ЗАТВЕРДЖУЮ

Ректор Державного університету інформаційно-комунікаційних технологій

_____ Володимир ШУЛЬГА

«18» червня 2025 року

ВИСНОВОК

міжкафедрального семінару кафедри Управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Лозової Ірини Леонідівни на тему: «Моделі та методи оцінювання негативних наслідків від витоку персональних даних», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»

Витяг

з протоколу № 15 засідання кафедри Управління кібербезпекою та захистом інформації
від “18” червня 2025 року

Присутні: Головуючий на засіданні – завідувач кафедри Управління кібербезпекою та захистом інформації, д.е.н., професор Легомінова Світлана Володимирівна.

З кафедри Управління кібербезпекою та захистом інформації:

професор кафедри – д.т.н., професор Савченко Віталій Анатолійович;
доцент кафедри – к.військ.н., доцент Якименко Юрій Михайлович;
доцент кафедри – к.т.н., доцент Щавінський Юрій Віталійович;
доцент кафедри – д.е.н., доцент Капелюшна Тетяна Вікторівна;
доцент кафедри – к.н.держ.упр., доцент Мужанова Тетяна Михайлівна;
доцент кафедри – к.т.н., Рабчун Дмитро Ігорович;
доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека Запорожченко Михайло Михайлович;
старший викладач кафедри – Тищенко Віталій Сергійович.

Запрошені:

- з кафедри Систем та технологій кібербезпеки:

завідувач кафедри – д.т.н., професор Гайдур Галина Іванівна;
професор кафедри – д.т.н., професор Кожухівський Андрій Дмитрович;
доцент кафедри – к.військ.н., доцент Гахов Сергій Олександрович;
доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека Марченко Віталій Вікторович;

- з кафедри Технічних систем кіберзахисту:

завідувач кафедри – д.т.н., професор Туровський Олександр Леонідович;
професор кафедри – к.т.н., доцент Пепа Юрій Володимирович;
доцент кафедри – к.т.н., доцент Котенко Андрій Миколайович;

- з кафедри Комп'ютерних наук:

завідувач кафедри – д.т.н., професор Вишнівський Віктор Вікторович.

Директор Навчально-наукового інституту кібербезпеки та захисту інформації – д.т.н., професор Іванченко Євгенія Вікторівна;

Перший проректор Державного університету інформаційно-комунікаційних технологій – д.т.н., професор Корченко Олександр Григорович.

Всього присутніх – 19 осіб. Серед присутніх 7 докторів технічних наук та 6 кандидатів технічних наук.

ПОРЯДОК ДЕННИЙ:

Обговорення дисертаційної роботи Лозової Ірини Леонідівни на тему: «Моделі та методи оцінювання негативних наслідків від витоку персональних даних», поданої на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

Дисертація виконана в Державному університеті інформаційно-комунікаційних технологій. Тема дисертаційної роботи затверджена в остаточній редакції на засіданні Вченої ради Державного університету інформаційно-комунікаційних технологій (протокол № 8 від 17.06.2025 р.), науковий керівник – доктор технічних наук, професор Корченко Олександр Григорович (наказ ректора Національного авіаційного університету № 1234/ст від 18.05.2007 року).

СЛУХАЛИ: доповідь про дисертаційну роботу Лозової Ірини Леонідівни на тему «Моделі та методи оцінювання негативних наслідків від витоку персональних даних», подану на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

ЛОЗОВА І.Л.: Шановні Голово, члени міжкафедрального семінару, присутні! Вашій увазі пропонується доповідь за дисертаційною роботою на тему: «Моделі та методи оцінювання негативних наслідків від витоку персональних даних».

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.

Метою 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.

Об'єктом дослідження є процес оцінювання негативних наслідків від витоку персональних даних.

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

Основними завданнями дослідження є: аналіз вітчизняного та міжнародного нормативно-правового забезпечення у сфері захисту персональних даних, а також існуючих методів, моделей та систем оцінювання можливих негативних наслідків їх витоку чи втрати; розробка моделі інтегрованого представлення параметрів збитків, спричинених витоком персональних даних, відповідно до вимог чинного українського законодавства та положень Регламенту ЄС GDPR; розробка 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; розробка структурної моделі системи оцінювання негативних наслідків від витоку персональних даних, що відповідає принципам і положенням Регламенту GDPR, та забезпечує врахування юридичних, технічних і організаційних чинників; розробка алгоритмічного та програмного забезпечення реалізації структурної моделі системи оцінювання негативних наслідків від витоку персональних даних для автоматизації відповідного процесу оцінювання, а також проведення експериментального дослідження з

метою підтвердження достовірності теоретичних розробок і практичної ефективності запропонованих рішень.

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 запропонованого підходу полягає у:

– 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.).

Таким чином, у дисертаційній роботі вирішено важливу наукову проблему, пов'язану 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. 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

Доповідь закінчено. Дякую за увагу!

По завершенню доповіді Лозовій Ірині Леонідівні присутніми були поставлені наступні запитання:

1. Які відомі вітчизняні та зарубіжні науковці досліджували проблему

оцінювання негативних наслідків витоку персональних даних, і які підходи вони пропонували?

2. Чи передбачено у моделі врахування зовнішніх нормативних і регуляторних змін (зокрема, оновлень GDPR) при оцінюванні ризиків та штрафних санкцій?

3. Яким чином у запропонованій моделі враховується вплив категорій та обсягів зкомпрометованих персональних даних на підсумкову оцінку збитку?

4. Чи здатне розроблене програмне забезпечення розраховувати розмір штрафів, співставний з тими, що були фактично накладені відповідно до Регламенту GDPR на реальні компанії?

5. Чи застосовуються у розробленій системі методи штучного інтелекту для підтримки процесу прийняття рішень під час оцінювання негативних наслідків витоку персональних даних?

6. На якому етапі розробленого алгоритму відбувається експертне оцінювання, які параметри при цьому?

7. Які основні етапи необхідно виконати для впровадження розробленої системи оцінювання у реальні корпоративні IT-інфраструктури?

8. Як у межах моделі враховується рівень інформаційної безпеки організації та її відповідність внутрішнім і міжнародним стандартам?

9. Які основні обмеження та можливі напрями подальшого удосконалення запропонованого методу оцінювання негативних наслідків від витоку персональних даних?

10. Яким чином у запропонованій моделі враховується вплив категорій та обсягів зкомпрометованих персональних даних на підсумкову оцінку збитку?

11. Яким пунктам паспорту спеціальності 05.13.21 «Системи захисту інформації» відповідає виконана дисертаційна робота та як саме реалізовано цю відповідність у наукових результатах?

На всі питання були дані вичерпні відповіді.

СЛУХАЛИ: відгук наукового керівника доктора технічних наук, професора, член-кореспондента НАН України, лауреата Державної премії України в галузі науки і техніки, Заслуженого діяча науки і техніки України першого проректора Державного університету інформаційно-комунікаційних технологій Корченка Олександра Григоровича про дисертаційну роботу Лозової Ірини Леонідівни на тему: «Моделі та методи оцінювання негативних наслідків від витоку персональних даних», подану на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

КОРЧЕНКО О.Г.: У процесі підготовки дисертації Лозова Ірина Леонідівна проявила себе як самостійний, наполегливий, відповідальний і високоерудований науковець, здатний формулювати та ефективно вирішувати складні наукові завдання. Вона володіє сучасними методами наукових досліджень, інструментами математичного моделювання, аналітичними підходами, а також комунікаційними та іншими професійними компетентностями, що дають змогу логічно й послідовно представляти результати власних досліджень, публікувати їх у вітчизняних та міжнародних

наукових виданнях, брати активну участь у наукових дискусіях, аргументовано обґрунтовуючи та відстоюючи власні наукові досягнення..

Автором дослідження коректно визначено мету, завдання, об'єкт і предмет дослідження. У процесі виконання дисертаційної роботи ефективно застосовано теоретико-множинний підхід, теорію нечіткої логіки, прийняття рішень, алгоритмів, алгебри логіки, методи експертного оцінювання, моделювання інформаційних процесів і структур та операції нечіткої арифметики. Такий підхід забезпечив не лише формулювання та теоретичне обґрунтування наукової новизни отриманих результатів, а й їх практичну реалізацію, що визначило значущість дослідження для розв'язання проблеми оцінювання негативних наслідків витоку персональних даних та підвищення рівня інформаційної безпеки організацій.

У ході виконання дисертаційної роботи автором досягнуто мети роботи – розроблено моделі та методи 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. Отримані результати мають важливе практичне значення для спеціалістів у галузі кібербезпеки, інформаційної безпеки, аудиту інформаційних систем, а також можуть бути використані у процесі навчання та підготовки кадрів з питань захисту персональних даних.

За результатами дисертаційних досліджень опубліковано 26 наукових праць. Опубліковано статей – 8, з яких 7 статей – у наукових фахових виданнях України з Переліку, затвердженого МОН України, 1 стаття у наукових виданнях Scopus, три колективні монографії та авторське свідоцтво на комп'ютерну програму. За матеріалами виступів на науково-технічних та науково-практичних конференціях опубліковано 14 публікацій, серед яких дві публікації проіндексовано в наукометричній базі Scopus.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. З наукових праць, які опубліковані у співавторстві, використано лише ті положення, ідеї та висновки, які є результатом власного дослідження здобувача.

Робота є самостійно виконаним науковим дослідженням, що відповідає принципам академічної доброчесності та не містить некоректних запозичень. Вона повністю відповідає спеціальності 05.13.21 «Системи захисту інформації», за якою подається до захисту.

Дисертаційна робота Лозової Ірини Леонідівни є завершеним науковим дослідженням, яке здійснює вагомий внесок у розвиток теоретичних і прикладних аспектів інформаційної безпеки, зокрема у сфері захисту персональних даних. Запропоновані автором науково-методичні підходи сприяють удосконаленню механізмів оцінки ризиків, сприяють зниженню ймовірності повторних інцидентів та забезпечують стійкість організацій до загроз, пов'язаних із витоком персональних даних. Дослідження виконане на високому науковому рівні, підтверджує наукову зрілість, ґрунтовну підготовку та високу компетентність здобувача в галузі кібербезпеки.

Вважаю, що дисертаційна робота повністю готова до захисту, а її автор заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

Призначені рецензенти:

Д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки Гайдур Галина Іванівна; к.т.н., доцент кафедри Управління кібербезпекою та захистом інформації Рабчун Дмитро Ігорович загалом позитивно оцінили дисертаційну роботу, відзначивши її високу актуальність, теоретичну значущість та практичну цінність. Особливу увагу було приділено науковій новизні, обґрунтованості результатів і систематизованому підходу до вирішення поставленої проблеми.

Зокрема, **доктор технічних наук, професор, завідувач кафедри Систем та технологій кібербезпеки Гайдур Г.І.** відзначила високий науковий рівень дисертаційної роботи Лозової Ірини Леонідівни та її актуальність у контексті сучасних викликів кібербезпеки.

Загальний аналіз дисертації дозволив зробити наступні висновки:

1. Ознайомлення зі змістом дисертаційної роботи підтверджує логічність її побудови, чіткість наукової аргументації, а також обґрунтованість висновків і рекомендацій, сформульованих автором самостійно.

2. Структура роботи відповідає визначеній меті та поставленому науковому завданню. Дисертація ґрунтується на положеннях інформаційної безпеки, теоретико-множинному підході, теоріях нечіткої логіки, прийняття рішень, алгоритмів, алгебри логіки, методах експертного оцінювання, моделювання інформаційних процесів і структур та операціях нечіткої арифметики, що забезпечує її теоретичну глибину. Актуальність дослідження підтверджується проведеним аналізом сучасного вітчизняного та міжнародного нормативно-правового забезпечення у сфері захисту персональних даних, а також існуючих методів, моделей та систем оцінювання можливих негативних наслідків їх витоку чи втрати.

3. Автором сформульовано оригінальні наукові положення, що стосуються розробки моделей і методів оцінювання негативних наслідків витоку персональних даних та формалізації параметрів інцидентів відповідно до вимог Регламенту GDPR. Отримані результати мають значний практичний потенціал для зниження ризиків витоку даних, мінімізації фінансових та репутаційних втрат організацій і підвищення їх відповідності міжнародним стандартам захисту персональних даних.

4. Дисертаційне дослідження є самостійною науковою працею, що не містить некоректних запозичень. Опубліковані результати досліджень відображають основні положення наукової новизни та відповідають вимогам до дисертацій за спеціальністю 05.13.21 «Системи захисту інформації».

Позитивно оцінюючи положення дисертаційного дослідження Лозової І.Л., **Гайдур Г.І.** звернула увагу на певні аспекти, що можуть бути уточнені або розширені:

1. У роботі ґрунтовно розглянуто нормативно-правове забезпечення,

моделі методи та системи оцінювання негативних наслідків витоку персональних даних, однак варто було б ширше висвітлити питання інтеграції розроблених моделей із сучасними міжнародними платформами моніторингу кіберзагроз та системами реагування на інциденти.

2. Запропоновані моделі та методи продемонстрували високу ефективність у рамках проведених експериментальних досліджень, проте потребує детальнішого розгляду питання масштабованості та продуктивності розробленого програмного забезпечення при обробці великої кількості інцидентів у реальному часі, зокрема для державних та транснаціональних організацій.

3. Значна увага у роботі приділена формалізації параметрів оцінювання збитків, але перспективним є подальший розвиток напрямку прогнозування наслідків витоків на основі методів машинного навчання та аналізу великих даних, що могло б підвищити точність та адаптивність системи.

Наведені зауваження стосуються переважно питань подальшого розвитку дослідження та не впливають на його загальну наукову й практичну значущість. Робота є завершеним науковим дослідженням, що робить вагомий внесок у розвиток методів та моделей оцінювання негативних наслідків витоку персональних даних і підвищення рівня інформаційної безпеки організацій. За рівнем наукової аргументації, методологічного підходу та практичної значущості висновків, дисертація відповідає вимогам, які висуваються до досліджень на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Робота виконана державною мовою, *з дотриманням норм та правил академічної доброчесності.*

Кандидат технічних наук, доцент кафедри Управління кібербезпекою та захистом інформації Рабчун Дмитро Ігорович охарактеризував дисертаційну роботу як ґрунтовне наукове дослідження високого рівня, що відображає актуальні виклики у сфері кібербезпеки, зокрема проблему оцінювання негативних наслідків від витоку персональних даних. Робота містить чітке теоретичне обґрунтування, новітні підходи до аналізу загроз та практичні рекомендації щодо їх мінімізації. Наукові результати дослідження мають важливе значення для подальшого розвитку систем інформаційної безпеки та практичного застосування в кіберзахисті організацій різного рівня.

Разом із позитивною оцінкою дисертації, рецензент висловив окремі зауваження та наголосив на деяких аспектах, що можуть бути предметом подальшого дослідження:

1. Запропоновані алгоритми продемонстрували ефективність у тестових сценаріях, однак потребує дослідження їх стійкість та точність у випадку неповних або суперечливих вхідних даних, що часто трапляється під час реальних кіберінцидентів.

2. Було б корисно доповнити дослідження економічним аналізом впровадження розроблених методів, включно з оцінкою вартості їх інтеграції та потенційної окупності для підприємств різного масштабу.

3. Запропонована структурна модель системи оцінювання негативних наслідків від витоку персональних даних має високий потенціал для

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.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлені власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані дисертантом особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. У роботах, опублікованих у співавторстві, автором: досліджено та проведено порівняльний аналіз стратегій кібербезпеки, розроблено рекомендації щодо удосконалення нормативно-правової бази; проведено аналіз поняття «кризова ситуація», сформовано підходи до класифікації кризових ситуацій; розроблено етапи моделі та проведено обрахунок методу; формалізовано механізм кореляції інцидентів, розроблено підходи до визначення рівня критичності кризової ситуації; розроблено теоретико-множинну GDPR-модель, описано структуру параметрів персональних даних; розроблено основні етапи методу оцінювання негативних наслідків від порушення конфіденційності персональних даних; розроблено структуру моделі системи оцінки негативних наслідків втрати персональних даних, визначено її основні компоненти; розроблено етап 5, модифікація механізмів послуг безпеки в багатоконтурній системі захисту інформації (інтеграція постквантових алгоритмів); проведено аналіз та узагальнення чинних нормативно-правових документів України та ЄС у сфері захисту персональних даних; розроблено алгоритмічне забезпечення системи оцінки негативних наслідків втрати персональних даних; визначено множини ознак для оцінки засобів оцінювання збитків від втрати персональних даних; досліджено та проведено порівняльний аналіз архітектури хмарних сервісів;

автоматизації, але перспективним є дослідження можливостей її адаптації для роботи в умовах хмарних середовищ та мультихмарної інфраструктури, де ризики та механізми захисту мають специфічні особливості.

Загалом, рецензована робота підготовлена на високому науковому рівні, вирізняється достатнім рівнем наукової новизни, теоретичною та практичною цінністю отриманих результатів, виконана *з дотриманням норм та правил академічної доброчесності*. Це дає підстави оцінити її позитивно та рекомендувати до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації».

Рецензентами відзначено, що дисертаційна робота відповідає встановленим вимогам щодо наукової новизни, теоретичної та практичної значущості, а також може бути рекомендована до спеціалізованої вченої ради для попереднього розгляду та захисту на здобуття наукового ступеня кандидата технічних наук.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Лозової Ірини Леонідівни на тему «Моделі та методи оцінювання негативних наслідків від витоку персональних даних», поданої на здобуття ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»

Актуальність теми дослідження. 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.

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, грантами.

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 завдання дослідження.

Метою дослідження 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 автором виконано наступні *окремі завдання дослідження*:

– проаналізовано 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.

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

– розроблено 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.

– розроблено 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.

– розроблено 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 дослідження:

– *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. Практичне значення одержаних результатів 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

досліджено та проведено аналіз існуючих типів сучасних баз даних і систем їх управління; проведено аналіз засобів оцінювання шкоди від втрати інформації з обмеженим доступом; сформульовано параметр «Рівень порушення», описано його множинне представлення; обґрунтовано логічний підхід до представлення параметрів; представлено параметри «Специфіка порушення» та «Характер порушення» з використанням теоретико-множинних підходів; розроблено програмну модель оцінки негативних наслідків від витоку персональних даних; визначено вхідні та вихідні параметри моделі оцінювання негативних наслідків витоку персональних даних.

Апробація результатів дослідження.

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. За результатами дисертаційних досліджень опубліковано 26 наукових праць. Опубліковано статей – 8, з яких 7 статей – у наукових фахових виданнях України з Переліку, затвердженого МОН України, 1 стаття у наукових виданнях Scopus, три колективні монографії та авторське свідоцтво на комп'ютерну програму. За матеріалами виступів на науково-технічних та науково-практичних конференціях опубліковано 14 публікацій, серед яких дві публікації проіндексовано в наукометричній базі Scopus.

Список опублікованих праць за темою дисертації

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. 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

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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.

8. 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.

9. 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

10. 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

11. 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

12. 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

13. 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.

14. 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.

Наукові праці, які додатково відображають наукові результати дисертації:

1. 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/

Структура та обсяг дисертації.

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 сторінках, рисунків – 32, таблиць – 15. Загальний обсяг роботи становить 205 сторінок.

Характеристика особистості здобувача.

Лозова Ірина Леонідівна у 2005 році закінчила Національний авіаційний університет та отримала диплом Спеціаліста за спеціальністю «Захист інформації з обмеженим доступом та автоматизація її обробки». У 2007 році вступила до аспірантури Національного авіаційного університету, м. Київ, Україна, за спеціальністю 05.13.21 «Системи захисту інформації».

Під час виконання дисертаційної роботи Лозова І.Л. провела ґрунтовне дослідження, спрямоване на аналіз сучасного стану проблематики, заявленої у дисертації. Було чітко визначено об'єкт, предмет, мету та завдання дослідження, обґрунтовано актуальність теми та обрано відповідні методи для досягнення поставлених цілей. Здобувачка Ірина Лозова приймала безпосередню участь під час постановки наукових завдань, планування та виконання експериментів, а також обговорення отриманих результатів. Проявила себе як відповідальна, дисциплінована та ініціативна дослідниця, здатна працювати як самостійно, так і в команді. Продемонструвала високий рівень теоретичної підготовки, володіє сучасними методами дослідження, аналітичними інструментами та практичними навичками. Системно підходить до вирішення наукових завдань, критично оцінює результати власної роботи, виявляє наполегливість у досягненні поставлених цілей. Постійно вдосконалює свої знання, прагнучи підвищити рівень наукової обґрунтованості та практичної значущості отриманих результатів.

Оцінка мови та стилю дисертації. Дисертація виконана фаховою українською мовою, текстове подання матеріалу відповідає стилю науково-дослідної літератури.

У результаті попередньої експертизи дисертації **Лозової Ірини Леонідівни** і повноти публікації основних результатів дослідження.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Лозової Ірини Леонідівни на тему «Моделі та методи оцінювання негативних наслідків від витоку персональних даних».
2. Констатувати, що за актуальністю, степенем наукової новизни, обґрунтованістю, теоретичною та практичною цінністю здобутих результатів дисертація Лозової І.Л. відповідає спеціальності 05.13.21 «Системи захисту інформації» та вимогам постанови Кабінету Міністрів України від 23 березня 2016 року № 261 «Про затвердження порядку підготовки здобувачів вищої освіти

ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», постанови Кабінету Міністрів України від 17 листопада 2021 року № 1197 «Деякі питання присудження (позбавлення) наукових ступенів» та наказу Міністерства освіти і науки України від 23 вересня 2019 року № 1120 «Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук» та паспорту спеціальності 05.13.21 – «Системи захисту інформації».

3. Рекомендувати дисертацію Лозової І.Л. на тему «Моделі та методи оцінювання негативних наслідків від витоку персональних даних» до захисту на здобуття ступеня кандидата технічних наук у спеціалізованій вченій раді Д 26.861.06 за спеціальністю 05.13.21 «Системи захисту інформації».

Результати голосування щодо рекомендації до захисту дисертації Лозової Ірини Леонідівни:

"За" – 19

"Проти" – немає

"Утримались" – немає

Головуючий на засіданні –
д.е.н., професор, завідувач кафедри
Управління кібербезпекою та захистом
інформації Світлана ЛЕГОМІНОВА

Секретар засідання Михайло ЗАПОРОЖЧЕНКО