMETROW_GDPR_DO_SZACOWANIA_STRAT_Z_UTRATY_DANYCH_OSOBOWYCH/links/675edfb7da24c8537c76497f/GDPR-MODEL-OF-PARAMETERS-FOR-ESTIMATING-LOSSES-FROM-LOSS-OF-PERSONAL-DATA-MODEL-PARAMETROW-GDPR-DO-SZACOWAN IA-STRAT-Z-UTRATY-DANYCH-OSOBOWYCH.pdf

12. Комп'ютерна програма «Програмний модуль оцінки негативних наслідків від витоку персональних даних»: а. с. 96927 Україна/ Ю. Дрейс., І. Лозова, Є. Педченко. Заявл. 27.03.2020 ; опубл. 29.05.2020, Бюл. № 58. URL: https://sis.nipo.gov.ua/uk/search/detail/1625864/

13. Лозова І., Корченко О. Розробка моделі системи оцінки негативних наслідків втрати персональних даних. *ITSec: Безпека інформаційних технологій*: Матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С.124-125. URL: https://drive.google.com/file/d/1Nt2w9E-N97TAIdAGqWKbaXsqASyP-4tt/view

14. Лозова І.Л., Корченко О.Г., Котик О.В. Оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали X Міжнарод. наук.-практ. конф., Київ, 25 квітня 2024 р. / Редкол.: О. І. Тимошенко та ін. Київ: Вид-во Європейського університету, 2024. С. 74-78. URL: https://e-u.edu.ua/userfiles/files/135/2024-zbirnik_h_mizhnarodna-_konf_aktualni_pitannya_zabezpechennya_kiberbezpeki_ta_zahistu_informacii.pdf

15. 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

16. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. Analysis of modern cloud services to ensure cybersecurity. *6th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES* 2022, Vol. 207, pp. 110 - 117. (*Scopus*). URL: https://doi.org/10.1016/j.procs.2022.09.043

17. Gnatyuk, S., Berdibayev, R., Azarov, I., Baisholan, N., Lozova I. Modern Types of Databases for SIEM System Development. *CEUR Workshop*

Proceedings, 2021, 3187, pp. 127-138. (*Scopus*). URL: https://ceur-ws.org/Vol-3187/paper12.pdf

18. Корченко О.Г., Лозова І.Л., Дрейс Ю.О., Хохлачова Ю.Є. Алгоритмічне забезпечення системи оцінки негативних наслідків від втрати персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали VII міжнарод. наук.-практ. конф., 24-27 лютого 2021 р. Київ: Вид-во Європейського університету, 2021. С.40-42. URL: https://www.researchgate.net/publication/389848654_ALGORITMICNE_ZABEZPECENNA_SISTEMI_OCINKI_NEGATIVNIH_NASLIDKIV_VID_VTRATI_PERSONALNIH_DANIH

19. 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.

20. Лозова І., Педченко Є., Баланда А. Теоретико-множинне представлення параметру «Рівень порушення» для кортежної GDPR-моделі, *ITSec-2020: Безпека інформаційних технологій*: Матеріали X міжнар. наук.-техніч. конф., м. Київ, 19-24 березня 2020 року. Київ, 2020. С. 47-49.

21. Дрейс Ю., Скворцов С., Лозова І., Біскупський А. Множинна інтерпретація параметрів «Зниження шкоди» та «Ступінь відповідальності» для кортежної GDPR-моделі. *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2020)*: Матеріали 12-ої Всеукр. науково-практ. конф., м. Миколаїв, 24-26 черв. 2020 р. Миколаїв, 2020. С. 21-24. URL: https://www.researchgate.net/publication/389848384_MNOZINNA_INTERPRETACIA_PARAMETRIV_ZNIZENNA_SKODI_TA_STUPIN_VIDPOVIDALNOSTI_DLA_KORTEZNOI_GDPR-MODELI

22. Лозова І. Теоретико-множинне представлення окремих параметрів для кортежної GDPR-моделі. *Безпека ресурсів інформаційних систем*: збірник тез І Міжнародної науково-практичної конференції, м. Чернігів, 16-17 квітня 2020 р.,

Чернігів: НУЧП, 2020. С. 110-116. URL: https://stu.cn.ua/wp-content/uploads/2021/04/bris-t.pdf

23. Дрейс Ю.О., Лозова І.Л., Ковальов Д.А. Структурно-параметрична GDPR-модель оцінки негативних наслідків від витоку персональних даних. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: Матеріали VI міжнарод. наук.-практ. конф., 19 – 22 лютого 2020 р. Київ: Вид-во Європейського університету, 2020. – С. 39-41. URL: https://www.researchgate.net/publication/389811894_STRUKTURNO-PARAMETRICNA_GDPR-MODEL_OCINKI_NEGATIVNIH_NASLIDKIV_VID_VITOKU_PERSONALNIH_DANIH

24. Дрейс Ю.О., Лозова І.Л. Розробка GDPR-моделі параметрів оцінювання наслідків витоку персональних даних. *Комп'ютерні технології: інновації, проблеми, рішення*: Матеріали II Всеукраїнської науково-технічної конференції, м. Житомир, 14-15 листопада 2019 р. Житомир, Житомирська політехніка, 2019. С. 78-79. URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/tezy-dopovidej-kt2019_os.pdf

25. Дрейс Ю.О., Лозова І.Л., Педченко Є.М. Оцінювання негативних наслідків від витоку персональних даних. *ITSec: Безпека інформаційних технологій*: Матеріали IX міжнародної науково-технічної конференції, м. Київ, 22-27 березня 2019 р. Київ, 2019. С.41-42.

26. Дрейс Ю.О., Лозова І.Л. Формування параметрів оцінювання негативних наслідків витоку персональних даних в автоматизованих системах. *ITSec: Безпека інформаційних технологій*: Матеріали VIII міжнародної науково-технічної конференції, м.Київ,16-18 травня 2018 р. Київ, 2018. С.14-15.