Голові разової
спеціалізованої вченої ради
Харківського національного
університету імені В. Н. Каразіна
професору Івану ГОРБЕНКУ
майдан Свободи 4, м. Харків, 61022

Рецензія

офіційного рецензента, доктора технічних наук, професора, професора кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна Олійникова Романа Васильовича на дисертаційну роботу Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації

У сучасному суспільстві інформація перетворилася на один з найважливіших ресурсів, а інформаційні системи, в яких бази даних є ключовим функціональним компонентом, стали необхідним інструментом для забезпечення ефективної діяльності у різних сферах. Ці системи завдяки базам даних (БД) надають достовірні дані, які є основою для ухвалення оптимальних рішень. Зростання обсягів Великих Даних та перехід до парадигми управління, заснованої на даних, створюють значні перспективи, але водночас супроводжуються низкою нерозв'язаних проблем, зокрема підвищеним інтересом до інформації з боку зловмисників.

Сучасний розвиток теорії та практики інформаційної безпеки, зокрема захисту баз і сховищ даних, відображає подвійність ситуації. З одного боку, існує підвищена увага до питань безпеки, яка проявляється у проведенні значної кількості досліджень, розробці систем захисту інформації, збільшенні інвестицій у цю сферу, а також у впровадженні міжнародних та національних стандартів, що встановлюють високі вимоги до безпеки інформаційних систем (ІС). Однак,

з іншого боку, постійно зростають збитки, яких зазнають власники інформаційних ресурсів через дії зловмисників, що свідчить про недостатню ефективність існуючих підходів до захисту даних.

Особливу важливість має забезпечення захисту баз і сховищ даних, які містять чутливу інформацію. У цьому контексті актуальним стає дослідження баз даних, побудованих на основі схеми з універсальним базисом відношень (УБВ). По-перше, це дає змогу забезпечити високий рівень захищеності даних і продемонструвати переваги таких БД перед традиційними реляційними базами даних. По-друге, інваріантність до предметних областей схеми бази із УБВ дозволяє використовувати їх як сховища даних, конфігураційні бази або інші компоненти інформаційних систем (ІС), що відкриває можливості для створення деякого цілісного рішення, що забезпечує безпеку баз даних із різними моделями даних. У цих умовах, беручи до уваги сучасний стан технологій баз даних, розвиток шкідливого програмного забезпечення, а також рекомендації нормативно-правових актів, перегляд підходів до управління даними та їхньої безпеки є необхідним. Застосування нових моделей, методів і засобів, розроблених на основі схеми з УБВ, може забезпечити підвищення рівня захисту БД (реляційних, NoSQL, NewSQL) та сприяти створенню універсальних рішень для ІС різних типів.

Таким чином, тема дисертаційного дослідження, що спрямована на розробку моделей, методів і засобів для підвищення захищеності баз даних, побудованих на основі схеми з універсальним базисом відношень, є надзвичайно актуальною та відповідає сучасним викликам інформаційної безпеки.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі Вілігури В. В., досягається 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.

Найвагоміші наукові результати, що містяться в дисертації

Основними науковими результатами, одержаними в дисертації, є наступні:

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 даних 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 (який вимагає значно більших обчислювальних витрат) захист коду від його розкриття зловмисником, при цьому гарантуючи цілісність коду.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 19 наукових праць, 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 індексуються у Scopus та Web of Science).

Оцінка змісту дисертації, її завершеності в цілому і оформлення

Дисертаційна робота містить: вступ, 6 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 252 сторінки друкованого тексту, з яких: 168 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 247 найменувань на 25 сторінках, додатки на 39 сторінках. Робота містить 12 таблиць та 39 рисунків.

Перший розділ присвячений аналізу основних проблем, сучасного стану та розвитку технологій баз даних, формальних моделей, як методологічної основи побудови систем захисту та оцінки їхньої безпеки. На підставі проведеного аналізу робиться висновок про те, що існуючі теоретичні розробки та практичні реалізації забезпечення безпеки баз даних інформаційних систем базуються на двох основних підходах: формальному моделюванні політики безпеки та криптографії. Причому ці підходи, різні за походженням і розв’язуваним завданням, доповнюють одне одного, але потребують подальшого вивчення. В результаті в першому розділі робиться висновок про доцільність проведення

подальших досліджень, результатом яких могла б стати певна методологія комплексного використання різних підходів, що призвело б до підвищення ефективності захисту баз даних.

У другому розділі розглядається формалізація завдання забезпечення безпеки бази даних на основі системи захисту з повним перекриттям, визначається показник безпеки бази даних, удосконалюється модель Клементса-Хоффмана для баз даних. Запропонований у розділі метод оцінки основних складових бар'єрів безпеки та захищеності баз даних є результатом синтезу вдосконаленої моделі Клементса-Хоффмана, інтегрального показника безпеки, положень теорії нечітких множин та ризику. Даний метод, маючи певну гнучкість, дозволяє, на відміну від відомих, досить просто, комплексно та кількісно оцінити захищеність баз даних, побудованих на основі різних моделей даних.

Третій розділ роботи присвячений розробці методу маскування даних, заснованого на обчисленні операцій за модулем, методу маскування даних поля рядка таблиці БД та методу приховування вихідного коду збережених програм. У цьому розділі проводиться порівняльний аналіз можливостей запропонованого методу маскування даних поля рядка таблиці та методу шифрування для приховування даних, надаються відповідні рекомендації щодо застосування методів маскування даних, а також оцінюється можливість використання шифрування для приховування вихідного коду збережених програм.

У четвертому розділі розробляється метод контролю цілісності та справжності збережених програм, що ґрунтується на можливостях технології блокчейн. Відповідно до запропонованого методу визначаються структура та правила формування первинного та наступних блоків у ланцюжку блокчейну, крім того, пропонується підхід до зберігання структури блокчейну в рамках реляційної моделі даних, що полягає у відображенні цієї структури у двох відношеннях та даються рекомендації щодо розміщення цих спеціальних відношень (таблиць). Формулюється вимога щодо необхідності підписання творцем конкретної схеми БД «своїх» відповідних даних, представлених в одній із спеціальних таблиць, одним із сучасних алгоритмів електронного підпису для захисту від неправомірних дій привілейованих користувачів, а також від нелегітимних дій зловмисників.

У п'ятому розділі дисертаційного дослідження, що є логічним продовженням усіх попередніх розділів, для забезпечення безпеки

корпоративних БД, побудованих на основі схеми бази з універсальним базисом відношень, пропонується використовувати комплексно загальні формальні моделі управління доступом та забезпечення цілісності даних, методи та механізми, що підтримуються системою управління БД, на платформі якої ця схема реалізована, а також власні заходи безпеки, розроблені в рамках створення інваріантної до предметної області схеми БД.

Шостий розділ присвячений порівняльному аналізу захищеності баз даних, побудованих за традиційною технологією та технологією, заснованої на універсальному базисі відношень. Проведений порівняльний аналіз дозволяє зробити загальний висновок про більшу ефективність запропонованих та реалізованих заходів, засобів забезпечення безпеки в рамках схеми БД з УБВ порівняно з існуючими заходами та засобами, реалізованими в рамках традиційних реляційних баз даних.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки баз даних.

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Зв’язок роботи з науковими програмами, планами, темами

Дисертаційні дослідження проводились в рамках науково-дослідницьких робіт: № 39-18 «Механізми, методи, протоколи та засоби криптографічного захисту інформації у пост квантовий період» (Шифр «Квант-2019»), № 29-19 «Механізми та засоби електронного підпису у пост квантовий період», (Шифр «Квант-2020»), № 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» (№ ДР 0121U109939), № 34-21 «Методи та алгоритми постквантових криптоперетворень, їх стандартизація та впровадження» (Шифр «Квант-2022»), № 09-22 «Методи та засоби генерування псевдовипадкових та випадкових

послідовностей на основі класичних та квантових ефектів» (Шифр «Квант-2023»).

Практичне значення отриманих результатів

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.

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі Strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Дискусійні положення та зауваження до змісту дисертації

1. Автор у дисертаційній роботі акцентує увагу на важливості здійснення маскування з метою протидії загрозі логічного висновку та пропонує відповідні методи вирішення цієї проблеми, однак у роботі не повною мірою розкриваються дії у разі компрометації окремих закритих ключів, які використовуються у процедурі динамічного маскування запропонованого рішення.
2. Розуміючи значущість таблиці R^{secret} у забезпеченні безпеки відповідних даних, залежних від неї, у дисертаційній роботі можна було б докладніше описати дії, які виконуються у разі компрометації ключа шифрування цієї таблиці.
3. Для кращого розуміння процесу перетворення «на льоту» – заміни запиту, що реалізує процедуру зворотного маскування, для легітимного автентифікованого користувача в поточному сеансі роботи з базою даних, було б доречно навести, наприклад, послідовність або перелік попередніх дій, які необхідно виконати, щоб згодом можна було здійснювати таку можливість.

Однак, висловлені зауваження не впливають суттєво на загальну високу оцінку дисертаційного дослідження, його цілісність та результативність. Наукова новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Загальні висновки

Дисертаційна робота Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень» є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Вілігура Владислав Вікторович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний рецензент
доктор технічних наук, професор,
професор кафедри кібербезпеки
інформаційних систем, мереж і технологій
Навчально-наукового інституту
комп’ютерних наук та
штучного інтелекту
Харківського національного
університету імені В. Н. Каразіна Роман ОЛІЙНИКОВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 17:11:26 02.01.2025

Назва файлу з підписом: Олійников_рецензія_оф_рецензента.pdf
Розмір файлу з підписом: 101.6 КБ

Перевірені файли:
Назва файлу без підпису: Олійников_рецензія_оф_рецензента.pdf
Розмір файлу без підпису: 67.5 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Олійников Роман Васильович
П.І.Б.: Олійников Роман Васильович
Країна: Україна
РНОКПП: 2796617236
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 17:11:20 02.01.2025
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 382367105294AF9704000000F9AA0F0060BBD402
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підписаний PDF-файл (PAdES)
Формат підпису: З повними даними для перевірки (PAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2024.10.24 15:00

Голові разової
спеціалізованої вченої ради
Харківського національного
університету імені В. Н. Каразіна
професору Івану ГОРБЕНКУ
майдан Свободи 4, м. Харків, 61022

Рецензія

офіційного рецензента, кандидата технічних наук, наукового співробітника науково-дослідної частини Харківського національного університету імені В. Н. Каразіна (кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту) Пономаря Володимира Андрійовича на дисертаційну роботу Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації

У сучасному суспільстві інформація стала одним з найцінніших ресурсів, а інформаційні системи (ІС), зокрема бази даних як їх ключовий елемент, стали незамінними у всіх сферах людської діяльності, забезпечуючи достовірні дані для ухвалення оптимальних рішень. Зростання обсягу Big Data і концепція даних, що керують світом, відкривають нові можливості, але водночас виявляють численні проблеми, оскільки інтерес до інформації в ІС зростає не лише з боку легітимних користувачів та власників, а й з боку зловмисників.

На сьогоднішній день у сфері інформаційної безпеки, зокрема в контексті баз і сховищ даних, існує парадоксальна ситуація: з одного боку, спостерігається зростання уваги до цих питань через активну наукову та практичну діяльність у створенні та вдосконаленні систем захисту інформації; збільшення фінансування на ці цілі; прийняття численних міжнародних і національних стандартів та законодавчих актів, що встановлюють високі вимоги до захисту інформації в ІС та передбачають штрафи за їх порушення. Це має позитивно вплинути на безпеку

ІС та БД. З іншого боку, фіксується постійне збільшення збитків для власників інформаційних ресурсів.

З цих обставин стає очевидним, що сучасні методи забезпечення інформаційної безпеки не повною мірою відповідають вимогам захисту. Без належного захисту баз і сховищ даних разом із чутливими даними нові інформаційні технології можуть загрожувати як приватності особистостей, так і діяльності великих організацій.

В умовах сучасного розвитку технологій баз і сховищ даних, включаючи універсальні бази відношень (УБВ), науково-практичні досягнення в галузі інформаційної безпеки та постійне вдосконалення зловмисниками своїх методів атак через шкідливе програмне забезпечення, актуальним є перегляд підходів до управління даними та забезпечення їх безпеки. Це може призвести до розробки нових методів і засобів, які будуть корисними як у теоретичному, так і в практичному контекстах.

Дослідження баз даних з УБВ є доцільним, оскільки це дозволяє підтвердити безпеку даних у таких системах і продемонструвати переваги їх захищеності порівняно з традиційними реляційними БД. Крім того, завдяки різноманітності застосувань УБВ – від звичайних БД до сховищ даних у різних предметних областях – можливо розробити комплексне рішення для забезпечення безпеки реляційних баз даних. До того ж, елементи цього рішення можуть бути адаптовані для захисту БД різних моделей (NoSQL, NewSQL).

Таким чином, тема дисертаційної роботи, що присвячена розробці моделей, методів і засобів для підвищення захищеності БД на основі УБВ, є актуальною та своєчасною.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Аналіз анотації, тексту дисертації та змісту фахових публікацій дисертанта дає змогу зробити висновок про достатню наукову обґрунтованість та достовірність результатів, отриманих у результаті проведеного дослідження. Усі наукові положення, висновки та рекомендації належним чином обґрунтовані та підкріплені теоретичними положеннями. Вони відповідають меті та завданням дисертаційної роботи, що забезпечується адекватністю обраних для дослідження методів. Вірогідність наукових результатів та висновків дисертаційної роботи

забезпечується достатнім рівнем апробації та високим рівнем наукових видань, в яких опубліковано результати дисертаційного дослідження.

Найбільш важливі результати, що містяться в дисертації

Основними науковими результатами, одержаними в дисертації, є:

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 даних 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 (який вимагає значно більших обчислювальних витрат) захист коду від його розкриття зловмисником, при цьому гарантуючи цілісність коду.

Апробація дисертації та публікації

Основні результати роботи були апробовані та опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 19 наукових праць: 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 індексуються у Scopus та Web of Science).

Оцінка змісту дисертації, її завершеності в цілому і оформлення

Дисертаційна робота містить: вступ, 6 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації – 252 сторінки, з них: 168 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 247 найменувань на 25 сторінках, додатки на 39 сторінках. У роботі міститься 12 таблиць та 39 рисунків.

Список використаних джерел відображає той факт, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки баз даних.

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційні дослідження проводились в рамках науково-дослідницьких робіт: № 39-18 «Механізми, методи, протоколи та засоби криптографічного захисту інформації у пост квантовий період» (Шифр «Квант-2019»), № 29-19 «Механізми та засоби електронного підпису у пост квантовий період», (Шифр «Квант-2020»), № 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» (№ ДР 0121U109939), № 34-21 «Методи та алгоритми постквантових криптоперетворень, їх стандартизація та впровадження» (Шифр «Квант-2022»), № 09-22 «Методи та засоби генерування псевдовипадкових та випадкових послідовностей на основі класичних та квантових ефектів» (Шифр «Квант-2023»).

Практичне значення отриманих результатів

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.

Дотримання академічної доброчесності

Аналіз дисертаційної роботи та публікацій автора не виявив порушень академічної доброчесності, елементів фальсифікації чи фабрикації тексту.

Дискусійні положення та зауваження до змісту дисертації

1. Розшифровування даних на льоту може вимагати додаткових обчислювальних витрат, що може призвести до збільшення часу виконання запитів у порівнянні з базами даних, які зберігають незашифровані дані.
2. Реалізація та забезпечення функціонування систем захисту складних інформаційних систем пов’язана з певними труднощами, у тому числі пов'язаними із забезпеченням безпеки компонентів програмного забезпечення, що додатково розробляються, проте в роботі це питання знайшло незначне (часткове) відображення.
3. У дисертаційній роботі підкреслюється необхідність криптографічного захисту конфіденційної інформацій та наводяться окремі способи її вирішення, але не повною мірою розкрито питання управління ключами.

Проте, зазначені зауваження в цілому не впливають на результативність, завершеність та загальну позитивну оцінку виконаної дисертаційної роботи, а також не знижують наукової та практичної цінності отриманих результатів.

Загальні висновки

Дисертаційна робота Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень» є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Вілігура Владислав Вікторович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний рецензент
кандидат технічних наук,
науковий співробітник
науково-дослідної частини
Харківського національного
університету імені В. Н. Каразіна
(кафедри кібербезпеки інформаційних
систем, мереж і технологій
Навчально-наукового інституту
комп’ютерних наук та
штучного інтелекту) Володимир ПОНОМАР

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 11:31:56 02.01.2025

Назва файлу з підписом: РЕЦЕНЗІЯ_оф_рецензента_Пономар_без_засвідчення_підпису.docx.p7s
Розмір файлу з підписом: 46.2 КБ

Перевірені файли:
Назва файлу без підпису: РЕЦЕНЗІЯ_оф_рецензента_Пономар_без_засвідчення_підпису.docx
Розмір файлу без підпису: 28.8 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ПОНОМАР ВОЛОДИМИР АНДРІЙОВИЧ
П.І.Б.: ПОНОМАР ВОЛОДИМИР АНДРІЙОВИЧ
Країна: Україна
РНОКПП: 3365403873
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 11:31:56 02.01.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000009DEF4C0123EADB04
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Серійний номер носія особистого ключа: 011
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в одному файлі (CAdES enveloped)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2024.10.24 15:00

Голові разової
спеціалізованої вченої ради
Харківського національного
університету імені В. Н. Каразіна
професору Івану ГОРБЕНКУ
майдан Свободи 4, м. Харків, 61022

Відгук

офіційного опонента, доктора технічних наук, професора, завідувача кафедри математичного забезпечення комп'ютерних систем Одеського національного університету імені І. І. Мечникова Малахова Євгенія Валерійовича на дисертаційну роботу Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

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. Зростання Великих Даних (Big Data) та бачення світу, керованого даними, відкривають багато цікавих можливостей, одночасно виявляючи безліч невирішених проблем, так як зростає інтерес до інформації, що циркулює всередині ІС, не тільки з боку законних користувачів і власників, але і з боку зловмисників. 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: у виконанні великої наукової та практичної роботи зі створення, організації та дослідження процесів функціонування, удосконалення та розвитку систем захисту інформації; у постійному зростанні асигнувань на забезпечення захисту; у прийнятті великої кількості різних міжнародних, вітчизняних стандартів та інших законодавчих актів у галузі

інформаційної безпеки, що передбачають високі вимоги до захисту інформації в ІС, 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.

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 (УБВ) 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 ІС. По-друге, на їх прикладі, через те, що бази даних з УБВ можуть використовуватися в різній якості – як звичайна БД, сховище даних різних предметних областей 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).

Тому тема дисертаційної роботи, яка присвячена рішенню науково-прикладного завдання, яке полягає в розробці моделей, методів і засобів, що дозволяють підвищити захищеність баз даних, побудованих на основі схеми з універсальним базисом відношень, є актуальною та своєчасною.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі, досягається 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.

Наукова новизна одержаних результатів

До основних нових наукових результатів дисертації слід віднести наступне:

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 даних 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 (який вимагає значно більших обчислювальних витрат) захист коду від його розкриття зловмисником, при цьому гарантуючи цілісність коду.

Повнота викладу основних наукових результатів у опублікованих працях

Основні отримані в роботі результати були апробовані і в належній мірі опубліковані у фахових виданнях. Відповідно до основного переліку робіт, за темою дисертаційної роботи було опубліковано 19 наукових праць, 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 індексуються у Scopus та Web of Science).

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора

філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024).

Оцінка змісту дисертаційної роботи, її завершеність

Дисертаційна робота складається зі вступу, 6 розділів, висновків, переліку посилань та додатків. Загальний обсяг дисертації складає 252 сторінки, з яких анотація на 10 сторінках, список публікацій здобувача за темою дисертації на 5 сторінках, зміст на 3 сторінках, перелік умовних позначень на 2 сторінках, основний текст на 168 сторінках, список використаних джерел із 247 найменувань на 25 сторінках, додатки на 39 сторінках. Робота містить 12 таблиць та 39 рисунків.

У вступі обґрунтовано актуальність дослідження, поставлену мету та визначено основні завдання дослідження, об’єкт та предмет дослідження. Викладено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача. Подано відомості про апробацію та опубліковані результати досліджень.

У першому розділі проведено аналіз ключових проблем, сучасного стану та розвитку технологій баз, формальних моделей, як методологічної основи побудови систем захисту та оцінки їх безпеки. В результаті проведеного аналізу було встановлено, що існуючі теоретичні розробки та практичні реалізації забезпечення безпеки ІС, БД ґрунтуються на двох парадигмах: формального моделювання політики безпеки та криптографії. Причому ці різні за походженням і вирішуваним завданням підходи доповнюють один одного. У зв’язку з чим у розділі 1 робиться висновок про доцільність проведення подальших досліджень, результатом яких була б деяка методологія комплексного використання різних парадигм, що веде до підвищення ефективності захисту баз даних.

У другому розділі формалізована задача забезпечення безпеки бази даних на основі системи захисту з повним перекриттям, визначено показник захищеності бази даних, удосконалена модель Клементса–Гофмана для баз даних. Запропоновано метод оцінювання основних компонентів бар’єрів безпеки та захищеності бази даних, який є результатом синтезу вдосконаленої моделі Клементса–Гофмана, інтегрального показника безпеки, положень теорії нечітких множин та ризику. Даний метод, на відміну від відомих, маючи певну

гнучкість, дозволяє досить просто, комплексно і кількісно оцінювати безпеку БД з різними моделями даних.

У третьому розділі розроблено метод маскування даних на основі обчислення операцій за модулем, метод маскування даних поля рядка таблиці бази даних, метод приховування вихідного коду збережених програм. Проведено порівняльний аналіз можливостей запропонованого методу маскування даних поля рядка таблиці та методу шифрування щодо приховування даних, наведено рекомендації щодо застосування методів маскування даних, оцінка можливості використання шифрування для приховування вихідного коду збережених програм.

У четвертому розділі розроблено метод контролю цілісності та справжності збережених програм, заснованого на можливостях технології блокчейн. Відповідно до запропонованого методу було визначено структуру та правила формування первинного та наступних блоків у блокчейновому ланцюжку; запропоновані: підхід до зберігання структури блокчейна в рамках реляційної моделі даних, що полягає у відображенні цієї структури у два відношення (таблиці) та рекомендації щодо розміщення цих спеціальних таблиць, виходячи з обмеження можливості несанкціонованої зміни їх даних; сформульовано вимогу про необхідність підпису творцем конкретної схеми БД «своїх» відповідних даних, представлених в одній із спеціальних таблиць, одним із сучасних алгоритмів цифрового підпису, щоб захиститися від неправомочних дій привілейованого користувача, а також від нелегітимних дій зловмисників.

П’ятий розділ дисертаційного дослідження є логічним продовженням попередніх розділів. У якому для забезпечення безпеки корпоративних баз даних, побудованих на основі схеми БД з універсальним базисом відношень, пропонується комплексне використання загальних формальних моделей управління доступом та забезпечення цілісності даних, методів, засобів, механізмів, що підтримуються СКБД, на платформі яких ця схема реалізується, та власних заходів забезпечення безпеки, розроблених у рамках створення інваріантної до предметної області схеми БД.

В шостому розділі наводиться порівняльний аналіз захищеності баз даних, побудованих за традиційною технологією та на основі універсального базису відношень. Проведений порівняльний аналіз дозволив зробити загальний висновок про більшу ефективність запропонованих та реалізованих у рамках

схеми БД з УБВ заходів щодо забезпечення безпеки порівняно з наявними, реалізованими в рамках традиційних реляційних баз даних.

Розділи дисертаційної роботи організовані за логічними блоками, прослідкується зв'язок між ними, що забезпечує достатньо наглядний перехід від одного аспекту дослідження до іншого. Простежується дотримання академічного стилю. Здобувач використовує наглядні приклади та ілюстрації, що допомагають усвідомити основні ідеї та результати досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки баз даних.

Академічна доброчесність

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено. Усі результати, які винесено автором на захист, містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Недоліки та зауваження до дисертаційної роботи

1. У розділі 5.1 йдеться про запропоноване рішення, що дозволяє здійснювати пошук, проводити безпечну вставку, модифікацію та видалення необхідних конфіденційних даних при розумних накладних витратах, проте його архітектура (як різновид трирівневої архітектури клієнт-сервер) не наводиться, хоча в роботі все ж таки є посилання на відповідну статтю автора.
2. Пропоновані методи маскування припускають здійснення відповідних перетворень лише для неключових атрибутів вибраних таблиць.
3. У роботі зазначається, що для полів таблиць типу BLOB, що мають велику розмірність, застосування методу маскування на основі перестановки всіх байт BLOB призводить до значних витрат часу, тому для вирішення цієї проблеми пропонуються деякі варіанти підходів, хоча при цьому не наводяться результати відповідних досліджень та аналізу застосування таких підходів.

Однак означені недоліки суттєво не впливають на зміст та отримані науково-практичні результати дисертації.

Висновок про дисертаційну роботу

Дисертаційна робота Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень» за своїм змістом відповідає спеціальності 125 Кібербезпека та захист інформації. Представлена робота виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеною науково-дослідною роботою, яка розв’язує актуальну науково-прикладну задачу розроблення та удосконалення моделей, методів і засобів, що дозволяють підвищити захищеність баз даних, побудованих на основі схеми з універсальним базисом відношень. В результаті проведених досліджень отримані нові науково обґрунтовані результати.

Вважаю, що дисертаційна робота Вілігури В. В. відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пунктів 6, 7, 8 і 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024), а здобувач Вілігура Владислав Вікторович заслуговує на присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент:
доктор технічних наук, професор,
завідувач кафедри математичного забезпечення
комп’ютерних систем
Одеського національного
університету імені І. І. Мечникова Євгеній МАЛАХОВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 11:33:46 02.01.2025

Назва файлу з підписом: ВІДГУК оф опонента Малахов.pdf.asice
Розмір файлу з підписом: 148.2 КБ

Перевірені файли:
Назва файлу без підпису: ВІДГУК оф опонента Малахов.pdf
Розмір файлу без підпису: 153.9 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: МАЛАХОВ ЄВГЕНІЙ ВАЛЕРІЙОВИЧ
П.І.Б.: МАЛАХОВ ЄВГЕНІЙ ВАЛЕРІЙОВИЧ
Країна: Україна
РНОКПП: 2399601337
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 11:33:43 02.01.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000001D8D6001BDB11005
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2024.10.24 15:00

Голові разової
спеціалізованої вченої ради
Харківського національного
університету імені В. Н. Каразіна
професору Івану ГОРБЕНКУ
майдан Свободи 4, м. Харків, 61022

Відгук

офіційного опонента, доктора технічних наук, професора, професора кафедри безпеки інформаційних технологій Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» Нємкової Олени Анатоліївни на дисертаційну роботу Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційного дослідження

У сучасному світі інформація стала одним із ключових ресурсів суспільства, а інформаційні системи, в яких бази даних відіграють роль основного функціонального компонента, є невід'ємним інструментом у багатьох сферах діяльності. Водночас розвиток технологій, зокрема Big Data, не тільки відкриває значні можливості, а ще й створює нові виклики у сфері захисту інформації. Інтерес до даних, що обробляються в інформаційних системах (ІС), зростає не лише серед законних користувачів, але й серед зловмисників, що вимагає удосконалення підходів до їхньої безпеки.

Попри суттєві досягнення у сфері інформаційної безпеки, включаючи розробку стандартів, впровадження нормативно-правових документів і значні інвестиції у створення систем захисту, збитки, яких зазнають власники інформаційних ресурсів через кібератаки, продовжують зростати. Це свідчить про те, що наявні підходи до захисту інформації не завжди відповідають сучасним викликам, особливо, коли йдеться про бази та сховища даних, які містять чутливу інформацію.

З огляду на розвиток технологій баз даних (БД), зокрема тих, що побудовані на схемі з універсальним базисом відношень (УББВ), доцільно переглянути підходи до управління даними та забезпечення їхньої безпеки. Дослідження баз даних із УББВ є актуальним, оскільки вони демонструють потенціал забезпечення вищого рівня захищеності порівняно з традиційними реляційними базами даних. Крім того, бази даних з УББВ можна застосовувати як сховища даних різних предметних областей або як конфігураційні бази для управління простором даних, що відкриває нові перспективи у створенні цілісних рішень для забезпечення інформаційної безпеки.

Таким чином, тема дисертаційного дослідження, спрямованого на розробку моделей, методів і засобів підвищення захищеності баз даних, побудованих на основі схеми з універсальним базисом відношень, є своєчасною та важливою для вирішення актуальних науково-прикладних завдань у галузі інформаційної безпеки.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Аналіз анотацій, тексту дисертації та змісту публікацій Вілігури В. В. дає змогу зробити висновок про наукову обґрунтованість та достовірність результатів, отриманих у результаті проведеного дослідження. Усі наукові положення, висновки та рекомендації належним чином обґрунтовані та підкріплені теоретичними положеннями. Вони відповідають меті та завданням дисертаційної роботи, що забезпечується адекватністю обраних для дослідження методів. Вірогідність наукових результатів та висновків дисертаційної роботи забезпечується достатнім рівнем апробації та високим рівнем наукових видань, в яких опубліковано результати дисертаційного дослідження.

Основні наукові результати, одержані автором, та їх новизна

Основними науковими результатами, одержаними автором, є наступні:

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 даних 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 (який вимагає значно

більших обчислювальних витрат) захист коду від його розкриття зловмисником, при цьому гарантуючи цілісність коду.

Апробація дисертації та публікації

Основні результати дисертаційного дослідження були апробовані та належною мірою опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційного дослідження було опубліковано 19 наукових праць, 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 індексуються у Scopus та Web of Science).

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пунктів 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 (редакція від 08.05.2024).

Оцінка змісту дисертації, її завершеності в цілому

Дисертаційна робота складається зі вступу, 6 розділів, висновків, переліку посилань та додатків. Загальний обсяг дисертації складає 252 сторінки друкованого тексту: 168 сторінок основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 5 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 247 найменувань на 25 сторінках, додатки на 39 сторінках. Робота містить 12 таблиць та 39 рисунків.

У вступі обґрунтовується актуальність дослідження, поставлена мета та визначаються основні завдання, об’єкт та предмет дослідження. Також тут викладено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача. Наводяться відомості щодо апробації та опублікованих результатів досліджень.

Перший розділ присвячено аналізу основних проблем, сучасного стану і розвитку технологій баз даних, формальних моделей, як методологічної основи побудови систем захисту, та оцінки їх безпеки. Результатом такого аналізу є висновок, що існуючі теоретичні розробки та практичні реалізації забезпечення безпеки інформаційних систем, баз даних ґрунтуються на двох парадигмах:

формального моделювання політики безпеки та криптографії. При цьому ці різні за походженням і розв'язуваною задачею підходи доповнюють один одного і вимагають подальшого вивчення. Виходячи з цього, у розділі 1 робиться висновок щодо доцільності проведення подальших досліджень, результатом яких була б деяка методологія комплексного використання різних парадигм, що призводить до підвищення ефективності захисту баз даних.

Другий розділ присвячено формалізації задачі забезпечення безпеки бази даних на основі системи захисту із повним перекриттям, визначенню показника захищеності бази даних, удосконаленню моделі Клементса–Гофмана для баз даних. Запропоновано метод оцінювання основних компонентів бар’єрів безпеки та захищеності бази даних, що є результатом синтезу удосконаленої моделі Клементса–Гофмана, інтегрального показника безпеки, положень теорії нечітких множин та ризику. Цей метод, маючи певну гнучкість, дозволяє досить просто, комплексно і кількісно оцінювати безпеку БД з різними моделями даних.

Третій розділ присвячено розробці методу маскування даних на основі обчислення операцій за модулем, методу маскування даних поля рядка таблиці бази даних, методу приховування вихідного коду збережених програм. У даному розділі проводиться порівняльний аналіз можливостей запропонованого методу маскування даних поля рядка таблиці та методу шифрування щодо приховування даних, наводяться рекомендації щодо застосування методів маскування даних, оцінки можливості використання шифрування для приховування вихідного коду збережених програм.

Четвертий розділ присвячено розробці методу контролю цілісності та справжності збережених програм, що заснований на можливостях технології блокчейн. Відповідно до запропонованого методу, було визначено структуру та правила формування первинного та наступних блоків у блокчейновому ланцюжку; запропоновано підхід до зберігання блокчейн-структури в рамках реляційної моделі даних, що полягає у відображенні цієї структури у два відношення та рекомендації щодо розміщення цих спеціальних відношень (таблиць), виходячи з обмеження можливості несанкціонованої зміни їх даних; сформульовано вимогу про необхідність підпису творцем конкретної схеми бази даних «своїх» відповідних даних, представлених в одній зі спеціальних таблиць, одним із сучасних алгоритмів електронного підпису, щоб захиститися від неправомірних дій привілейованого користувача, а також від нелегітимних дій зловмисників.

П’ятий розділ дисертаційного дослідження є логічним продовженням усіх попередніх розділів, у якому для забезпечення безпеки корпоративних БД, побудованих на основі схеми БД з УБВ, пропонується комплексне використання загальних формальних моделей управління доступом та забезпечення цілісності даних, методів, механізмів, засобів, що підтримуються системою керування БД, на платформі яких ця схема реалізується, та власних заходів забезпечення безпеки, розроблених у рамках створення інваріантної до предметної області схеми бази даних.

Шостий розділ присвячено порівняльному аналізу захищеності баз даних, що побудовані за традиційною технологією та на основі універсального базису відношень. Проведений порівняльний аналіз дозволяє зробити загальний висновок про більшу ефективність запропонованих та реалізованих у рамках схеми БД з УБВ заходів щодо забезпечення безпеки порівняно з наявними, реалізованими в рамках традиційних реляційних БД.

При викладенні матеріалу, здобувач використовує наглядні приклади та ілюстрації, які допомагають зрозуміти основні ідеї та результати досліджень. Простежується чіткий логічних зв’язок між усіма розділами дисертаційної роботи.

Список використаних джерел свідчить про те, що під час роботи було проаналізовано сучасні результати наукових досліджень.

Дисертаційне дослідження є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки баз даних.

Оформлення дисертації

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Дотримання академічної доброчесності

Аналіз дисертаційної роботи та публікацій автора не виявив порушень академічної доброчесності, елементів фальсифікації чи фабрикації тексту.

Усі результати, винесені автором дисертаційного дослідження на захист, містяться в опублікованих роботах. У роботах, що були написані та опубліковані

у співавторстві, використано лише ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків автора дисертаційного дослідження.

Недоліки та зауваження до дисертаційного дослідження

1. У дисертаційній роботі вказується на проблему реалізації механізмів контролю цілісності збережених програм, зокрема, пов'язану з визначенням періодичності запуску відповідної процедури перевірки їх цілісності, проте розширених досліджень у цьому напрямі не наводиться у роботі.

2. Деякі речення у роботі занадто довгі, і їх можна переписати на менші. Один із прикладів (п. 3.2.4, с. 113): «Враховуючи, що захист конфіденційності може забезпечити широкий спектр заходів безпеки, а кожна організація має оцінити нюанси ...».

3. Вимірювання безпеки – це складна проблема, яку не можна недооцінювати, тому автор роботи, усвідомлюючи важливість цього питання, насамперед, пов'язану з об'єктивністю, обґрунтованістю та довірою до методів оцінки безпеки баз даних, запропонував науково-методологічний, загальний підхід до вирішення цієї проблеми, заснований на розширеній моделі Клементса-Гофмана. Однак, хотілося б побачити порівняльний аналіз запропонованого підходу з іншими підходами оцінки безпеки баз даних.

Однак, слід зазначити, що вказані зауваження та недоліки суттєво не впливають на зміст та отримані науково-практичні результати дисертаційного дослідження.

Загальні висновки про дисертаційне дослідження

Дисертаційна робота Вілігури Владислава Вікторовича «Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень» є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Вілігура Владислав Вікторович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент,
доктор технічних наук, професор,
професор кафедри безпеки
інформаційних технологій
Інституту комп'ютерних технологій,
автоматики та метрології
Національного університету
«Львівська політехніка» Олена НЄМКОВА

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 00:14:41 02.01.2025

Назва файлу з підписом: ВІДГУК оф опонента Нємкова_без_засвідчення_підпису.docx.p7s
Розмір файлу з підписом: 54.0 КБ

Перевірені файли:
Назва файлу без підпису: ВІДГУК оф опонента Нємкова_без_засвідчення_підпису.docx
Розмір файлу без підпису: 36.8 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: НЄМКОВА ОЛЕНА АНАТОЛІЇВНА
П.І.Б.: НЄМКОВА ОЛЕНА АНАТОЛІЇВНА
Країна: Україна
РНОКПП: 2226707021
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 00:14:40 02.01.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F04000000C033A6011A57CD05
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в одному файлі (CAdES enveloped)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2024.10.24 15:00