ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

Вілігури Владислава Вікторовича

«Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень»,

яка подається на здобуття наукового ступеня доктора філософії

з галузі знань 12 – Інформаційні технології

за спеціальністю 125 – Кібербезпека та захист інформації

1. Оцінка роботи здобувача у процесі підготовки дисертації і виконання індивідуального плану навчальної та наукової роботи.

Здобувач Вілігура Владислав Вікторович виконав у повному обсязі Індивідуальний план виконання освітньо-наукової програми підготовки доктора філософії. Освітня програма в обсязі 40 кредитів ECTS виконана у повному об'ємі. Він успішно склав наступні дисципліни:

- залік з навчальної дисципліни «Філософські засади та методологія наукових досліджень» (81 бал);

- іспит з навчальної дисципліни «Іноземна мова для аспірантів (англійська)» (94 бали);

- залік з навчальної дисципліни «Підготовка наукових публікацій та презентація результатів досліджень» (92 бали);

- залік з навчальної дисципліни «Реєстрація прав інтелектуальної власності» (90 балів);

- іспит з навчальної дисципліни «Математичні методи в кібербезпеці» (91 бал);

- іспит з навчальної дисципліни «Математичні методи синтезу та аналізу криптографічних примітивів» (92 бали);

- залік з навчальної дисципліни «Моделі і методи комп'ютерної стеганографії» (93 бали);

Всі заплановані види робіт були виконані своєчасно. Здобувач плідно співпрацював з науковим керівником протягом усього терміну навчання.

2. Обґрунтування вибору теми дослідження.

У сучасному світі інформація перетворилася на один з найважливіших ресурсів суспільства, а інформаційні системи (ІС), основним функціональним компонентом яких є бази даних (БД), стали необхідним інструментом практично у всіх сферах діяльності людини, надаючи їй достовірну інформацію для прийняття оптимального рішення. При цьому вдосконалення технологій баз даних це напрям, що динамічно розвивається, дослідження в якому не припиняються, а ведуться з наростаючою інтенсивністю, так як з часом змінюються середовища та умови функціонування систем баз даних, удосконалюються апаратні засоби та засоби програмування, з'являються нові сфери застосунків, змінюються їх характер та вимоги. Зростання Великих Даних (Big Data) та бачення світу, керованого даними, відкривають багато цікавих можливостей, одночасно виявляючи безліч невирішених проблем. У тому числі, нова епоха Big Data, що залучила багатьох дослідників у «гру управління даними» і змусила відмовитися від звичних способів проектування, розробки та впровадження рішень управління даними, загострила проблему безпеки даних. Так як зріс інтерес до інформації, що циркулює всередині ІС, не тільки з боку законних користувачів і власників, але і з боку зловмисників. Для останніх бази, сховища даних, як найважливіший інформаційний ресурс, є одним із найуразливіших і найпривабливіших елементів ІС.

Усе це змушує шукати нові підходи ефективного вирішення новостворених і традиційних проблем. Проведені дослідження актуального стану інформатизації у різних компаніях, організаціях, установах свідчать, що у багатьох із них сьогодні експлуатуються різнопланові інформаційні системи організаційного управління (ІСОУ), призначені для автоматизації функцій управлінського персоналу, як промислових підприємств, так і непромислових організацій. При цьому для вирішення нових завдань, пов'язаних з розширенням сфери діяльності та, відповідно, предметних областей (ПрО), у них виникає потреба у більш функціональних, з покращеними характеристиками якості

інформаційних систем, у тому числі, що забезпечують високі вимоги безпеки даних, що зберігаються, та в сукупності, що вимагають менших витрат на супровід. У цих умовах затребуваними стають проекти з розробки нових ІСОУ та їх інтеграції з інформаційними системами, що існують; з розробки нових ІСОУ з метою заміни існуючих ІС; модернізації існуючих ІСОУ. Суть даних проектів полягає у систематичній трансформації існуючої системи – проведенні процедур реінжинірингу існуючих ІС та їх основного функціонального компонента – бази даних. При цьому однією з важливих вимог, що висуваються до процесу реінжинірингу існуючих ІСОУ та їх баз даних, є своєчасність завершення відповідних проектів з інформаційних технологій (ІТ) у рамках запланованого бюджету із заданими характеристиками якості. Проте, як свідчать результати аналізу ІТ-проектів, багато проектів було провалено або завершено із запізненням, причому з набагато більшими витратами, ніж планувалося. Це, як правило, пов'язане з обмеженістю функціональності відповідних методів проектування. У контексті баз даних, конкретніше реляційних баз даних (РБД), як тих, що отримали найбільше поширення, зазначена обмеженість обумовлена орієнтацією традиційної методології їх проектування на ітераційну, досить складну та трудомістку процедуру створення унікальних концептуальної моделі, логічної та фізичної схем при розробці нової БД, або на істотне їх перетворення при модернізації. Що часто спричиняє значні, не завжди прогнозовані об'єктивні витрати часових та фінансових ресурсів. У зв'язку з чим для вирішення цієї проблеми в окремих роботах було методологічно обґрунтовано та запропоновано використання баз даних, побудованих на основі схеми з універсальним базисом відношень. Однак, хоча в частині цих робіт і були порушені питання присвячені необхідності забезпечення безпеки даних, що зберігаються в ній, але глибокого опрацювання ця проблема в них не отримала. На сучасному етапі розвитку теорії та практики забезпечення безпеки інформації, у тому числі в базах та сховищах даних, склалася суперечлива ситуація, коли з одного боку є підвищена увага до цих питань, що виражається: 1) у виконанні великої наукової та практичної роботи зі створення, організації та дослідження процесів функціонування, удосконалення та розвитку систем захисту інформації, що була проведена і тієї,

що проводиться сьогодні вітчизняними та зарубіжними вченими; 2) у постійному зростанні асигнувань на забезпечення захисту; 3) у прийнятті великої кількості різних міжнародних, вітчизняних стандартів та інших законодавчих актів у галузі інформаційної безпеки (ІБ), що передбачають високі вимоги до захисту інформації (ЗІ) в інформаційних системах, що створюються та експлуатуються, та штрафи за їх невиконання. Що в цілому має покращити ситуацію із захищеністю ІС та їх основного функціонального компонента – БД.

З іншого боку, спостерігається постійне зростання завданих власникам інформаційних ресурсів збитків (тобто дія породжує протидію), про що свідчать дані, що регулярно публікуються авторитетними експертами. Найбільшу небезпеку для даних становить зростаюча кількість інцидентів: від кібератак до втрати даних та простою систем. Зловмисники продовжують удосконалювати шкідливе програмне забезпечення (ПЗ) і виводять його на нові рівні складності та сили ураження. Зростаючі можливості кібер-злочинних груп, що використовують нові техніки злому, а також складність виявлення таких проникнень звичайними засобами викликає серйозну занепокоєність у департаментах ІТ-безпеки. Ця проблема посилюється, до того ж, гострою нестачею кваліфікованих спеціалістів з питань безпеки.

З усього вищевказаного стає очевидним, що сучасні підходи до забезпечення безпеки інформації не повною мірою відповідають відповідним вимогам щодо її захисту. Зокрема, без необхідного захисту баз і сховищ даних, разом із відповідними чутливими даними, нові інформаційні технології здатні порушити як приватне життя людей, а й діяльність різних великих організацій.

У ситуації, що склалася, беручи до уваги сучасний стан розвитку технологій баз, сховищ даних, у тому числі побудованих на основі схеми з універсальним базисом відношень, науково-практичні досягнення в галузі ІБ, кваліфікацію зловмисників, які постійно вдосконалюють можливості відповідного впливу за допомогою шкідливого програмного забезпечення, положення та рекомендації різних нормативно-правових актів, доцільним є перегляд підходу до вирішення проблеми управління даними та забезпечення їх

безпеки, результатом якого були певні методи, прийоми, засоби, актуальні як у теоретичному, так і в прикладному аспектах.

При цьому, доцільність досліджень саме баз даних з універсальним базисом відношень (УББВ) обумовлена тим, що, по-перше, це дозволить переконатися в безпеці даних, що зберігаються і оброблюються в них, а також показати певні переваги в захищеності таких БД перед традиційними реляційними базами даних ІСОУ. По-друге, на їх прикладі, через те, що бази даних з УББВ можуть використовуватися в різній якості – як звичайна БД, сховище даних різних предметних областей (ПрО) або конфігураційна БД середовища управління простором даних, застосовуючи певні нові підходи, стає можливою розробка деякого цілісного рішення, що забезпечує безпеку реляційних баз даних. Окремі елементи такого рішення можуть бути використані для захисту баз та сховищ даних із різними моделями (реляційними, NoSQL, NewSQL). Все вищенаведене дозволяє зробити висновок про актуальність і своєчасність рішення науково-прикладного завдання, яке полягає в розробці та застосуванні моделей, методів і засобів, що дозволяють підвищити захищеність баз даних, побудованих на основі схеми з універсальним базисом відношень.

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення ефективності захисту баз даних, побудованих на основі схеми з універсальним базисом відношень, шляхом розробки та застосування моделей, методів та засобів забезпечення їхньої безпеки.

Основні завдання дисертаційного дослідження:

1. Аналіз сучасного стану та основних проблем забезпечення безпеки баз даних. Обґрунтування напряму досліджень.

2. Розробка та обґрунтування моделі захисту бази даних на основі системи безпеки з повним перекриттям та методу оцінки безпеки БД.

3. Розробка та обґрунтування методів маскування даних, що дозволяють зменшити ймовірність реалізації загрози логічного висновку та приховати код критично важливих модулів, що постійно зберігаються.

4. Розробка та обґрунтування методу контролю цілісності та справжності модулів, що постійно зберігаються, заснованого на можливостях технології блокчейн.

5. Обґрунтування та систематизація реалізованих заходів захисту, що забезпечують конфіденційність, цілісність даних та постійно збережених модулів баз даних з універсальним базисом відношень.

6. Оцінка безпеки бази даних із універсальним базисом відношень.

Об'єкт та предмет дослідження.

Об'єкт дослідження – процес забезпечення безпеки баз даних в умовах реалізації різних типів загроз.

Предмет дослідження – моделі та методи управління доступом, забезпечення конфіденційності, цілісності та справжності даних, що зберігаються в базах даних з універсальним базисом відношень.

Методи дослідження.

Методи досліджень визначені сутністю розв'язуваних задач і включають основні положення теорії множин, у тому числі нечітких, теорії графів, баз даних, розділи сучасної криптографії, методи математичної логіки та статистики, методи маскування, що знайшли застосування у певних класах завдань із приховування інформації в базах та сховищах даних, сучасний варіант алгоритму тасування Фішера-Йейтса, методи верифікації блоків даних у сучасній блокчейновій моделі.

3. Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційні дослідження проводились в рамках науково-дослідницьких робіт: No 39-18 «Механізми, методи, протоколи та засоби криптографічного захисту інформації у пост квантовий період» (Шифр «Квант-2019»), No 29-19 «Механізми та засоби електронного підпису у пост квантовий період», (Шифр «Квант-2020»), No 28-20 «Механізми та засоби асиметричних криптоперетворень у постквантовий період» (Шифр «Квант-2021»), «Математичні та програмні моделі, методи та механізми криптографічного захисту інформації для пост- квантового середовища в інтересах національної безпеки держави» (No ДР 0121U109939), No 34-21 «Методи та алгоритми

постквантових криптоперетворень, їх стандартизація та впровадження» (Шифр «Квант-2022»), No 09-22 «Методи та засоби генерування псевдовипадкових та випадкових послідовностей на основі класичних та квантових ефектів» (Шифр «Квант-2023»).

4. Особистий внесок дисертанта в отриманні наукових результатів та їх новизна.

Особистий внесок дисертанта в отриманні наукових результатів та їх новизна полягає у наступному:

1. Вперше запропоновано метод моніторингу збережених програм, що ґрунтується на можливостях технології блокчейн, який на відміну від відомих дозволяє за рахунок використання створеної зумовленої структури, правил формування первинного та наступних блоків у блокчейновому ланцюжку, організації зберігання цієї структури в рамках реляційної моделі даних, способів обчислення кореня геш-дерева, суворо контролювати набір програм БД, їх цілісність, справжність при менших обсягах збережених для цього даних і необхідних ресурсів процесора.

2. Удосконалено:

– модель системи безпеки з повним перекриттям Клементса–Гофмана, яка відрізняється від відомої розширеною, за рахунок доповнення моделі множиною вразливостей об'єктів, як окремо об'єктивно існуючої категорії, та конкретизованим для баз даних складом компонент, що дозволяє більш адекватно оцінювати ймовірність небажаного інциденту (реалізації загрози) та захищеність бази даних у цілому;

– метод оцінювання основних компонент бар'єрів безпеки та захищеності бази даних в цілому, який на відміну від відомих, за рахунок комплексування вдосконаленої моделі Клементса–Гофмана, введеного інтегрального показника безпеки, положень теорії нечітких множин та ризику, дозволяє адаптуватися до нових умов функціонування та прозоро, комплексно та кількісно оцінювати безпеку баз даних з різними моделями даних;

– метод маскування MOBAT, що відрізняється від відомого, можливістю обфускації даних, шляхом математичних перетворень на основі обчислення

операцій за модулем, що застосовуються до елементів даних не тільки числового, а й широко поширеного в базах даних рядкового типу, що дозволяє суттєво розширити охоплення різноманітних маскованих з метою утруднення реалізації зловмисником загрози умовиводу даних БД.

3. Отримали подальший розвиток:

– метод маскування елементів даних не ключових полів кортежів таблиць виробничої бази даних, що відрізняється від відомих оригінальним підходом до процесу перемішування з можливістю випадкової заміни елементів даних різного типу всередині заданого поля рядка та використання технології динамічного маскування, що дозволяє при менших обчислювальних витратах на перетворення і без зміни формату вихідних даних забезпечити ефективне приховування даних, яке ускладнює реалізацію загрози логічного висновку;

– метод приховування коду збережених у базі даних програм, який на відміну від відомих, дозволяє за рахунок випадкової перестановки (що спирається на сучасний варіант алгоритму тасування Фішера-Йейтса) символів коду з можливою заміною кожного з них на інший випадково вибраний із стандарту Unicode забезпечити більше ефективний (якій вимагає значно більших обчислювальних витрат) захист коду від його розкриття зловмисником, при цьому гарантуючи цілісність коду.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі, забезпечується: коректним використанням відомих положень теорії множин, відношень, графів, математичної логіки, математичної статистики, формальних моделей безпеки, комплексним урахуванням набору взаємопов'язаних об'єктів БД, загроз, вразливостей, заходів забезпечення безпеки, як відповідних елементів бар'єрів безпеки у базовій системі захисту, несуперечливістю відомим результатам, науковою апробацією результатів дисертаційних досліджень на науково-технічних і науково-практичних конференціях різного рівня.

Основні результати дисертаційного дослідження опубліковані в індексованих наукових журналах та доповідалися на міжнародних наукових конференціях. Висновки дисертаційної роботи є обґрунтованими.

6. Наукове, теоретичне та практичне значення результатів дисертації.

Беручи до уваги сучасний стан розвитку технологій баз, сховищ даних, у тому числі побудованих на основі схеми з універсальним базисом відношень, науково-практичні досягнення в галузі ІБ, кваліфікацію зловмисників, положення та рекомендації різних нормативно-правових актів, у роботі було переглянуто підхід до вирішення проблеми управління даними та забезпечення їхньої безпеки, результатом якого стали моделі, методи, засоби, актуальні як у теоретичному, так і в прикладному аспектах. У результаті вирішення поставлених завдань були отримані нові наукові результати, представлені вище, та наступні практично значущі для досліджуваної області результати:

1. Розроблений метод маскування елементів даних не ключових полів кортежів таблиць виробничої бази даних, орієнтований на заплутування, псевдонімізацію даних та ускладнення реалізації загрози логічного висновку, дозволяє зменшити час на відповідні операції перетворення на (10-17)% щодо методу класичного шифрування, при цьому не наводячи до зміни формату та збільшення розмірності даних, що зберігаються. Даний метод може бути також використаний у невиробничих базах даних, розширюючи можливості так званого статичного маскування даних.

2. Запропонований метод моніторингу модулів БД, що постійно зберігаються, вимагає менших обсягів збережених для цього даних і ресурсів процесора, ніж відомий метод контрольних сум, який для підтримки аналогічного контролю цілісності та справжності PSM вимагає виконання процедур гешування та цифрового підпису із збереженням відповідних даних для кожного конкретного PSM у конкретній схемі БД, причому однаково, не забезпечуючи контроль всього набору PSM загалом.

3. Розроблені в процесі створення схеми БД з УБВ спеціальні заходи у вигляді відповідних методів, реалізованих об'єктів схеми та правил їх використання підвищують безпеку таких баз даних, забезпечуючи високий

ступінь контрольованості доступу до даних (аж до конкретного елемента), необхідну конфіденційність, цілісність даних та об'єктів схеми БД, на відміну від традиційних РБД, що не володіють подібними заходами та функціональністю. Використання запропонованих рішень дозволяє підвищити ефективність / результативність захисту баз даних, побудованих на основі схеми з універсальним базисом відношень, більш ніж у 1.5 рази щодо традиційних реляційних БД.

Теоретичні та практичні результати дисертаційних досліджень реалізовані у приватному акціонерному товаристві «Інститут інформаційних технологій» та застосовуються у навчальному процесі Харківського національного університету імені В. Н. Каразіна.

Отримані у роботі теоретичні та практичні результати дисертаційних досліджень також можуть бути використані організаціями та компаніями, що займаються проектуванням та розробкою систем та засобів захисту для баз даних, оцінкою їх захищеності.

7. Повнота викладення матеріалів дисертації в роботах, опублікованих автором.

Основні результати дисертаційних досліджень опубліковано у **19** наукових працях, серед яких: **7** статей у фахових виданнях України, **7** статей у зарубіжних виданнях (індексується у Scopus, Web of Science), **2** розділи у колективних монографіях, **3** матеріали та тези доповідей на конференціях (у тому числі **1** конференція, матеріали якої індексується у Scopus та Web of Science).

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Наукові публікації у фахових виданнях України:

1. Yesin V. I., Vilihura V. V. Some approach to data masking as means to counter the inference threat. Radiotekhnika. 2019. No 198. P. 113–130.

(Особистий внесок здобувача: розроблені метод маскування даних на основі обчислення операцій за модулем, метод маскування даних поля рядка таблиці бази даних).

2. Вілігура В. В., Горбенко Ю. І., Єсін В. І., Рассомахін С. Г. Використання формальних моделей безпеки в захищених базах даних. Фізико-математичне моделювання та інформаційні технології. 2021. No 32. С. 70–74.

(Особистий внесок здобувача: аналіз моделей безпеки на основі дискреційної, мандатної, рольової політики із зазначенням рекомендацій щодо їх застосування при розробці захищених баз даних).

3. Єсін В. І., Вілігура В. В. Дослідження основних методів і схем шифрування з можливостю пошуку. Радіотехніка. 2022. No 209. С. 138–155.

(Особистий внесок здобувача: аналіз моделей та архітектур існуючих захищених пошукових систем з урахуванням особливостей сценаріїв їхнього функціонування; порівняльний аналіз продуктивності відомих класичних схем симетричного шифрування з можливістю пошуку).

4. Єсін В. І., Вілігура В. В. Дослідження основних схем шифрування з можливістю пошуку у базах даних, які підтримують SQL. Радіотехніка. 2022. No 210. С. 53– 74.

(Особистий внесок здобувача: аналіз основних систем шифрування з можливістю пошуку в базах даних, які підтримують мову структурних запитів SQL, з метою виявлення слабких і сильних сторін аналізованих систем та реалізованих у них методів для визначення можливості практичного їх використання в конкретних умовах функціонування).

5. Єсін В. І., Вілігура В. В. Основні категорії NewSQL баз даних та їх особливості. Радіотехніка. 2022. No 211. С. 37–66.

(*Особистий внесок здобувача: аналіз важливих характеристик (зокрема безпеки), властивих NewSQL, традиційним реляційним і NoSQL системам баз даних, із зазначенням рекомендацій щодо їх застосування у майбутньому, на наступному витку спіралі розвитку технологій баз даних).*

6. Єсін В. І., Вілігура В. В., Сватовський І. І. Забезпечення безпеки у розподілених інформаційних системах: основні аспекти. Радіотехніка. 2023. Вип. 214. С. 32– 63.

(Особистий внесок здобувача: аналіз актуальних сучасних методів, прийомів та засобів забезпечення безпеки розподілених інформаційних системах та їх основного функціонального компонента – бази даних).

7. Єсін В. І., Вілігура В. В., Узлов Д. Ю. Огляд існуючих моделей та основних принципів нульової довіри. *Радіотехніка.* 2024. Вип. 217. С. 39–54.

(Особистий внесок здобувача: аналіз моделей та ключових принципів концепції нульової довіри, як нового фундаментального підходу до інформаційної безпеки, кібербезпеки).

Наукова публікація у зарубіжних виданнях, що входять до міжнародних наукометричних баз Scopus та Web of Science:

8. Yesin V. I., Vilihura V. V. Method for development of databases easily adaptable to variations in the subject domain. Telecommunications and Radio Engineering. 2019. No 78(7). P. 595–605. (Scopus).

(Особистий внесок здобувача: оцінка завершеності створення бази даних, що відповідає заданим вимогам, на основі аналізу певних значень показників якості).

9. Yesin V. I., Karpinski M., Yesina M. V., Vilihura V. V. Formalized representation for the data model with the universal basis of relations. International Journal of Computing. 2019. No 18(4). P. 453–460. (Scopus).

(Особистий внесок здобувача: розробка принципів побудови алгоритму відображення концептуальної моделі предметної області у відношення універсального базису, що дозволяє в умовах динамічних змін предметних областей спростити процес створення логічних схем реляційних баз даних, що задовольняють заданим вимогам).

10. Yesin V. I., Yesina M. V., Vilihura V. V. Monitoring the integrity and authenticity of stored database objects. Telecommunications and Radio Engineering. 2020. No 79(12). P. 1029–1054. (Scopus).

(Особистий внесок здобувача: визначення структур блоків у блокчейновому ланцюжку та методів обчислення кореня геш-дерева, що формується на основі бінарних дерев різних типів, розробка принципів відображення структури блокчейну у відношення реляційної моделі даних, що

дозволяє забезпечувати своєчасний моніторинг цілісності, справжності об'єктів, що зберігаються в базі даних при меншому обчислювальному ресурсі і меншій надмірності необхідних для цього даних, порівняно з існуючими методами).

11. Yesin V., Karpinski M., Yesina M., Vilihura V., K. Warwas K. Hiding the Source Code of Stored Database Programs. Information. 2020. No 11(12). 576. (Scopus, Web of Science).

(Особистий внесок здобувача: розробка методу та основних принципів побудови алгоритмів маскування вихідного коду збережених програм та дослідження їх властивостей).

12. Yesin V., Karpinski M., Yesina M., Vilihura V., Warwas K. Ensuring Data Integrity in Databases with the Universal Basis of Relations. Applied Sciences. 2021. No 11(18). 8781. (Scopus, Web of Science).

(Особистий внесок здобувача: аналіз моделі Кларка-Вілсона та розробка на основі її рекомендацій методів та засобів, що забезпечують цілісність основних компонентів бази даних з універсальним базисом відношень).

13. Yesin V., Karpinski M., Yesina M., Vilihura V., Rajba S. A. Technique for Evaluating the Security of Relational Databases Based on the Enhanced Clements–Hoffman Model. *Applied Sciences*. 2021. No 11(23). 11175. (Scopus, Web of Science).

(Особистий внесок здобувача: розробка вдосконаленої моделі Клементса-Хоффмана та методу оцінювання захищеності бази даних, дослідження безпеки реляційних баз даних, спроектованих за різними технологіями).

14. Yesin V., Karpinski M., Yesina M., Vilihura V., Kozak R., Shevchuk R. Technique for Searching Data in a Cryptographically Protected SQL Database. Applied Sciences. 2023. No 13(20). 11525. (Scopus, Web of Science).

(Особистий внесок здобувача: розробка методики пошуку в криптографічно захищеній базі даних, що дозволяє серверу СКБД виконувати функції пошуку за зашифрованими даними так само, як і в незашифрованій базі даних, і що забезпечує належну конфіденційність даних, що зберігаються, при прийнятних накладних витратах).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

15. Вілігура В. В., Єсін В. В. Використання національного криптоалгоритму для захисту персональних даних в СУБД Oracle. Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2016): Праці науково-технічної міжнародної конференції, 26-31 травня 2016 р. Харків: Харківський національний університет імені В. Н. Каразіна, 2016. С. 77–80.

(Особистий внесок здобувача: оцінка можливості та доцільності використання національного криптоалгоритму «Калина» для захисту персональних даних в СКБД Oracle).

16. Yesin V. I., Karpinski M., Yesina M. V., Vilihura V. V., Veselska O., L. Wieclaw L. Approach to Managing Data From Diverse Sources. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS): Proceedings of the 2019 10th IEEE International Conference, 18-21 September, 2019, Metz, France, Volume 1, P. 1–6. (Scopus, Web of Science).

(Особистий внесок здобувача: розробка методу, операції якого спрямовані на підготовку інформаційних продуктів та конфігураційної бази даних середовища управління простором даних компанії до використання).

17. Вілігура В. В. Систематизація загроз і вразливостей характерних для баз даних і СУБД. Праці 7-ої Міжнародній конференції «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021), 21-23 квітня 2021 р. Харків: Харківський національний університет імені В. Н. Каразіна, 2021. С. 83–86.

Наукові публікації, що додатково відображають зміст дисертації:

18. Advances in Information Security and Privacy. In: Lax G., Russo A. (eds). MDPI: Basel, Switzerland. 2022. 344 p. (Yesin V., Karpinski M., Yesina M., Vilihura V., Rajba S. A., Warwas K. P. 257–294). ISBN 978-3-0365-5296-5 (hardback); ISBN 978-3- 0365-5295-8 (PDF). https://doi.org/10.3390/books978-3-0365-5295-8.

(Особистий внесок здобувача: аналіз моделей Кларка-Вілсона та Клементса-Хоффмана із розробкою методів та засобів, що забезпечують цілісність основних компонентів бази даних з універсальним базисом відношень,

та дозволяють оцінювати захищеність баз даних, спроектованих за різними технологіями).

19. Mathematics and Computer Science – Contemporary Developments. In: El-Sayed Mohamed Abo-Dahab Khedary (eds). BP International: Hooghly, West Bengal, India, 2024. Vol. 1. 95 p. (Yesin V., Karpinski M., Yesina M., Vilihura V., Kozak R., Shevchuk R. Introducing a Technique for Searching Data in a Cryptographically Protected SQL Database. P. 1–29.). ISBN 978-81-977283-5-8 (Print), ISBN 978-81-977283-6-5 (eBook). https://doi.org/10.9734/bpi/mcscd/v1.

(Особистий внесок здобувача: розробка методики пошуку даних у криптографічно захищеній базі даних із збереженням конфіденційності даних, що зберігаються, при прийнятних накладних витратах).

Результати дисертаційної роботи повністю відображено в публікаціях.

8. Дотримання академічної доброчесності.

На підставі вивчення тексту дисертації здобувача, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній інтернет-системі Strikeplagiarism.com) встановлено, що дисертаційна робота виконана самостійно, текст дисертації не містить плагіату, а дисертація відповідає вимогам академічної доброчесності.

9. Апробація матеріалів дисертації.

Результати проведених досліджень представлялись на міжнародних та вітчизняних наукових конференціях у формі доповідей, за результатами яких були опубліковані матеріали конференцій:

1. Вілігура В. В., Єсін В. В. Використання національного криптоалгоритму для захисту персональних даних в СУБД Oracle. Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2016): Праці науково-технічної міжнародної конференції, 26-31 травня 2016 р. Харків: Харківський національний університет імені В. Н. Каразіна, 2016. С. 77–80.

2. Yesin V. I., Karpinski M., Yesina M. V., Vilihura V. V., Veselska O., L. Wieclaw L. Approach to Managing Data From Diverse Sources. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications

(IDAACS): Proceedings of the 2019 10th IEEE International Conference, 18-21 September, 2019, Metz, France, Volume 1, P. 1–6. (Scopus, Web of Science).

3. Вілігура В. В. Систематизація загроз і вразливостей характерних для баз даних і СУБД. Праці 7-ої Міжнародній конференції «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021), 21-23 квітня 2021 р. Харків: Харківський національний університет імені В. Н. Каразіна, 2021. С. 83–86.

10. Оцінка структури, мови та стилю дисертації.

Матеріал дисертації викладено в логічній послідовності та доступно для сприйняття. Дисертація написана науковим стилем мовлення, структура дисертації відповідає алгоритму здійсненого автором дослідження. Зміст, структура, оформлення дисертації та кількість публікацій відповідають вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 р. № 44), наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

11. Відповідність змісту дисертації спеціальності, за якою вона подається до захисту.

За своїм фаховим спрямуванням, науковою новизною і практичною значимістю дисертаційна робота Вілігури В. В. «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень» повністю відповідає спеціальності 125 – Кібербезпека та захист інформації. Здобувачем повністю виконано освітню та наукову складову третього (освітньо-наукового) рівня вищої освіти.

12. Результати обговорення та проведення презентації. Рекомендація дисертації до захисту.

Здобувач представив основні результати своєї дисертаційної роботи на розширеному засіданні кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна щодо попередньої експертизи дисертації (Витяг з протоколу № 3 розширеного

засідання кафедри кібербезпеки інформаційних систем, мереж і технологій від 28 жовтня 2024 р.) у формі презентації та наукової дискусії після її завершення. На даному засіданні були присутні 13 співробітників Харківського національного університету імені В. Н. Каразіна, із яких 4 докторів наук та 8 кандидатів наук. Дисертанту було задано 6 запитань, на які він надав вичерпні відповіді. Також виступили 4 науковця, які позитивно відізвались про дисертаційне дослідження Вілігури В. В.

У рамках цього розширеного засідання було ухвалено одноголосно (13 голосів) рекомендувати дисертаційну роботу здобувача Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень» до захисту на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації.

Доктор технічних наук, професор,
професор кафедри кібербезпеки
інформаційних систем, мереж і технологій
Харківського національного
університету імені В. Н. Каразіна  Ірина ЛИСИЦЬКА