МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЛОЗОВА ІРИНА ЛЕОНІДІВНА

УДК 004.056.5:004.4(043)

МОДЕЛІ ТА МЕТОДИ ОЦІНЮВАННЯ НЕГАТИВНИХ НАСЛІДКІВ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

Спеціальність 05.13.21 «Системи захисту інформації»

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2025

Дисертацією є рукопис.

Робота виконана в Державному університеті інформаційно-комунікаційних технологій Міністерства освіти і науки України.

Науковий керівник	доктор технічних наук, професор **Корченко Олександр Григорович** Державний університет інформаційно-комунікаційних технологій, перший проректор
Офіційні опоненти:	доктор технічних наук, старший дослідник **Гончар Сергій Феодосійович**, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, заступник директора з науково-технічної роботи
	доктор технічних наук, професор **Опірський Іван Романович**, Національний університет «Львівська політехніка», завідувач кафедри захисту інформації

Захист відбудеться «08» вересня 2025 року об 11:00 годині на засіданні спеціалізованої вченої ради Д 26.861.06 у Державному університеті інформаційно-комунікаційних технологій за адресою: 03110, м. Київ, вул. Солом'янська, 7.

З дисертацією можна ознайомитись у бібліотеці Державного університету інформаційно-комунікаційних технологій за адресою: 03110, м. Київ, вул. Солом'янська, 7.

Автореферат розісланий «08» серпня 2025 року.

Учений секретар
спеціалізованої вченої ради Д 26.861.06

PhD Віталій МАРЧЕНКО

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У сучасних умовах стрімкої цифровізації, зростання кількості онлайн-сервісів та обсягів персональних даних, питання забезпечення конфіденційності та безпеки персональної інформації набуває особливої актуальності. Витоки даних призводять до порушень прав людини, фінансових і репутаційних втрат для організацій, а в окремих випадках – до загроз національній безпеці.

Власники та розпорядники персональних даних, згідно з GDPR і чинним законодавством України, зобов'язані впроваджувати ефективні засоби оцінки шкоди та інформування постраждалих. Проте на практиці бракує універсальних формалізованих моделей для оцінки втрат від витоків, зокрема з урахуванням множинності інцидентів, їх взаємозв'язку та змінності ризиків. Особливо це актуально для державних і критичних інформаційних систем, банківської, медичної та освітньої сфер.

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. тощо. Проте, незважаючи на значні досягнення в цій галузі, переважна більшість наукових досліджень присвячена правовим аспектам забезпечення конфіденційності персональних даних, тоді як технічні механізми захисту, а також методи оцінювання наслідків інцидентів, пов'язаних із витоком інформації 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 та 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).

Мета і задачі дослідження. 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.

Для досягнення поставленої мети в роботі вирішуються **основні 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 дослідження 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:

– 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. Практична цінність роботи полягає в наступному:

– 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] та 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 та обсяг роботи. 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.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і задачі досліджень, визначено наукову новизну і практичну цінність отриманих результатів, наведено дані про їх апробацію та впровадження.

У **першому розділі** узагальнено термінологічний апарат у сфері захисту персональних даних відповідно до законодавства України та стандартів ЄС (зокрема GDPR). Визначено, що персональні дані мають стратегічне значення, а їх захист є важливим елементом інформаційної безпеки. Узгодженість термінології між українським правом і GDPR розглядається як основа для інтеграції у європейський правовий простір.

Проведений аналіз нормативно-правового забезпечення захисту персональних даних продемонстрував багатовекторний 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.

Проаналізовано широкий спектр існуючих моделей, методів та систем оцінювання наслідків витоків персональних даних. Дослідження охопило як міжнародні (FAIR, NIST, DPIA, ISO, OCTAVE, MEHARI, EBIOS, Ponemon, CyberVaR), так і вітчизняні підходи (моделі для освітніх, військових установ, соцмереж). Усі вони були оцінені за критеріями відповідності GDPR, наявності реалізації, категорій втрат, типів оцінки та результатів. В результаті аналізу встановлено, що існує реальна 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.

Другий розділ присвячений розробці моделей оцінювання втрат від витоку персональних даних.

Розроблено *теоретико-множинну GDPR-модель параметрів персональних даних* у вигляді $\mathbf{IDF}^{\varphi} = < \mathbf{IDF}_1^{\varphi}, \mathbf{IDF}_2^{\varphi}, ..., \mathbf{IDF}_i^{\varphi}, ..., \mathbf{IDF}_n^{\varphi} >$, де: $\mathbf{IDF}_i^{\varphi} \subseteq \mathbf{IDF}^{\varphi}$ $(i = \overline{1,n})$ – компонент, що відображає *i*-й ідентифікатор параметрів φ-ї організації, а n – максимальне число таких параметрів. Відповідно до Регламенту GDPR, при $n = 14$ кортеж визначимо як: $\mathbf{IDF}^{\varphi} = < \mathbf{IDF}_1^{\varphi}, \mathbf{IDF}_2^{\varphi}, ..., \mathbf{IDF}_7^{\varphi}, ..., \mathbf{IDF}_{14}^{\varphi} > = < \mathbf{T}^{\varphi}, \mathbf{L}^{\varphi}, \mathbf{N}^{\varphi}, \mathbf{CH}^{\varphi}, \mathbf{A}^{\varphi}, \mathbf{R}^{\varphi}, \mathbf{I}^{\varphi}, \mathbf{C}^{\varphi}, \mathbf{CA}^{\varphi},$

$\mathbf{M^{\varphi}, ME^{\varphi}, AD^{\varphi}, F^{\varphi}, RE^{\varphi}}$ >, де $\mathbf{T^{\varphi}}$ – річний обіг; $\mathbf{L^{\varphi}}$ – рівень порушення; $\mathbf{N^{\varphi}}$ – специфіка порушення; $\mathbf{CH^{\varphi}}$ – характер порушення; $\mathbf{A^{\varphi}}$ – зниження шкоди; $\mathbf{R^{\varphi}}$ – ступінь відповідальності; $\mathbf{I^{\varphi}}$ – рецидив порушення; $\mathbf{C^{\varphi}}$ – рівень співпраці; $\mathbf{CA^{\varphi}}$ – категорії даних; $\mathbf{M^{\varphi}}$ – спосіб виявлення; $\mathbf{ME^{\varphi}}$ – відповідність заходам; $\mathbf{AD^{\varphi}}$ – дотримання кодексів; $\mathbf{F^{\varphi}}$ – визначаючий чинник; $\mathbf{RE^{\varphi}}$ – превентивні рекомендації.

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 автоматизованих системах. Дана модель має наступну структуру: < **A,B, C, D,E,F,G,H,I** >, де **A** – характеристика персональних даних (ідентифікація їх складу та змісту); **B** – характеристика середовища обробки персональних даних в автоматизованих системах; **C** – мета обробки персональних даних; **D** – аудит застосованих механізмів безпеки; **E** – характеристика існуючих функціональних послуг безпеки; **F** – ідентифікація загроз безпеці персональних даних при обробці в автоматизованих системах; **G** – величина можливих збитків від втрати персональних даних; **H** – оцінка ризику захисту персональних даних в автоматизованих системах; **I** – керування ризиком та досягнення необхідного рівня гарантій захисту персональних даних.

Розроблено *модель параметрів для оцінювання критичності кризових ситуацій*, що дозволяє враховувати як індивідуальні характеристики інцидентів, так і їх взаємозалежність через механізм кореляції подій. Основним елементом моделі 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: $\mathbf{IKS} = \{\bigcup_{i=1}^{5} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \mathbf{IKS_2}, \mathbf{IKS_3}, \mathbf{IKS_4}, \mathbf{IKS_5}\} = \{\mathbf{A},\mathbf{B},\mathbf{C},\mathbf{D},\mathbf{E}\}$, де **A**,**B**,**C**,**D**,**E** – назви інцидентів. Відповідно для кожного з цих інцидентів характерні свої набори оціночних параметрів $\mathbf{L_i} = \bigcup_{i=1}^{N}\left\{\bigcup_{e=1}^{E} \underset{\sim}{L_e}\right\} = \bigcup_{i=1}^{N}\left\{\underset{\sim}{L_1}, \underset{\sim}{L_2}, ..., \underset{\sim}{L_E}\right\}$, $e = \overline{1,E}$, де E – кількість параметрів. 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 персональних даних.

У **третьому розділі** проведено розробку методів та системи оцінювання негативних наслідків від витоку персональних даних.

Розроблений *метод оцінювання негативних наслідків від порушення конфіденційності персональних даних* базується на структурно-параметричній моделі, що враховує специфіку GDPR і дозволяє автоматизувати процес оцінки наслідків.

Етап 1. Ідентифікація об’єкта оцінювання. Визначення глобального річного обігу підприємства за минулий рік. Формування параметра T^{φ} здійснюється шляхом визначення експертом річного обігу в €.

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:

$$P_{РП}^{\varphi} = \bigvee_{i=1}^{n_1} \bigvee_{j=1}^{n_{1i}} B_{ij}^{\varphi L} C_{ij}^{\varphi L} = (B_{11}^{\varphi L} C_{11}^{\varphi L} \vee B_{12}^{\varphi L} C_{12}^{\varphi L} \vee ... \vee B_{1n_{11}}^{\varphi L} C_{1n_{11}}^{\varphi L}) \vee$$

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

Етап 3. Формування первинної експертної інформації

Крок 1. Починається з визначення показника «Специфіка порушення». Для визначення $P_{СП}^{\varphi}$ для φ-го об’єкту скористаємося виразом:

$$P_{СП}^{\varphi} = \sum_{i=1}^{n_2} \bigvee_{j=1}^{n_{2i}} B_{ij}^{\varphi N} C_{ij}^{\varphi N} = (B_{11}^{\varphi N} C_{11}^{\varphi N} \vee B_{12}^{\varphi N} C_{12}^{\varphi N} \vee ... \vee B_{1n_{21}}^{\varphi N} C_{1n_{21}}^{\varphi N}) +$$

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

Аналогічним чином обчислюється **Крок 2 – Крок 11**. 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 відповідно приймають числові значення, 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. 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. Використовуються значення показників, отриманих на Етапі 3. Сумарне значення для кожного виразу присвоюється його власному ідентифікатору P_i^{φ}. Даний вираз матиме наступний вигляд: $\sum_{i=1}^{11} P_i^{\varphi} = P_{СП}^{\varphi} + P_{ХП}^{\varphi} + P_{ЗШ}^{\varphi} + P_{СВ}^{\varphi} + P_{РЦП}^{\varphi} +$

$P_{РС}^{\varphi} + P_{КД}^{\varphi} + P_{СПВ}^{\varphi} + P_{ВЗ}^{\varphi} + P_{ДК}^{\varphi} + P_{ВЧ}^{\varphi}$, де $P_i^{\varphi} \subseteq \mathbf{P}^{\varphi}$ $(i = \overline{1,11})$ – сума всіх набраних балів виходячи із суджень експерта. Максимальна сума для всіх кроків Етапу 3 складає 160 балів. Введемо змінну TMC^{φ}, що буде містити коефіцієнт

обчисленої кількості отриманих балів для всіх 11 кроків Етапу 3: $TMC^{\varphi} = \sum_{i=1}^{11} P_i^{\varphi} / 160.$

Крок 3. Обчислення максимально-наближеного штрафу для підприємства. Введемо змінну MF^{φ}, що буде відповідати за максимальний штраф: $MF^{\varphi} = T^{\varphi} \times P_{СП}^{\varphi}$. Для обчислення максимально наближеного штрафу, введемо зміну $AF^{\varphi} = MF^{\varphi} \times TMC^{\varphi}$.

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 персональних даних та відповідні заходи захисту, особливо в державних автоматизованих системах відповідно до національного законодавства.

Етап 1. Проведення аналізу документів, середовища та мети обробки персональних даних

Крок 1. Визначаємо документи, що містять персональні дані та коефіцієнт їх важливості: $K_{vd} = \sum_{i=1}^{n} K_{vd_n}, K_{vd} = K_{vd_1} + K_{vd_2} + K_{vd_3} ... + K_{vd_i}$.

Крок 2. Визначення середовища обробки персональних даних, що містяться у вказаних документах. Аналогічно, за кроком 1, визначаються коефіцієнти K_v та K_{vr} для програмних засобів обробки персональних даних.

Крок 3. Визначення мети обробки персональних даних. Мета обробки персональних даних визначається в залежності від того, саме де та для якого очікуваного кінцевого результату такі персональні дані будуть оброблятися. Даний параметр представляється у вигляді множини ідентифікаторів згідно до законодавства: $C_n \in \{C_1, C_2, C_3, C_4, C_5, C_6 ... C_i\}$. Визначення максимально можливого розрахункового значення ризику R_{max} знаходиться за відношенням суми коефіцієнтів важливості всіх об'єктів, що знаходяться під загрозою, до сумарної величини коефіцієнтів важливості об'єктів та визначається за формулою: $R_{max} = (K_{vdr} + K_{vpr}) / (K_{vd} + K_{vp})$.

Етап 2. Аналіз функціонуючих механізмів безпеки. Кожен із запропонованих механізмів безпеки в моделі забезпечує корегування визначеного максимально можливого розрахункового значення ризику на коефіцієнт 0,2: $K_m = \sum_{n=1}^{i} D_n \times 0,2, (i = \overline{1,n})$.

Етап 3. Ідентифікація можливих загроз захисту персональних даних при обробці в автоматизованих системах. Даний параметр наводиться у вигляді набору елементів відомих загроз безпеці персональних даних, а саме $F_n \in \{F_1, F_2, F_3, F_4, F_5, F_6 ... F_i\}$. По відношенню до визначених загроз визначається ймовірність їх реалізації (настання) як: «низька» P_{r_1}, «середня» P_{r_2} та «висока»

P_{r_3} що приведено формулою: $P_{riv\_zag} = \{\bigcup_{i=1}^{n} P_{r_i}\} = \{P_{r_1}, P_{r_2}, P_{r_3}, ... P_{r_i}\}$, $R_{riv\_zag} \in \{R_{riv\_zag_{i_{max}}}\}$, $(i=\overrightarrow{1,n})$, де n – кількість запропонованих загроз, i – номер загрози. Розрахункове значення ризику з урахуванням рівня реалізації загроз $R_{zag_{corr}}$ визначається за формулою: $R_{zag_{corr}} = P_{riv\_zag} \times R_{max}$. Після розрахунку $R_{zag_{corr}}$, визначимо розрахунковий інтервал – в межах якого і знаходиться реальний ризик захисту персональних даних.

Етап 4. Визначення величини можливого збитку від витоку персональних даних. Визначається як кількісними, так і якісними показниками: розрахунковий інтервал ризику можливого витоку персональних даних; грошовий еквівалент ризику можливих збитків; бальна оцінка ризику втрати персональних даних.

Етап 5. Оцінка ризиків захисту персональних даних. На даному етапі визначається корекція ймовірності з врахуванням механізмів захисту R_{C_corr} за формулою $R_{C\_corr} = (I_{min} + (I_{max} - I_{min}) \times (1-K_m)), I \in (I_{min}, I_{max})$. Даний інтервал витоку персональних даних визначається збитками в грошовому еквіваленті на рівні $G \in (G_{min}, G_{max})$. Таким чином ймовірні збитки в грошовому еквіваленті, визначаються як: $R_g = G_{min} + (G_{max} - G_{min}) \times R_{C\_corr}$.

Етап 6. Управління ризиком захисту персональних даних. Після проведення аналізу та оцінки ризиків персональних даних, можна сформувати кінцеві висновки про стан рівня захищеності персональних даних в конкретній автоматизованій системі. А отже, можна надати рекомендації щодо підвищення цього стану, а саме через впровадження тих чи інших механізмів безпеки відповідно до національного законодавства.

Розроблено *метод оцінювання рівня критичності у разі витоку персональних даних*, що складається з наступних етапів: 1. Визначення кількості кризових ситуацій, з якими проводяться операції, та наборів оціночних параметрів для кожного з них; 2. Визначення основної і залежної кризових ситуацій; 3. Визначення коефіцієнтів кореляції для кожної залежної та основної кризової ситуації відповідно; 4. Визначення сумарного рівня критичності з врахуванням залежності між окремими інцидентами в аспекті спричиненого ними впливу обчислюється 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 кризових ситуацій з врахуванням кореляції між ними, N - загальна кількість інцидентів, $\underset{\sim}{LCS}^K_i = K_{IKS_{осн} IKS_{заг_i}} * \underset{\sim}{LCS}_i, i = \overline{2,N}$ – рівень критичності корельованої i-ї кризової ситуації , $\underset{\sim}{LCS}^K_1 = \underset{\sim}{LCS}_{осн}$, N – загальна кількість інцидентів. 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.

Розроблено *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 персональних даних.

Розроблено *структурну модель системи оцінювання негативних наслідків втрати персональних даних*, яка містить (рис.2): блок формування та зберігання даних (БФЗД); блок ідентифікації та визначення рівня порушення (БІВРП); блок формування експертної інформації (БФЕІ); блок обробки експертних даних (БОЕД).

БФЗД служить для підготовки даних, заснованих на судженнях експертів і складається з: бази даних групи питань (БДГП) – містить питання для аналізу ризиків; бази даних результатів опитувань (БДРО) – включає зібрані відповіді експертів; бази даних рекомендацій (БДР) – зберігає пропозиції щодо мінімізації ризиків.

БІВРП складається з: модуля визначення загального глобального річного обігу (ЗГРО) – формування компоненти T^{φ} ; модуля визначення показника рівня порушення (ПРП) – $P_{РП}^{\varphi}$ обчислюється на основі множини визначених рівнів порушення, відносно яких формується коефіцієнт максимально можливого збитку.

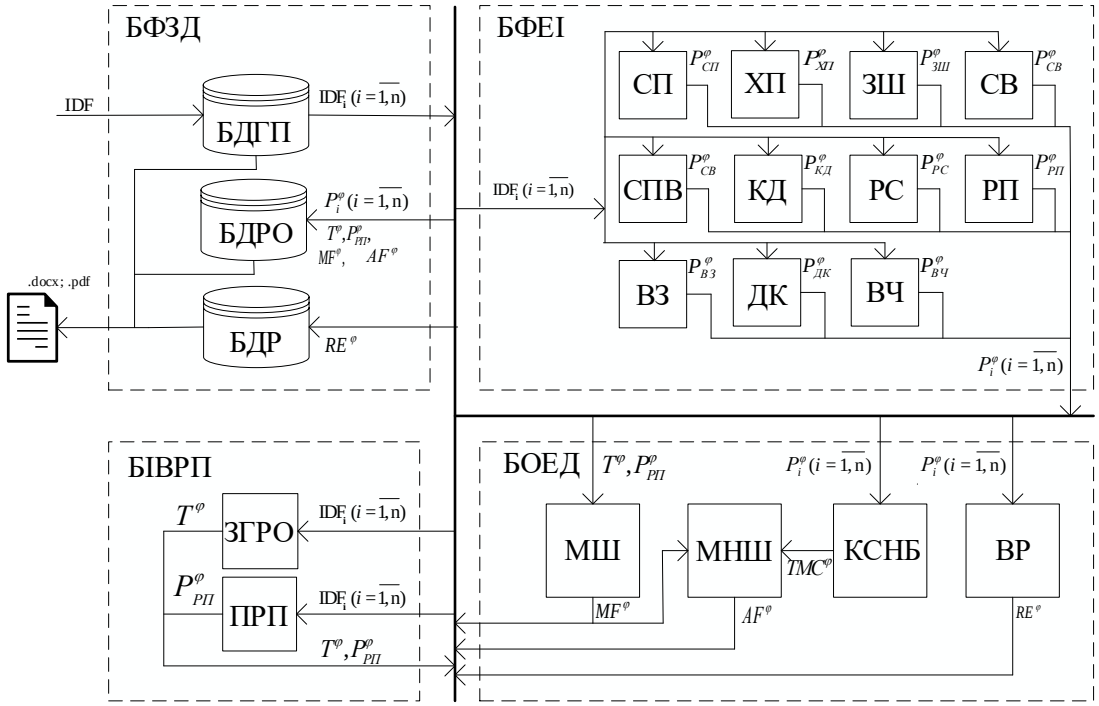

Рис.2. Структурна модель системи оцінки негативних наслідків втрати персональних даних

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 $P_{СП}^{\varphi}$, $P_{ХП}^{\varphi}$, $P_{ЗШ}^{\varphi}$, $P_{СВ}^{\varphi}$, $P_{РЦП}^{\varphi}$, $P_{РС}^{\varphi}$, $P_{КД}^{\varphi}$, $P_{СПВ}^{\varphi}$, $P_{ВЗ}^{\varphi}$, $P_{ДК}^{\varphi}$ та $P_{ВЧ}^{\varphi}$, що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства.

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) – 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.

В **4 розділі** проведено експериментальне дослідження розроблених засобів для оцінювання негативних наслідків від витоку персональних даних.

При *верифікації* розробленого *методу оцінювання негативних наслідків від порушення конфіденційності персональних даних* отримано результати, що показали високу чутливість методу до зміни вихідних параметрів, зокрема – рівня конфіденційності, періоду зберігання, виду інциденту, наявності реагування та ступеня шкоди. Завдяки бальній шкалі та грошовим еквівалентам метод обґрунтовує фінансові наслідки у форматі, придатному для бізнес-рішень і відповідає принципам прозорості GDPR. Результати підтверджують коректність роботи методу в різних контекстах, його адаптивність та можливість масштабування як частини автоматизованої системи управління ризиками.

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.

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 враховувати кореляційні зв’язки між подіями, що дозволяє уникнути

дублювання впливу інцидентів і надмірної оцінки. 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.

Рис.3. Алгоритм роботи системи

Розроблене *алгоритмічне та програмне забезпечення* (реалізована мовою C#) реалізує усі компоненти структурної моделі системи оцінки негативних наслідків втрати персональних даних відповідно до положень Регламенту GDPR. У стисненому вигляді алгоритм роботи системи представлено на рис. 3.

Ідентифікація порушення – введення базової інформації про підприємство, в якому стався інцидент.

Вибір рівня порушення – визначення порушеної статті Регламенту GDPR з автоматичним встановленням рівня порушення.

Оцінка вартості штрафу – проходження користувачем послідовності питань за одинадцятьма підпроцесами, кожен з яких охоплює окремий аспект інциденту; результати записуються для подальшої обробки.

Формування звіту – узагальнення введених даних і результатів оцінювання, розрахунок орієнтовної суми штрафу та генерація рекомендацій щодо усунення виявлених недоліків.

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 (рис. 4) показало 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.

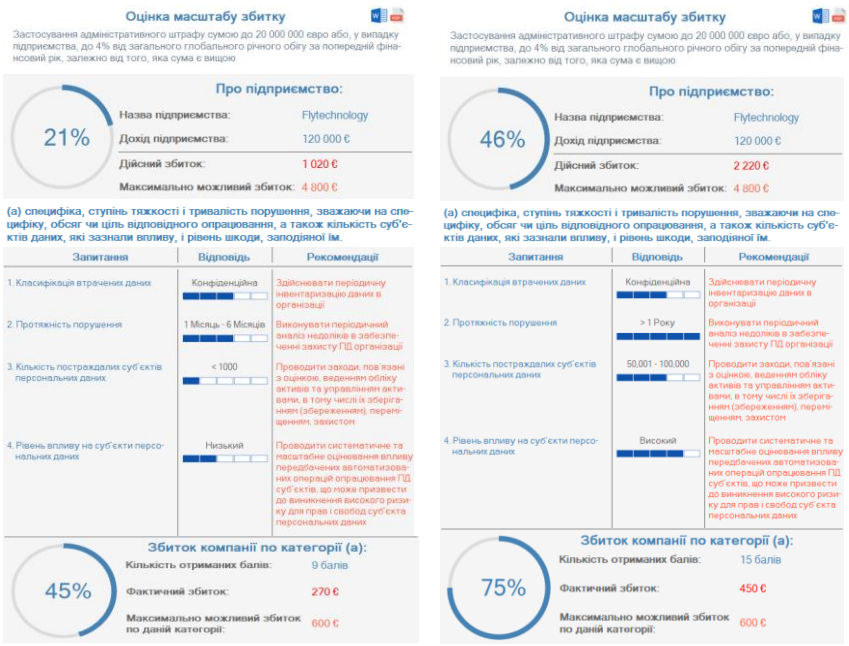

Рис 4. Результат верифікації розробленої системи

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Результатом виконаної роботи є вирішення важливої наукової 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 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. 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

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.

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.

Дисертаційна робота присвячена розробці нових методів і моделей оцінювання негативних наслідків від витоку персональних даних, що обумовлено зростанням кіберзагроз, вимогами GDPR та необхідністю підвищення ефективності управління інформаційною безпекою. У роботі розроблено теоретико-множинну та кортежну моделі параметрів персональних даних, які забезпечують формалізацію впливу окремих чинників на величину збитків у разі витоку, та слугують основою для побудови методів оцінювання ризику втрати персональних даних відповідно до вимог GDPR і національного законодавства. Розроблено метод оцінювання негативних наслідків від порушення конфіденційності персональних даних відповідно до положень Регламенту GDPR, який дозволяє визначати величину максимального та фактичного збитку для організації у разі витоку та метод оцінювання безпеки персональних даних, що забезпечує вибір політики захисту та послуг безпеки відповідно до функціонального профілю захищеності з урахуванням національного нормативно-правового забезпечення. Створено структурну модель автоматизованої системи оцінювання негативних наслідків від витоку персональних даних, алгоритмічне забезпечення та базу даних, яка інтегрує фактори відповідності GDPR. Проведено експериментальне дослідження на прикладах реальних інцидентів, яке підтвердило точність і практичну ефективність розробленої системи в умовах реального функціонування організацій, її здатність підтримувати прозору, кількісну та адаптивну оцінку втрат у сфері захисту персональних даних.

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 is devoted to the development of new models and methods for assessing the negative consequences of personal data breaches, driven by the growing cyber threats, GDPR requirements, and the need to improve information security management efficiency. The study proposes set-theoretic and tuple-based models of personal data parameters, which formalize the influence of various factors on the magnitude of losses in the event of a breach and serve as the basis for constructing risk assessment methods in accordance with GDPR and national regulations. A method for assessing the negative consequences of personal data confidentiality breaches is developed in compliance with the GDPR provisions, enabling the determination of maximum and actual losses to an organization in case of a data breach. Additionally, a method for assessing personal data security is proposed, which facilitates the selection of protection policies and security services based on the functional protection profile and national regulatory framework. A structural model of an automated system for assessing the negative consequences of personal data breaches was developed, along with algorithmic support and a database integrating GDPR compliance factors. Experimental research based on real incident scenarios confirmed the accuracy and practical efficiency of the proposed system under real organizational conditions, demonstrating its ability to provide transparent, quantitative, and adaptive loss assessment in the field of personal data protection.

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