НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«СИСТЕМНИЙ АНАЛІЗ ЗАХИЩЕНОСТІ ТА ОРГАНІЗАЦІЇ РЕЛЯЦІЙНИХ БАЗ ДАНИХ»

Виконав здобувач 2 курсу
Рівень магістр
Галузь знань 12 «Інформаційні технології»,
спеціальність 124 «Системний аналіз»
Роговий Геннадій Олексійович

Керівник: к.т.н., доцент
Трофименко Олена Григорівна

Рецензент: к.пед.н., доцент
Логінова Наталія Іванівна

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет кібербезпеки та інформаційних технологій
Кафедра інформаційних технологій
Галузь знань: 12 Інформаційні технології
Спеціальність: 124 Системний аналіз
Назва освітньої програми: Аналіз та безпека даних

ЗАТВЕРДЖУЮ
Завідувач кафедри інформаційних технологій
доцент Н.І. Логінова
_____«____»_____20__ року

З А В Д А Н Н Я

на кваліфікаційну (магістерську) роботу
здобувачу Роговому Геннадію Олексійовичу

1. Тема роботи: «Системний аналіз захищеності та організації реляційних баз даних»
Керівник роботи: к.т.н, доцент Трофименко Олена Григорівна
затверджені наказом НУ ОЮА від «23» жовтня 2023 року № 3487-6
2. Строк подання здобувачем роботи «01» лютого 2024 рік
3. Дата видачі завдання «01» червня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Теоретико-методологічні засади розвитку реляційних баз даних	25.09.2023	
2	Характеристика методів захисту реляційних баз даних	27.10.2023	
3	Моделювання систем захисту реляційних баз даних	22.12.2023	
4	Оформлення пояснювальної записки	14.01.2024	
5	Рецензування роботи	20.01.2024	
6	Попередній захист	10.02.2024	
7	Захист	13.02.2024	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Системний аналіз захищеності та організації реляційних баз даних” на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 124 “Системний аналіз”, освітньою програмою: “Аналіз та безпека даних” містить 8 рисунків, 1 таблицю, 3 додатки, 45 літературних джерел за переліком посилань. Робота виконана на 59 сторінках загального тексту і 53 сторінках основного тексту.

Метою даної магістерської роботи є системний аналіз захищеності та організації реляційних баз даних з урахуванням актуальних вимог та викликів інформаційної безпеки.

Об'єктом дослідження є процеси, системи та явища, пов'язані із захистом реляційних баз даних.

Предметом дослідження є аналіз властивостей та організації реляційних баз даних для забезпечення їхньої ефективної захищеності від загроз та атак.

Розроблено коди моделі виявлення та відповіді на інциденти для підвищення рівня захищеності баз даних в реальних умовах експлуатації

БАЗА ДАНИХ, ШИФРУВАННЯ, СИСТЕМИ ЗАХИСТУ

ABSTRACT

Qualification work on the topic “System analysis of security and organization of relational databases” for the second (master's) level of higher education in the specialty 124 “System Analysis”, educational program: “Data Analysis and Security” contains 8 figures, 1 table, 3 appendices, 45 references. The work is executed on 59 pages of the general text and 53 pages of the main text.

The purpose of this master's thesis is a systematic analysis of the security and organization of relational databases, taking into account current requirements and challenges of information security.

The object of research is the processes, systems, and phenomena associated with the protection of relational databases.

The subject of the study is the analysis of the properties and organization of relational databases to ensure their effective protection against threats and attacks.

The codes of the incident detection and response model are developed to increase the level of database security in real-world conditions.

DATABASE, ENCRYPTION, SECURITY SYSTEMS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ABAC – (Attribute-Based Access Control) контроль доступу на основі атрибутів
DAC – (Discretionary Access Control) дискреційний контроль доступу, вибіркове керування доступом
DBA – (database administrator) адміністратор бази даних
DES – (Data Encryption Standard)
HMAC – (hash-based message authentication code) код аутентификации (проверки подлинности) сообщений
HOTP – (HMAC-Based One-Time Password Algorithm) алгоритм захищеної автентифікації з використанням одноразового пароля
MAC – (Mandatory Access Control) обов'язковий контроль доступу
MLS – (Multi-Level Security) багаторівнева безпека
RBAC – (Role-Based Access Control) контроль доступу на основі ролей
RDB – Relational Data Base
RSA – (абревіатура від прізвищ Rivest, Shamir та Adleman) криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі
SSL – Secure Sockets Layer
TCB – Trusted Computing Base
TCP – (Transmission Control Protocol) протокол управління передачею
TOTP – (Time-based One-Time Password Algorithm) алгоритм створення одноразових паролів для захищеної аутентифікації, що є покращенням HOTP
БД – база даних
РБД – реляційна база даних
СКБД – система керування базами даних

ВСТУП

Залежність організацій від комп’ютерних технологій зумовлює актуальність забезпечення надійного захисту інформації. Невдачі в роботі систем баз даних спричиняють значні фінансові втрати у різних сферах діяльності. Однією з актуальних проблем у галузі сучасних комп’ютерних технологій є забезпечення безпеки баз даних.

Для забезпечення захисту баз даних важливо встановити конкретні правила, які забезпечать комплексний захист. Бази даних є фундаментом для будь-якої сучасної програмної вебсистеми з динамічним контентом. Головною задачею системних адміністраторів є забезпечення безпеки баз даних. Є кілька варіантів вирішення цього: регулярне резервне копіювання, ускладнення паролів та встановлення ієрархії прав користувачів.

Метою магістерської кваліфікаційної роботи є системний аналіз захищеності та організації реляційних баз даних з урахуванням актуальних вимог та викликів інформаційної безпеки.

Для досягнення поставленої мети потрібно вирішити такі *завдання*:

1. розглянути основні поняття системного аналізу в контексті інформаційної безпеки;
2. проаналізувати принципи організації та засоби захисту реляційних баз даних;
3. розглянути методи захисту реляційних баз даних
4. розробити моделювання систем захисту реляційних баз даних;
5. оцінити ефективність моделі системи захисту.

Об'єктом дослідження є процеси, системи та явища, пов'язані із захистом реляційних баз даних.

Предметом дослідження є аналіз властивостей та організації реляційних баз даних для забезпечення їхньої ефективної захищеності від загроз та атак.

Методи проведення дослідження: аналіз, синтез, абстрагування, узагальнення, індукція, дедукція, пояснення, класифікація тощо.

Наукова новизна одержаних результатів. Отримані результати полягають у визначенні оптимальних моделей виявлення та відповіді на інциденти для захисту РБД, що відповідають сучасним викликам кібербезпеки.

Практичне значення здобутих результатів. Результатом роботи є розроблені коди моделі виявлення та відповіді на інциденти для захисту реляційних баз даних. Отримані результати мають безпосереднє практичне значення для адміністраторів баз даних, кібербезпекових спеціалістів та розробників програмного забезпечення. Рекомендації, розроблені у магістерській роботі, можуть бути використані для порівняння ефективності та захищеності РБД в реальних умовах експлуатації.

Результати роботи були апробовані у публікації:

Роговий Г. Системний аналіз захищеності та організації реляційних баз даних. *Актуальні проблеми сучасної науки та освіти: матеріали X Міжнародної науково-практичної конференції.* м. Львів, 19-20 січня 2024 року. Львів: Львівський науковий форум, 2024. С. 71-73.

ВИСНОВКИ

У ході виконання магістерської роботи проведено дослідження, спрямоване на вивчення та вдосконалення систем захисту реляційних баз даних. Актуальність проблеми безпеки інформації у віртуальному середовищі зумовлена зростаючим значенням комп'ютерних технологій у діяльності організацій.

Для досягнення мети роботи використовувалися різні методи дослідження, зокрема аналіз, синтез, абстрагування, узагальнення, індукція, дедукція, пояснення, класифікація практичних аспектів систем безпеки даних.

Отримані результати дозволяють визначити оптимальні шляхи підвищення ефективності захисту реляційних баз даних, зменшуючи ймовірність інцидентів та максимізуючи відновлення системи у разі їхнього виникнення.

Зазначені у роботі методи та підходи можуть слугувати основою для подальших досліджень у сфері захисту інформації та створення більш вдосконалених стратегій безпеки в сучасних комп'ютерних системах.

У першому розділі проаналізовано сучасні методи та підходи до захисту реляційних баз даних, визначено ключові терміни та взаємозв'язки між ними.

У другому розділі розглянуто теоретичні засади та методи для розв'язання поставленої задачі. Для цього формалізовано і визначено методи захисту даних у реляційних базах.

Третій розділ роботи має практичний аспект через розроблену структуру для експериментального дослідження. Описано архітектуру програмного проєкту, реалізацію методів, а також проведення експериментів для практичної перевірки ефективності розроблених рішень. Висновок щодо ефективності системи зроблено на основі аналізу аспектів безпеки, враховуючи результати впроваджених кодів.

Дослідження в магістерській роботі спрямоване на розгляд основних понять системного аналізу у контексті інформаційної безпеки, що дозволяє глибше зрозуміти та використовувати ці принципи у сфері захисту даних.

Визначено основні принципи організації та засоби захисту реляційних баз даних, проаналізовано аспекти захисту в інформаційних системах. Детально розглянуті методи захисту реляційних баз даних, доступні інструменти та підходи для забезпечення безпеки даних.

Розроблений проєкт моделювання систем захисту реляційних баз даних враховує важливі аспекти захисту та надає практичні рекомендації щодо його впровадження. Отримані результати свідчать про необхідність впровадження комплексних заходів захисту в реляційних базах даних для ефективного управління безпекою та запобігання можливим інцидентам. Модель виявлення та відповіді на інциденти виявилася ефективною в управлінні потенційними загрозами.

Практичне значення отриманих результатів полягає у можливості впровадження рекомендацій та розроблених рішень для підвищення рівня безпеки інформації в організаціях, які використовують реляційні бази даних.