

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U003653

Особливі позначки: відкрита

Дата реєстрації: 20-12-2024

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ ХНУ імені В. Н. Каразіна № 0302-Зк/157 від 05.02.2025 р.



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Вілігура Владислав Вікторович

2. Vladyslav Vilihura

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-1137-2382

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 17-01-2025

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 7314

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.02, 20.54.04, 20.56.01

Тема дисертації:

1. Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень
2. Models and methods for ensuring the security of databases with the universal basis of relations

Реферат:

1. Дисертація присвячена розробці, удосконаленню та використанню моделей та методів забезпечення безпеки баз даних. 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. У першому розділі дисертації виконано аналіз сучасного стану, основних проблем забезпечення безпеки баз даних (БД) та постановку задач дослідження. Зокрема, було проведено аналіз підходів та досягнень у галузі забезпечення та оцінки безпеки інформаційних систем загалом та баз даних, як їх основного функціонального компонента, зокрема, в тому числі проведено аналіз формальних моделей управління доступом та забезпечення цілісності даних, як методологічної основи побудови систем захисту та оцінки їхньої безпеки. За результатами аналізу виявлено недоліки та невирішені питання, що стосуються безпеки баз даних та її оцінки, виходячи з яких сформульовано задачі дисертаційного дослідження. У другому розділі вирішено завдання розробки та обґрунтування моделі захисту бази даних на основі системи безпеки з повним перекриттям та методу оцінки безпеки бази даних.

Завдяки розширенню моделі Клементса–Гофмана (Clements–Hoffman model) за рахунок включення безлічі вразливостей об'єктів (що дозволяє більш адекватно оцінювати ймовірність небажаного інциденту (реалізації загрози) у двофакторній моделі), певному інтегральному показнику захищеності БД (як величини зворотної сумарному залишковому ризику, складові компоненти якої представляються у вигляді відповідних лінгвістичних змінних), розробленому методу оцінювання основних компонент бар'єрів безпеки та захищеності бази даних в цілому, що спирається на теорію нечітких множин та ризику, стає можливою кількісна оцінка безпеки бази даних, що аналізується. Отримано перший та другий наукові результати. У третьому розділі вирішено завдання розробки та обґрунтування методів маскуванню даних, що дозволяють зменшити ймовірність реалізації загрози логічного висновку та забезпечити більш ефективне приховування коду критично важливих модулів, що постійно зберігаються, яке вимагає значно більших обчислювальних і часових витрат на його розкриття злоумисником, ніж при використанні існуючих способів, що надаються розробниками деяких сучасних систем керування базами даних (СКБД). Отримано третій, четвертий та п'ятий наукові результати, та перший практичний результат. У четвертому розділі вирішено завдання розробки та обґрунтування методу контролю цілісності та справжності модулів, що постійно зберігаються, заснованого на можливостях технології блокчейн. Отримано шостий науковий результат: вперше запропоновано метод моніторингу, 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. Отримано другий практичний результат. У п'ятому розділі вирішено завдання обґрунтування та систематизації реалізованих заходів захисту, що забезпечують конфіденційність, цілісність даних та постійно збережених модулів баз даних з універсальним базисом відношень. Ці заходи ґрунтуються як на загальних формальних моделях управління доступом, забезпечення цілісності даних, методах, засобах, механізмах, що підтримуються СКБД, на платформі якої запропонована схема реалізується, так і на власних, розроблених у рамках створення інваріантної до предметних областей схеми БД. Отримано третій практичний результат. У шостому розділі здійснено оцінку безпеки бази даних з універсальним базисом відношень та наведено порівняльний аналіз захищеності баз даних, побудованих за традиційною технологією та на основі універсального базису відношень. Порівняльний аналіз показав, що використання запропонованих у роботі рішень дозволить підвищити ефективність / результативність захисту баз даних, побудованих на основі схеми з універсальним базисом відношень, більш ніж у 1.5 рази щодо традиційних реляційних БД.

2. The thesis is devoted to the development, improvement and use of models and methods for ensuring database security. The purpose of the thesis is to increase the efficiency of protection of databases built based on the scheme with the universal basis of relations, through the development and application of models, methods and means of ensuring their security. In the first section of the thesis the analysis of the current state, the main problems of ensuring the security of databases (DB) and the formulation of research tasks are carried out. In particular, an analysis of approaches and achievements in the field of ensuring and assessing the security of information systems in general and databases, as their main functional component, was carried out, in particular, an analysis of formal models of access control and ensuring the integrity of data as a methodological basis for building protection systems and assessing their security. Based on the results of the analysis, disadvantages and unresolved issues related to the security of databases and its assessment have been identified, on the basis of which the tasks of the thesis research have been formulated. In the second section, the problem of developing and justifying the database security model based on a full overlap security system and the database security assessment method is solved. Due to the extension of the Clements–Hoffman model due to the inclusion of a set of vulnerabilities of objects (which allows for a more adequate assessment of the probability of an undesirable incident (threat realization) in a two-factor model), a certain integral indicator of database security (as the inverse of the total residual risk, the constituent components of which are represented in the form of corresponding linguistic variables), the developed method for assessing the main components of security barriers and security of

the database as a whole, based on the theory of fuzzy sets and risk, it becomes possible to quantify the security of the analyzed database. The first and second scientific results were obtained. The third section solves the problem of developing and justifying data masking methods that reduce the probability of the threat of logical inference and ensure more effective hiding of the code of critically stored modules, which requires much more computational and time costs for its disclosure by an attacker than when using the existing methods provided by the developers of some modern database management systems (DBMS). The third, fourth and fifth scientific results and the first practical result were obtained. In the fourth section, the problem of developing and substantiating a method for controlling the integrity and authenticity of permanently stored modules, based on the capabilities of blockchain technology, is solved. The sixth scientific result was obtained: for the first time a method of monitoring based on the capabilities of blockchain technology is proposed, which, unlike the known ones, allows, through the use of the created predetermined structure, rules for the formation of the primary and subsequent blocks in the blockchain chain, the organization of storage of this structure within the framework of a relational data model, methods of calculating the root of the hash tree, to strictly control the set of database programs, their integrity, authenticity with smaller volumes of data stored for this and the necessary resources processor. The second practical result was obtained. In the fifth section the problem of substantiation and systematization of the implemented protection measures that ensure confidentiality, data integrity and permanently stored database modules with the universal basis of relations is solved. These measures are based on both general formal models of access control, data integrity, methods, means, mechanisms supported by the DBMS, on the platform of which the proposed scheme is being implemented, and on our own, developed within the framework of creating a database scheme invariant to subject areas. The third practical result was obtained. In the sixth section an assessment of the security of a database with the universal basis of relations is carried out and a comparative analysis of the security of databases built on the traditional technology and on the basis of the universal basis of relations is provided. A comparative analysis has shown that the use of the solutions proposed in the work will increase the efficiency / effectiveness of the protection of databases built on the basis of the scheme with the universal basis of relations, more than 1.5 times relative to traditional relational databases.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Єсін В. І., Вілігура В. В. Дослідження основних методів і схем шифрування з можливістю пошуку. Радіотехніка. 2022. No 209. С. 138–155. <http://rt.nure.ua/article/view/262517/258939>
DOI:10.30837/rt.2022.2.209.14
- 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. <http://rt.nure.ua/article/view/268563/264142>
DOI:10.30837/rt.2022.3.210.04
- Єсін В. І., Вілігура В. В. Основні категорії NewSQL баз даних та їх особливості. Радіотехніка. 2022. No 211. С. 37–66. <http://rt.nure.ua/article/view/278029/272798> DOI:10.30837/rt.2022.4.211.03
- Єсін В. І., Вілігура В. В., Сватовський І. І. Забезпечення безпеки у розподілених інформаційних системах: основні аспекти. Радіотехніка. 2023. Вип. 214. С. 32– 63. <http://rt.nure.ua/article/view/297954/290786>
DOI:10.30837/rt.2023.3.214.04
- Єсін В. І., Вілігура В. В., Узлов Д. Ю. Огляд існуючих моделей та основних принципів нульової довіри. Радіотехніка. 2024. Вип. 217. С. 39–54. <http://rt.nure.ua/article/view/310808/302048>
DOI:10.30837/rt.2024.2.217.03

- 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). <https://www.mdpi.com/2076-3417/11/18/8781> <https://doi.org/10.3390/app11188781>
- 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). <https://www.mdpi.com/2076-3417/11/23/11175> <https://doi.org/10.3390/app112311175>
- 8. 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) <https://www.mdpi.com/2076-3417/13/20/11525> <https://doi.org/10.3390/app132011525>

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U109939

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Узлов Дмитро Юрійович

2. Uzlov Dmytro Yu.

Кваліфікація: к. т. н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Малахов Євгеній Валерійович

2. Eugene Malakhov

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-9314-6062

Додаткова інформація:**Повне найменування юридичної особи:** Одеський національний університет імені І. І. Мечникова**Код за ЄДРПОУ:** 02071091**Місцезнаходження:** вул. Дворянська, буд. 2, Одеса, 65082, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****Власне Прізвище Ім'я По-батькові:**

1. Немкова Олена Анатоліївна

2. Olena Nyemkova

Кваліфікація: д. т. н., професор, 05.13.21**Ідентифікатор ORCID ID:** 0000-0003-0690-2657**Додаткова інформація:****Повне найменування юридичної особи:** Національний університет "Львівська політехніка"**Код за ЄДРПОУ:** 02071010**Місцезнаходження:** вул. Степана Бандери, буд. 12, Львів, 79013, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****Рецензенти****Власне Прізвище Ім'я По-батькові:**

1. Пономар Володимир Андрійович

2. Volodymyr Ponomar

Кваліфікація: к. т. н., 05.13.21**Ідентифікатор ORCID ID:** 0000-0001-5271-2251**Додаткова інформація:****Повне найменування юридичної особи:** Харківський національний університет імені В. Н. Каразіна**Код за ЄДРПОУ:** 02071205**Місцезнаходження:** майдан Свободи, буд. 4, Харків, Харківський р-н., 61022, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****Власне Прізвище Ім'я По-батькові:**

1. Олійников Роман Васильович

2. Roman Oliynykov

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-3494-0493

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Горбенко Іван Дмитрович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Горбенко Іван Дмитрович

**Відповідальний за підготовку
облікових документів**

Шевченко Андрій Олександрович

Реєстратор

УкрІНТЕІ

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна