Голові спеціалізованої вченої ради
Д 26.861.06 Державного
університету інформаційно-
комунікаційних технологій
вул. Солом'янська 7, м. Київ

ВІДГУК

офіційного опонента

завідувача кафедри захисту інформації Національного університету «Львівська політехніка», доктора технічних наук, професора Опірського Івана Романовича на дисертацію Лозової Ірини Леонідівни за темою «Моделі та методи оцінювання негативних наслідків від витоку персональних даних», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність теми. У сучасних умовах цифровізації та збільшення обсягів обробки персональних даних проблема забезпечення їх конфіденційності та безпеки є надзвичайно актуальною. Витоки даних призводять до порушення прав громадян, фінансових та репутаційних втрат для організацій, а в окремих випадках можуть становити загрозу національній безпеці. Незважаючи на наявність міжнародних стандартів, зокрема Регламенту ЄС GDPR, та українського законодавства, практично відсутні достатньо формалізовані та адаптивні моделі та методи оцінки негативних наслідків витоків даних у критично важливих інформаційних системах.

Дисертаційне дослідження робить важливий внесок у вирішення цієї проблеми, пропонуючи науково обґрунтовані моделі та методи оцінки збитків, що враховують правові, технічні, організаційні та соціальні аспекти функціонування інформаційних систем. Запропоновані підходи дозволяють оцінювати збитки у кількісному та якісному вимірах, що сприятиме підвищенню стійкості організацій до кіберзагроз, мінімізації економічних втрат та зміцненню національної інформаційної безпеки.

Оцінка обґрунтованості та достовірності наукових положень. Викладені в дисертації наукові положення, висновки та рекомендації є цілком обґрунтованими. Їх достовірність підтверджується експериментальними результатами та перевіркою запропонованих моделей і методів. Отримані дані експериментів узгоджуються з теоретичними висновками дослідження та повністю їх підтверджують, що свідчить про надійність і практичну значущість проведеної роботи.

Наукова новизна отриманих результатів дисертаційної роботи:

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.

4)

Практична значимість отриманих результатів дослідження. У дисертаційній роботі розроблено алгоритмічне забезпечення, яке реалізує структурну модель системи оцінювання негативних наслідків від витоку персональних даних відповідно до положень Регламенту GDPR. Створено інтегровану базу даних параметрів інцидентів та оціночних характеристик, що забезпечує збір, обробку, збереження та повторне використання інформації для оцінювання шкоди. Розроблене прикладне програмне забезпечення автоматизує процес оцінювання негативних наслідків витоків персональних даних, дозволяє моделювати інциденти, визначати ймовірні штрафні санкції, генерувати звіти та формувати рекомендації щодо підвищення рівня інформаційної безпеки та відповідності вимогам GDPR.

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).

Крім того, практична цінність результатів підтверджена актами впровадження в таких підприємствах, як 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.).

Значення результатів для науки та практики. Результати дисертаційного дослідження мають значну наукову та практичну цінність. Наукове значення полягає у розробці комплексних, теоретично обґрунтованих моделей і методів оцінювання негативних наслідків від витоку персональних даних, які інтегрують правові, технічні, організаційні та соціальні аспекти функціонування інформаційних систем. Запропоновані підходи дозволяють системно аналізувати інциденти, враховувати їх множинність та взаємозалежність, оцінювати рівень ризику та можливі наслідки у кількісному та якісному вимірах, що створює надійну наукову базу для подальших досліджень у галузі кібербезпеки та захисту персональних даних.

Практичне значення результатів дисертації підтверджується їх впровадженням у науково-дослідну діяльність та в реальні інформаційні системи. Розроблені алгоритми та прикладне програмне забезпечення дозволяють автоматизувати процес оцінювання негативних наслідків витоків даних, моделювати потенційні інциденти, визначати ймовірні штрафні санкції та формувати персоналізовані рекомендації для підвищення рівня інформаційної безпеки. Впровадження результатів у державні проекти та комерційні організації сприяє підвищенню стійкості інформаційних систем до кіберзагроз, мінімізації фінансових та репутаційних втрат, а також зміцненню відповідності законодавчим вимогам, що підкреслює їх високу практичну цінність і значущість для розвитку національної системи інформаційної безпеки.

Публікації та апробація результатів дисертаційної роботи. Результати дисертаційного дослідження висвітлено у 26 наукових працях. Зокрема, опубліковано 8 статей, серед яких 7 – у наукових фахових виданнях України, включених до Переліку, затвердженого МОН України, та 1 – у виданні, що індексується в наукометричній базі Scopus. Крім того, підготовлено три колективні монографії та отримано авторське свідоцтво на комп'ютерну програму. За матеріалами виступів на науково-технічних і науково-практичних конференціях опубліковано 14 публікацій, з яких дві індексуються в базі Scopus. Таким чином, результати дослідження пройшли належну апробацію у науковому середовищі.

Зміст та оформлення дисертаційної роботи. У дисертаційній роботі чітко дотримано структурної організації: вона містить вступ, чотири розділи, висновки, список використаних джерел (113 найменувань) та чотири додатки загальним обсягом 19 сторінок. Основний зміст дослідження викладено на 171 сторінці та проілюстровано 32 рисунками і 15 таблицями. Загальний обсяг дисертації становить 205 сторінок, що відповідає вимогам до обсягу наукового дослідження.

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** дисертаційної роботи узагальнено термінологічний апарат у сфері захисту персональних даних відповідно до чинного законодавства України та міжнародних нормативів, зокрема GDPR, визначено ключові поняття («персональні дані», «обробка», «володілець», «розпорядник») та проаналізовано нормативно-правову базу на національному та міжнародному рівнях, виявлено потребу вдосконалення українського законодавства та гармонізації його з GDPR. Проведено порівняльний аналіз методів, моделей та систем оцінювання втрат від витоку персональних даних, визначено їх переваги й недоліки, виявлено прогалини щодо комплексності, адаптивності та

програмної реалізації, а також окреслено необхідність розробки нових інтегрованих моделей і методів, що забезпечують кількісну та якісну оцінку ризиків і відповідають правовому полю ЄС.

У **другому розділі** дисертаційної роботи розроблено комплекс моделей для оцінювання ризиків, збитків і критичності інцидентів витоку персональних даних на рівні організацій та держави. Створено теоретико-множинну та кортежну моделі параметрів персональних даних, що враховують юридичні, технічні та організаційні аспекти обробки персональних даних, дозволяють формалізовано оцінювати ймовірність реалізації загроз, потенційні збитки та рівень необхідної безпеки. Розроблено ієрархічну структуру параметрів і модель критичності кризових ситуацій із врахуванням кореляції подій, що підвищує точність прогнозування та реагування на надзвичайні ситуації. Таким чином, у розділі сформовано інструментарій для аналітики у сфері захисту персональних даних, що має важливе значення для удосконалення політик безпеки, нормативно-правових підходів і систем оцінювання негативних наслідків витоків персональних даних.

У **третьому розділі** дисертаційної роботи запропоновано комплекс методів і систем для оцінювання ризиків, критичності та наслідків порушення конфіденційності персональних даних у сучасних інформаційних середовищах, зокрема соціокіберфізичних системах. Розроблено методи оцінювання негативних наслідків витоку персональних даних відповідно до вимог GDPR, оцінки безпеки персональних даних в автоматизованих системах на основі кортежної моделі та визначення рівня критичності інцидентів із застосуванням механізму кореляції подій. Запропоновано систему забезпечення безпеки персональних даних із багатоконтурною архітектурою, врахуванням гібридних загроз, соціальної інженерії та використанням постквантових криптографічних алгоритмів, а також структурну модель системи оцінювання негативних наслідків витоку даних. Отримані результати формують методологічну основу для побудови інформаційно-аналітичних і захисних систем, що дозволяють кількісно оцінювати ризики та збитки і формувати практичні рекомендації щодо зниження рівня загроз у сфері захисту персональних даних..

У **четвертому розділі** дисертаційної роботи проведено експериментальне дослідження запропонованих методів та систем оцінювання наслідків витоку персональних даних, що показало їх здатність точно оцінювати кількісні та якісні характеристики інцидентів, визначати ризики, обчислювати ймовірні штрафні санкції та критичність інцидентів з урахуванням кореляційних зв'язків. Розроблене програмне забезпечення реалізує структурну модель системи оцінювання негативних наслідків, дозволяє автоматизувати аналіз інцидентів і підтримує прийняття рішень у практичних сценаріях. Порівняння з існуючими міжнародними підходами свідчить про переваги системи: повну відповідність GDPR, наявність реалізації у вигляді програмного продукту, інтеграцію експертних та фактичних даних, комплексну оцінку фінансових, репутаційних та організаційних втрат, що підтверджує її високу практичну значущість та унікальність.

У **додатках** містяться документи про впровадження результатів дисертаційної роботи, які відображають практичну частину дисертаційного дослідження.

Зауваження щодо змісту та оформлення дисертації. Незважаючи на високий науковий та практичний рівень дослідження, у дисертаційній роботі виявлено деякі недоліки щодо змісту та оформлення:

1. У роботі наводяться основні положення GDPR та чинного українського законодавства щодо захисту персональних даних, проте відсутній детальний аналіз рішень судів та регуляторних органів (як в Україні, так і в ЄС), які вже розглядали кейси витоків даних і визначали розміри штрафів чи порядок відшкодування репутаційних втрат. Такий аналіз дав би змогу більш точно налаштувати алгоритми розрахунку збитків, зробив би модель більш практичною та наближеною до реальних умов правозастосування.

2. При розробці методу оцінювання негативних наслідків від порушення конфіденційності персональних даних авторкою не враховано ймовірні похибки прогнозу, які виникають через обмежену точність вихідних даних або суб'єктивність експертних оцінок. Відсутність довірчих інтервалів у результатах

робить неможливим оцінювання статистичної надійності прогнозу. Для підвищення достовірності результатів доцільно додати розрахунок похибок (наприклад, стандартне відхилення або інтервали довіри 95%) та провести аналіз чутливості моделі до зміни ключових параметрів.

3. Хоча в роботі наведено «акти впровадження» результатів дослідження, вони не містять чітких кількісних показників до і після використання розробленої моделі (наприклад, скорочення часу реагування на інциденти, зменшення середньої суми штрафів, підвищення точності прогнозу). Рекомендовано додати порівняльну статистику у вигляді таблиць і графіків, що продемонструють відсоткове поліпшення ключових метрик.

4. У дисертації немає окремого підрозділу, де були б чітко описані обмеження розробленого підходу: типи організацій, для яких він не підходить; ситуації, коли модель може давати некоректні результати; межі точності при відсутності повних даних. Такий підрозділ є важливим елементом будь-якого наукового дослідження, адже він дає змогу оцінити ризики неправильного використання результатів і визначити напрями подальшого вдосконалення.

5. Перевірка працездатності моделі проводилась переважно на вибірках середнього розміру, що відповідають даним окремих організацій. Проте у реальних умовах модель може застосовуватися як у малих компаніях (де обсяг даних незначний), так і в корпораціях чи державних реєстрах із мільйонами записів. Відсутність тестування на «екстремальних» обсягах даних створює ризик, що модель виявиться нестійкою або надто повільною у масштабованих середовищах. Рекомендовано провести додаткові експерименти із застосуванням великих синтетичних та реальних наборів даних, оцінити швидкодію та стабільність алгоритмів.

Зазначені зауваження не зменшують загальної позитивної оцінки дисертаційного дослідження.

Загальний висновок.

У цілому дисертаційна робота Лозової І.Л. є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні

результати, що у сукупності є суттєвими для розвитку теорії й практики наукової проблеми, пов'язаної з розробкою моделей і методів оцінювання негативних наслідків від витоку персональних даних.

Вважаю, що дисертаційна робота «Моделі та методи оцінювання негативних наслідків від витоку персональних даних» повністю відповідає вимогам МОН України, «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України № 567 від 24 липня 2013 року (із змінами, внесеними згідно з Постановами КМ № 656 від 19.08.2015 року № 1159 від 30.12.2015 року та № 567 від 27.07.2016 року) та «Порядку присудження та позбавлення наукового ступеня доктора наук» затвердженого Постановою Кабінету Міністрів України № 1197 від 17 листопада 2021 року, а її автор Лозова Ірина Леонідівна заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент:
доктор технічних наук, професор
завідувач кафедри захисту інформації
Національного університету «Львівська
політехніка» Іван ОПІРСЬКИЙ

Підпис д.т.н., професора Опірського І.Р. засвідчую
Вчений секретар Національного університету
«Львівська політехніка», к.т.н., доцент Роман БРИЛИНСЬКИЙ