Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Шемчук Уляни Андріївни

на здобуття ступеня вищої освіти Бакалавра

Система криптографічного захисту баз даних в освітньому закладі

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.2102165.21.02.25 ПЗ

Виконала студентка 4 курсу, група КБ-21-2 — Підпис, дата 30.05.2025 — Уляна ШЕМЧУК (Ініціали, прізвище)

Керівник канд. тех. наук, доцент (Науковий ступінь, вчене звання) — Підпис, дата — Віра ТІТОВА (Ініціали, прізвище)

Нормоконтролер старший викладач (Науковий ступінь, вчене звання) — Підпис, дата 05.06.25 — Сергій МОСТОВИЙ (Ініціали, прізвище)

До захисту допускаю:

Зав. кафедри кібербезпеки — Підпис, дата 5.06.25 — Юрій КЛЬОЦ (Ініціали, прізвище)

5 06 2025р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
15 лютого 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Шемчук Уляни Андріївни

1 Тема роботи Система криптографічного захисту баз даних в освітньому закладі

Керівник роботи к.т.н, доц. кафедри кібербезпеки Віра Юріївна Тітова

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 02.06.2025

3 Вихідні дані до роботи створити систему криптографічного захисту баз даних в освітньому закладі

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Обґрунтування вибору інформаційної системи танцювальної школи. Аналіз загроз безпеці баз даних в освітньому середовищі. Огляд методів криптографічного захисту інформації. Оцінка ефективності моделі захисту за методологією CORAS. Проєктування захищеної архітектури бази даних. Реалізація криптозахисту та контролю доступу.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Модель загроз баз даних з порушенням конфіденційності. Модель загроз баз даних з порушенням цілісності. Структурні схеми системи.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	лютий	
Ознайомлення з предметною областю	лютий	
Дослідження існуючих рішень	лютий	
Постановка задачі	березень	
Визначення загальних принципів рішення задачі	березень	
Деталізація принципів рішення задачі	квітень	
Розробка проєктних рішень	квітень	
Апробація проєктних рішень	травень	
Оформлення пояснювальної записки згідно вимог	травень	
Оформлення графічної частини	червень	
Захист КР	червень	

Студентка _____ Уляна ШЕМЧУК

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система криптографічного захисту баз даних в освітньому закладі».

Авторка роботи: Шемчук Уляна Андріївна.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 76 с., 2 додатки, 10 рис., 40 джерел.

Графічна частина: 4 плакати.

КРИПТОГРАФІЧНИЙ ЗАХИСТ, БАЗИ ДАНИХ, ОСВІТНІЙ ЗАКЛАД, ШИФРУВАННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ.

Дипломна робота присвячена розробці системи криптографічного захисту баз даних в освітньому закладі. У роботі проведено аналіз загроз інформаційній безпеці, що можуть виникати під час обробки, зберігання та передачі даних в освітніх інформаційних системах. Розглянуто сучасні методи криптографічного захисту, зокрема алгоритми шифрування, механізми керування доступом, а також методи автентифікації та авторизації користувачів.

Запропонована система спрямована на забезпечення конфіденційності, цілісності та доступності даних у базах даних навчальних закладів. У процесі роботи було розроблено архітектуру безпеки, яка інтегрується з існуючими інформаційними системами, а також проведено тестування запропонованих механізмів у реальних умовах. Отримані результати підтверджують ефективність застосованих методів захисту та їхню відповідність сучасним стандартам кібербезпеки.

Результати дослідження можуть бути використані для підвищення рівня інформаційної безпеки в освітніх закладах та інших організаціях, що працюють із конфіденційною інформацією.

30.05.2025

ABSTRACT

Theme of the qualification work: «Cryptographic database protection system in an educational institution».

Author of the work: Shemchuk Uliana Andriivna.

Supervisor: Titova Vira Yuriivna.

Explanatory note: 76 p., 2 appendices, 10 figures, 40 references.

Graphic part: 4 posters.

CRYPTOGRAPHIC PROTECTION, DATABASES, EDUCATIONAL INSTITUTION, ENCRYPTION, INFORMATION SECURITY, AUTHENTICATION, AUTHORIZATION.

The thesis is devoted to the development of a system of cryptographic database protection in an educational institution. The paper analyzes information security threats that may arise during the processing, storage and transmission of data in educational information systems. Modern methods of cryptographic protection are considered, in particular encryption algorithms, access control mechanisms, as well as methods of user authentication and authorization.

The proposed system is aimed at ensuring the confidentiality, integrity and availability of data in the databases of educational institutions. In the course of the work, a security architecture was developed that integrates with existing information systems, and the proposed mechanisms were tested in real conditions. The results obtained confirm the effectiveness of the protection methods used and their compliance with modern cybersecurity standards.

The results of the study can be used to increase the level of information security in educational institutions and other organizations that work with confidential information.

30.05.2025

ЗМІСТ

ВСТУП

У сучасному цифровому світі інформація є одним із найцінніших ресурсів. Особливо це стосується освітніх закладів, які активно впроваджують цифрові технології для організації навчального процесу, управління адміністративними системами та зберігання академічних даних. Електронні бази даних стають невід'ємною частиною цих систем, забезпечуючи збереження великої кількості інформації, зокрема персональних даних студентів, викладачів, адміністрації, академічних результатів і фінансової документації. Проте зростання обсягів і складності даних супроводжується підвищеним ризиком несанкціонованого доступу, витоку інформації та її несанкціонованої модифікації, що створює численні загрози для безпеки.

Відтак, питання захисту баз даних набуває особливої актуальності. Одним із ключових викликів є баланс між рівнем захисту та продуктивністю системи. Використання складних криптографічних алгоритмів може значно збільшувати навантаження на сервери та впливати на швидкість доступу до баз даних. Це особливо важливо для освітніх закладів, де інформаційні системи мають забезпечувати одночасну роботу великої кількості користувачів, включаючи студентів, викладачів та адміністрацію.

Ще одним важливим аспектом є інтеграція криптографічних рішень із наявними системами управління базами даних. Оскільки багато освітніх установ вже використовують певні програмні рішення, впровадження нових механізмів безпеки не повинно порушувати їхню стабільну роботу. Крім того, необхідно враховувати сумісність криптографічних методів із різними платформами та забезпечувати їхню гнучкість для подальшої модернізації.

Управління криптографічними ключами є ще одним критично важливим завданням. Необхідно не лише забезпечити їхній надійний захист від компрометації, а й організувати ефективний механізм розподілу, зберігання та оновлення ключів.

Також слід враховувати людський фактор. Навіть найсучасніші засоби безпеки можуть бути неефективними у разі недостатньої обізнаності персоналу щодо правил роботи з конфіденційною інформацією. Тому важливим завданням є впровадження навчальних програм для співробітників та студентів, які допоможуть уникнути випадкових витоків даних і соціальної інженерії.

Окрім технічних аспектів, велике значення має відповідність міжнародним стандартам інформаційної безпеки. Дотримання цих норм не лише підвищує рівень захисту, а й сприяє довірі до закладу з боку користувачів та регуляторних органів.

Тому, ефективне впровадження криптографічного захисту в освітніх установах потребує комплексного підходу, що включає технічні, організаційні та освітні заходи. Метою даної дипломної роботи є дослідження та розробка ефективної системи криптографічного захисту баз даних для освітнього закладу. Завдання роботи полягають у комплексному аналізі сучасних криптографічних методів, вивченні існуючих рішень щодо захисту баз даних, а також розробці рекомендацій щодо оптимізації впровадження криптографічних технологій у специфічних умовах навчальних установ. Результати дослідження дозволять підвищити рівень безпеки інформаційних систем, знизити ризики витоку або несанкціонованої модифікації даних та сприятимуть подальшому розвитку сучасних методів захисту інформації в освітньому середовищі.

Актуальність теми обумовлена необхідністю створення надійних та ефективних засобів захисту даних, впровадження криптографічних технологій у базах даних навчальних установ є необхідною умовою для їхнього безпечного функціонування. Надійний захист інформації сприяє стабільній роботі освітніх платформ, електронних журналів, внутрішніх адміністративних систем, що дозволять забезпечити безпечну роботу інформаційних систем в умовах зростаючих кіберзагроз та сприятимуть підтриманню високої якості освітніх послуг у цифрову епоху.

1 АНАЛІЗ СИСТЕМ КРИПТОГРАФІЧНОГО ЗАХИСТУ БАЗ ДАНИХ В ОСВІТНІХ ЗАКЛАДАХ

1.1 Бази даних та їх проєктування

База даних (далі – БД) є основою будь-якої сучасної інформаційної системи, оскільки саме від її правильного проєктування та організації залежить ефективність зберігання, швидкість обробки, достовірність та цілісність інформації. Під базою даних розуміють впорядкований набір взаємопов’язаних даних, структурованих спеціальною системою керування, що забезпечує механізми доступу, модифікації, пошуку, відновлення та захисту інформації. У широкому сенсі концепція бази даних передбачає не лише сам набір даних, а й комплекс програмних засобів, процедур, політик і метаданих, які дозволяють користувачам та додаткам виконувати задані операції з інформацією без ризику порушити її цілісність або безпеку.

Проєктування бази даних починається з аналізу предметної області, виявлення ключових сутностей, їх властивостей та взаємозв’язків. Для освітнього закладу це означає визначити, наприклад, сутності «Студент», «Викладач», «Курс», «Група», «Аудиторія», «Розклад», «Оцінка» та інші, а також встановити правила їх взаємодії: студент навчається на курсі, викладач викладає курс, оцінка ставиться за результатами виконаної роботи. На концептуальному рівні моделлю зазвичай слугує діаграма «сутність – зв’язок», яка надає візуальне представлення структури майбутньої бази даних, допомагаючи узгодити вимоги замовника й розробника до складу даних та правил збереження. Концептуальна модель не прив’язується до конкретної технології; вона показує лише об’єкти бізнес-доменної області та їх взаємозв’язки, без зазначення типів даних або структур систем управління базою даних (далі – СУБД) [1].

Після затвердження концептуальної моделі настає етап логічного проєктування, де сутності перетворюються на відношення (таблиці), атрибути сутностей стають стовпцями таблиць, а зв’язки між сутностями реалізуються через

первинні та зовнішні ключі. Логічне проєктування передбачає нормалізацію бази даних – процес організації таблиць таким чином, щоб уникнути дублювання даних і аномалій оновлення. Нормалізація включає приведення структури до першої нормальної форми (усунення груп повторюваних атрибутів, забезпечення атомарності значень), другої нормальної форми (усунення часткових залежностей, коли атрибут залежить лише від частини складеного ключа) та третьої нормальної форми (усунення транзитивних залежностей, коли один неключовий атрибут залежить від іншого неключового). Для складніших доменних моделей інколи застосовують нормальні форми вищого порядку або розглядають денормалізацію з метою оптимізації продуктивності запитів [2].

Ключовим елементом логічного проєктування є ретельний аналіз вимог до операцій із базою даних. Якщо система передбачає великі об’єми читання аналітичних даних, то може знадобитися спеціальне проєктування таблиць із денормалізацією або створенням матеріалізованих подань. Якщо ж основне навантаження припадає на транзакції запису та оновлення, слід зосередитися на оптимізації блокувань, підборі індексів і розбитті даних на партиції. У будь-якому разі вже на логічному етапі проєктування варто передбачити можливість масштабування: горизонтального (розбиття таблиць за ключами) або вертикального (розподіл різних модулів даних на окремі сервери).Після завершення логічного моделювання починається фізичне проєктування, що прив’язує модель до конкретної СУБД і апаратної архітектури. Тут обирають типи індексів (B-дерево, хеш-індекс, bitmap-індекс), визначають налаштування сторінкового розподілу даних, розміщення файлів бази даних у файловій системі чи на мережевому сховищі [3]. Для великих масивів інформації використовують партиціонування – горизонтальне або вертикальне, а для підвищення відмовостійкості – реплікацію і кластерні розподілені рішення. Важливо налаштувати буферний пул СУБД таким чином, щоб частина часто використовуваних даних і індексів містилася в оперативній пам’яті, зменшуючи затримки доступу.

Фізичне проєктування також охоплює розгортання механізмів резервного копіювання: плану регулярних бекапів (повних, диференційних та журналів транзакцій) і процедури відновлення, перевірені на тестовому середовищі, щоб гарантувати мінімальні втрати даних у разі відмови.

Вибір типу БД залежить від характеру інформації, яку потрібно обробляти, а також від вимог до масштабованості, доступності та гнучкості.

Однією з найпоширеніших архітектур є реляційні бази даних, що побудовані на основі математичної теорії множин і реляційної алгебри. У реляційній моделі всі дані зберігаються у вигляді таблиць, де кожна таблиця (відношення) містить рядки (записи) та стовпці (атрибути). Кожен запис ідентифікується первинним ключем, а зв'язки між таблицями задаються за допомогою зовнішніх ключів. Така структура забезпечує строгий контроль над типами даних і зв'язками між сутностями, дозволяє ефективно реалізовувати механізми нормалізації для усунення надлишковості та забезпечення цілісності [4].

Реляційні бази даних добре підходять для ситуацій, коли інформація має чітку, табличну структуру та коли важливо забезпечити транзакційність і консистентність. Вони активно використовуються у фінансових системах, кадровому обліку, електронних щоденниках, CRM-системах. Серед найвідоміших СУБД цього класу – MySQL, PostgreSQL, Oracle Database, Microsoft SQL Server. При проєктуванні реляційної бази даних велике значення має побудова Entity-Relationship – моделі, яка описує сутності, атрибути та зв'язки між ними. Подальше логічне та фізичне проєктування включає вибір типів даних, індексацію, створення обмежень цілісності, а також оптимізацію запитів [5].

З розвитком об'єктно-орієнтованого програмування виникла потреба у більш природному відображенні об'єктів програмного коду в базі даних. Так з'явилися об'єктно-орієнтовані бази даних, які дозволяють зберігати не лише дані, а й поведінку – методи, що визначають операції над цими даними. На відміну від реляційної моделі, де об'єкти представляються у вигляді окремих таблиць і зв'язків, у об'єктно-орієнтованих БД дані зберігаються у вигляді об'єктів,

аналогічно до мов програмування. Такий підхід дозволяє уникнути проблеми об’єктно-реляційного розриву та підвищити узгодженість між логікою застосунку і структурою бази.

Об’єктно – орієнтовані бази даних мають складнішу структуру, вони підтримують спадкування, інкапсуляцію та поліморфізм. Це робить їх зручними для використання у системах, де дані мають складну ієрархічну або мережеву структуру: інженерні системи, моделювання, телекомунікації. Для проєктування таких БД важливо не лише визначити класову ієрархію, а й задати механізми збереження об’єктів, керування посиланнями між ними, синхронізацію об’єктів у пам’яті з їх представленням у сховищі. Типовими прикладами СУБД цього типу є ObjectDB, database for objects, InterSystems Caché.

У свою чергу, з поширенням веб-застосунків, соціальних мереж і хмарних сервісів, де дані надходять у великих об’ємах і мають часто неструктурований або слабо структурований вигляд, актуальними стали документо-орієнтовані бази даних. Вони належать до категорії Not Only SQL – систем і оперують не таблицями, а документами, представленими у форматах JSON, BSON або XML. Кожен документ містить набір пар «ключ – значення», що дозволяє динамічно змінювати структуру записів та зберігати вкладені дані, масиви, об’єкти [6]. Ця гнучкість дозволяє швидко розробляти застосунки без необхідності жорсткої схемної моделі.

Документо-орієнтовані БД мають високу продуктивність при масштабованості, добре справляються з розподіленим зберіганням і обробкою запитів. Вони використовуються в мобільних застосунках, IoT, системах реального часу. Однією з найвідоміших реалізацій є MongoDB, що забезпечує потужні засоби агрегації, індексації, реплікації та шардінгу [7]. Проєктування такої бази даних передбачає ретельне планування структури документів, узгодження назв полів, формування колекцій за логічною ознакою, а також вибір стратегій кешування, контролю версій та обробки дублікатів. Незважаючи на відсутність строгих схем, для великих проєктів часто створюють спеціальні документи-схеми, які дозволяють описати структуру й валідувати дані на рівні додатка. Кожен із

зазначених типів баз даних має свої переваги та обмеження.

Реляційні системи забезпечують строгість і цілісність, але менш гнучкі в роботі з динамічними структурами. Об’єктно-орієнтовані моделі добре підходять для складних систем із великою кількістю взаємодіючих сутностей, але можуть вимагати складнішого налаштування і спеціалізованих СУБД. Документо-орієнтовані бази забезпечують високу швидкість розробки й масштабованість, однак потребують обережного підходу до забезпечення узгодженості та обмежень цілісності. Вибір моделі проєктування залежить від особливостей предметної області, обсягів даних, потреб у масштабуванні, очікуваної навантаженості та вимог до захисту.

У процесі проєктування бази даних особливу увагу слід приділити реалізації багаторівневих механізмів безпеки, що забезпечують захист даних як від ненавмисних помилок користувачів, так і від цілеспрямованих зловмисних дій. Ефективний захист бази даних повинен починатися з правильно сформованої політики розмежування доступу. Для цього необхідно чітко визначити ролі всіх типів користувачів системи – адміністратора, розробника, викладача, студента та для кожної ролі встановити мінімальний необхідний набір привілей згідно з принципом найменших прав [8]. Це дозволяє зменшити площу потенційної атаки та запобігти несанкціонованим діям навіть у разі компрометації облікового запису.

Наступним етапом є впровадження надійних механізмів аутентифікації та авторизації. Базовий рівень безпеки передбачає використання складних паролів, але для підвищення захищеності рекомендується застосовувати сучасні методи: одноразові паролі, двофакторну аутентифікацію через мобільні додатки або фізичні токени, а також централізовані сервіси управління обліковими записами – такі як LDAP, Active Directory або хмарні Identity and Access Management-рішення [9]. Це дозволяє централізовано контролювати політику безпеки, виявляти підозрілу активність і оперативно реагувати на інциденти, пов’язані з обліковими записами.

Крім управління доступом, важливим аспектом є впровадження логічних

обмежень на рівні самої структури бази даних. Для цього в логічній моделі слід прописати всі необхідні обмеження цілісності – PRIMARY KEY для унікальної ідентифікації записів, FOREIGN KEY для підтримки зв'язків між таблицями, UNIQUE для уникнення дублювання критично важливих полів (наприклад, електронної пошти або номера телефону), CHECK для контролю допустимих значень у полях [10]. Такі обмеження не лише гарантують коректність і несуперечливість даних, а й запобігають внесенню неправдивої, помилкової або навіть шкідливої інформації – зокрема SQL-ін'єкцій або логічно неконсистентних даних.

Загалом, проектування безпеки має відбуватись паралельно з розробкою структури бази даних, а не як окремий етап, що виконується після завершення технічного проєкту. Такий інтегрований підхід дозволяє закласти високий рівень захищеності з самого початку, зменшуючи потребу у складних пізніших модифікаціях та мінімізуючи ризики для конфіденційної та критично важливої інформації освітнього закладу.

Не менш критичним елементом комплексного захисту є забезпечення конфіденційності даних під час їх передавання та зберігання. Для цього слід реалізовувати шифрування «на льоту», тобто під час передачі даних між клієнтськими додатками й сервером бази даних. Найбільш надійним сучасним стандартом для цього є використання TLS 1.3 або SSL–з’єднань із обов’язковою верифікацією цифрових сертифікатів [11]. Такий підхід гарантує, що навіть у разі перехоплення мережевого трафіку зловмисник не зможе отримати доступ до змісту переданих повідомлень або викрасти облікові дані.

Однак шифрування передачі, лише одна частина загальної стратегії. Необхідно також впровадити шифрування даних «у стані спокою», тобто безпосередньо на сервері або в хмарному сховищі. Це досягається через механізми Transparent Data Encryption (далі – TDE), які працюють на рівні файлової системи або безпосередньо в СУБД (наприклад, MS SQL Server, Oracle, PostgreSQL із розширеннями) [12]. Завдяки TDE, навіть у випадку фізичної компрометації

сервера, резервної копії чи знімка віртуальної машини, вміст таблиць, журналів транзакцій і службових файлів залишиться захищеним і непридатним для аналізу без ключів дешифрування.

Окрему увагу слід приділити керуванню ключами шифрування, оскільки саме вони є головною ціллю зловмисників. Ключові матеріали – приватні ключі, сертифікати, токени доступу, повинні зберігатися у спеціалізованих сховищах секретів, таких як Hardware Security Module або Vault-системи (наприклад, HashiCorp Vault, AWS KMS). Ці сховища забезпечують надійний фізичний і логічний захист, дають змогу централізовано керувати доступом до ключів, застосовувати політики ротації, а також вести повний аудит усіх звернень до критично важливої інформації.

Важливо спланувати систему журналювання та моніторингу дій користувачів. Така система має забезпечувати фіксацію критичних подій, виявлення підозрілої активності, аналіз збоїв та інцидентів безпеки. До основних аспектів реалізації слід віднести:

- відстеження всіх спроб автентифікації, зокрема неуспішних входів, які можуть сигналізувати про спроби підбору пароля або несанкціонований доступ;
- фіксацію виконання привілейованих SQL-операцій (створення, видалення чи зміна таблиць, зміна прав доступу, робота з конфіденційними даними);
- моніторинг змін у схемах бази та модифікацій даних, що дозволяє виявити несанкціоновані або помилкові дії користувачів;
- аналіз підозрілих запитів (наприклад, повторювані помилкові запити), що може вказувати на спроби SQL-ін’єкцій або інші форми атак;
- зберігання логів на окремому сервері чи у хмарному сховищі з обмеженим доступом, шифруванням та цифровим підписом для забезпечення їхньої цілісності;
- встановлення регламентованого терміну збереження журналів (наприклад, 90 або 180 днів), автоматичного архівування та періодичної перевірки

на наявність аномалій [13];

– використання спеціалізованих рішень на зразок SIEM–систем (наприклад, ELK Stack, Splunk) для централізованого збору, аналізу та кореляції логів з метою оперативного реагування на загрози.

Система журналювання повинна стати невід'ємною частиною загальної архітектури безпеки, забезпечуючи контроль, прозорість і підзвітність дій у середовищі бази даних.

Необхідно з самого початку закласти стратегії резервного копіювання й відновлення: поєднувати повні, диференційні бекапи та журнали транзакцій, регулярно перевіряти відновлення на тестовому середовищі, а також захистити резервні копії шифруванням і фізичним відокремленням від основного сховища. Це знижує ризик втрати даних у разі відмови обладнання, помилок адміністрування або цілеспрямованих атак типу ransomware.

Не можна оминути відповідності законодавчим нормам і галузевим стандартам, що зобов'язує реалізовувати механізми анонімізації та псевдонімізації чутливих даних (ПІБ студентів, контактні дані), а також встановлювати чіткі терміни їхнього зберігання. У великих навчальних закладах має сенс впровадити Data Protection Officer і внутрішні процедури оцінки ризиків Data Privacy Impact Assessment, щоб систематично виявляти та усувати вразливості [14].

Також, безпека бази даних – це не лише технічні засоби, а й організаційні заходи: регулярне навчання персоналу, тестові «червоні команди» (penetration testing) для виявлення слабких місць, інструкції з реагування на інциденти й чіткі ролі відповідальних.

Не менш важливо, у процесі впровадження нової бази даних необхідно організувати комплексне тестування навантаження, яке дозволить виявити потенційні «вузькі місця» ще до виходу системи в експлуатацію. Спочатку формуються сценарії, що імітують пікові ситуації: масову реєстрацію студентів, одночасну обробку результатів іспитів або запуск пакетних завдань із оновлення розкладу. Для цього створюють окреме тестове середовище, максимально схоже на

продакшн, з такими ж параметрами серверів, дискових підсистем і налаштуваннями кешування.

Тестові дані генерують із максимально реалістичною структурою, відтворюючи всі особливості реального навантаження – великі текстові поля, бінарні файли та зв'язки між таблицями. Інструменти на кшталт JMeter або Locust дозволяють емулювати сотні й тисячі одночасних користувачів, а готові бенчмарки (TPC-C, TPC-H) допомагають оцінити, як система справляється із транзакційними та аналітичними навантаженнями [15].

Під час тестів особлива увага звертається на поведінку запитів різної складності та співпрацю компонентів системи. Аналіз планів виконання SQL-операцій дозволяє зрозуміти, де відбуваються повільні послідовні сканування чи надмірні злиття даних, і вчасно скоригувати дизайн: додати індекси, спростити запити або оновити модель даних. Також перевіряється, як система реагує на паралельний доступ із кількох джерел – веб-додатків, ETL-задач чи BI-звітів.

Навантажувальні тести проводяться в кілька ітерацій: після кожного раунду роблять коригування – налаштовують параметри СУБД, змінюють індекси, змінюють схему партиціонування чи розподіляють ресурси на рівні операційної системи. Кожна ітерація підтверджує, що виконані зміни дійсно покращують поведінку системи під навантаженням.

Для підтримки стабільної роботи після запуску варто впровадити регулярні автоматизовані випробування: наприклад, у рамках CI/CD щотижня перевіряти, як зміни в коді або оновлення СУБД впливають на здатність бази даних обслуговувати піковий трафік [16]. Крім того, доцільно виконати стрес-тестування на межі пропускної здатності, щоб сформувати план реагування, наприклад, додаткове масштабування реплік чи перенесення частини навантаження на віддалені вузли.

Ретельне навантажувальне і стрес-тестування забезпечує упевненість у тому, що база даних витримає реальні сценарії використання в умовах освітнього закладу і дозволить запланувати її подальше розширення без ризику несподіваних збоїв.

У контексті освітнього закладу варто також передбачити аналітичні

можливості: створення окремого сховища даних (Data Warehouse) або схеми «data marts» для формування звітів про успішність студентів, відвідуваність занять, ефективність навчальних програм. Таке сховище може формуватися за допомогою ETL-процесів, які витягують дані з операційної БД, трансформують їх згідно бізнес-правил та завантажують у структуру, оптимізовану для аналітики. CASE-інструменти інтегруються з ETL-платформами і каталогами метаданих, підтримуючи обмін інформацією про структуру даних і їх призначення.

Детальне проєктування бази даних включає поєднання аналітичних, технічних і організаційних заходів: від створення концептуальної моделі та її нормалізації до фізичного налаштування СУБД, забезпечення безпеки, продуктивності та готовності до масштабування. Проєктування бази даних - це не одноразовий процес, а постійна ітеративна діяльність, що включає аналіз предметної області, виявлення сутностей і зв’язків, формалізацію вимог, побудову логічної та фізичної моделей, оптимізацію запитів, моделювання безпеки та налаштування середовища зберігання. Завдяки комплексному підходу до проектування баз даних досягається висока надійність, ефективність та гнучкість системи, що відповідає вимогам сучасної освіти та інформаційних технологій.

1.2 Загальні принципи захисту баз даних в освітніх закладах

Захист баз даних в освітніх закладах є критично важливим завданням, оскільки вони містять персональні дані студентів, викладачів і співробітників, а також навчальну, фінансову та адміністративну інформацію. Несанкціонований доступ або компрометація цих даних може мати серйозні наслідки, включаючи витік особистої інформації, підробку результатів навчання або фінансові махінації. Для забезпечення безпеки необхідно впроваджувати комплексні заходи захисту, що охоплюють різні аспекти управління даними та інформаційних систем [17].

Одним із ключових принципів захисту баз даних є контроль доступу та

автентифікація користувачів. Освітні заклади повинні забезпечувати, щоб доступ до інформації мали лише авторизовані особи відповідно до їхніх посадових обов'язків. Це реалізується через використання автентифікаційних механізмів, таких як паролі, двофакторна автентифікація або біометричні дані. Важливо також надавати користувачам лише мінімально необхідний рівень доступу для виконання їхніх функцій, що знижує ризик ненавмисних або навмисних змін у базі даних. Використання ролей і груп користувачів дозволяє гнучко управляти рівнями доступу [18].

Наступним важливим принципом є шифрування даних, яке забезпечує їхню безпеку як під час зберігання, так і при передачі. Шифрування допомагає запобігти витоку інформації навіть у разі несанкціонованого доступу до серверів або каналів зв'язку. Освітні заклади можуть використовувати сучасні криптографічні алгоритми, такі як Advanced Encryption Standard (далі – AES) або Rivest – Shamir – Adleman (далі – RSA), для захисту персональних даних студентів і викладачів. Крім того, слід впроваджувати механізми резервного копіювання, щоб у разі втрати або пошкодження даних можна було швидко відновити їх без ризику втрати важливої інформації.

Контроль змін та аудит баз даних також є важливими заходами захисту. Логування всіх дій користувачів дозволяє відстежувати, хто, коли і які операції виконував з даними. Це допомагає виявляти підозрілі дії та оперативно реагувати на можливі загрози. Регулярний аналіз журналів подій дозволяє вчасно виявляти потенційні атаки або збої в системі безпеки [19].

Фізична безпека серверів, на яких зберігаються бази даних, є ще одним важливим аспектом. Доступ до серверних приміщень повинен бути обмежений лише для відповідального персоналу, а самі сервери мають бути захищені від фізичного пошкодження, наприклад, шляхом використання систем безперебійного живлення та заходів пожежної безпеки [20].

Важливою складовою захисту є регулярне оновлення програмного забезпечення та систем управління базами даних. Багато атак стають можливими

через використання застарілих версій програмного забезпечення, які містять відомі вразливості. Тому адміністратори повинні регулярно встановлювати оновлення та застосовувати виправлення безпеки, рекомендовані розробниками.

Останнім, але не менш важливим принципом, є навчання персоналу та користувачів баз даних. Часто найбільшу загрозу безпеці становить людський фактор – використання слабких паролів, нехтування політиками безпеки або відкриття підозрілих листів. Проведення тренінгів і роз'яснювальних заходів допомагає зменшити ризик помилок, які можуть призвести до витоку або втрати даних.

Захист баз даних в освітніх закладах потребує комплексного підходу, що включає як технічні, так і організаційні заходи. Впровадження контролю доступу, шифрування, моніторингу, регулярного резервного копіювання, оновлення програмного забезпечення та навчання персоналу дозволяє забезпечити надійний рівень безпеки. Це особливо важливо в умовах цифровізації освітнього процесу, коли велика кількість конфіденційної інформації зберігається та передається в електронному вигляді.

1.3 Методи та алгоритми криптографічного захисту баз даних

Методи та алгоритми криптографічного захисту даних відіграють ключову роль у забезпеченні безпеки інформаційних систем, особливо в освітніх закладах, де зберігаються конфіденційні дані студентів, викладачів, фінансова та адміністративна інформація. Криптографія забезпечує основні принципи інформаційної безпеки, такі як конфіденційність, цілісність, автентичність і доступність даних. Найпоширенішими методами криптографічного захисту є шифрування, хешування, електронний цифровий підпис та управління криптографічними ключами.

Шифрування є основним механізмом захисту даних і передбачає їхнє

перетворення у форму, яку неможливо прочитати без спеціального ключа. Воно поділяється на два типи: симетричне та асиметричне. Симетричне шифрування використовує один і той самий ключ для шифрування і розшифрування даних, що забезпечує високу швидкість роботи, але вимагає безпечного способу передачі ключа між сторонами. Найвідомішим алгоритмом цього типу є AES, що використовує один спільний секретний ключ для шифрування та дешифрування даних. Генерація ключа для AES зазвичай відбувається шляхом випадкового вибору послідовності бітів довжиною 128, 192 або 256 біт, що визначає рівень безпеки алгоритму. Під час шифрування даних алгоритмом AES вхідне повідомлення розбивається на блоки фіксованої довжини – 128 біт, і кожен блок проходить через кілька раундів обробки, що включають операції заміни байтів, перестановки, змішування стовпців та додавання раундового ключа. Кількість раундів залежить від довжини ключа для 128-бітного ключа їх зазвичай 10, для 192-бітного – 12, а для 256-бітного – 14. Дешифрування в AES здійснюється шляхом послідовного виконання обернених операцій, що дозволяє точно відновити оригінальні дані [21]. Це схематично можна побачити на рисунку 1.1.

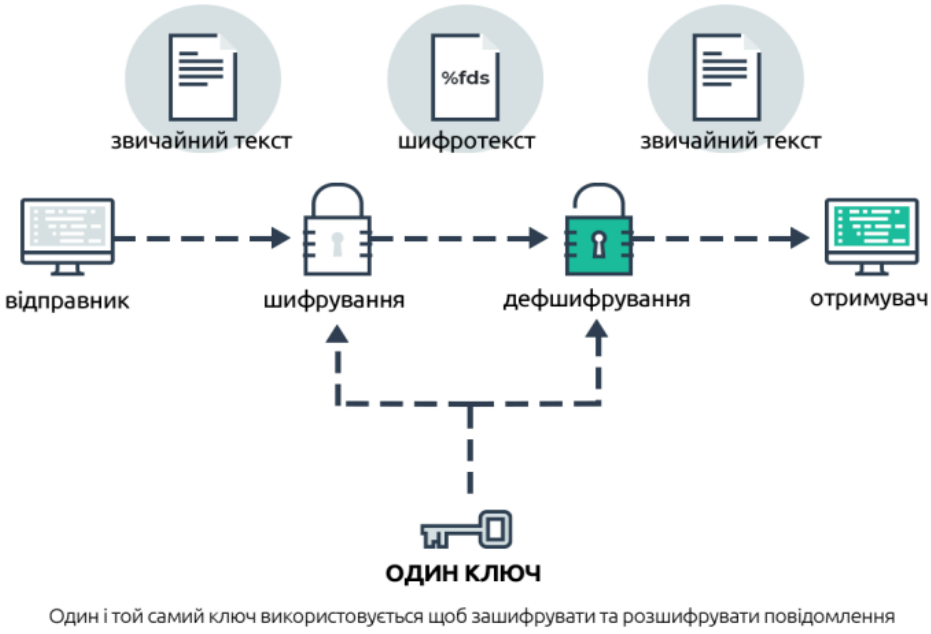


Рисунок 1.1 – Схема шифрування симетричним алгоритм

Асиметричне шифрування, рисунок 1.2, базується на використанні двох пов’язаних між собою ключів: відкритого (публічного) та закритого (приватного). Відкритий ключ застосовується для шифрування інформації, тоді як закритий, для її розшифрування. Такий підхід усуває проблему необхідності безпечної передачі ключів, що є однією з основних переваг цього методу.

Найбільш відомим алгоритмом асиметричного шифрування є RSA, який працює з парою ключів, що пов’язані математично. Генерація ключів у RSA починається зі створення двох великих простих чисел. На основі цих чисел формується частина відкритого ключа, а також додаткове значення, яке використовується для подальших обчислень. Публічний ключ створюється таким чином, щоб його параметри були взаємно простими з певним числовим значенням, отриманим із початкових простих чисел. Приватний ключ обчислюється як число, яке у певному сенсі "обернене" до відкритого – тобто дозволяє відновити оригінальне повідомлення після його шифрування.

Під час шифрування повідомлення перетворюється у числову форму, після чого за допомогою відкритого ключа створюється зашифрований текст. Для розшифрування використовується приватний ключ, який дозволяє відновити початкове повідомлення [22].

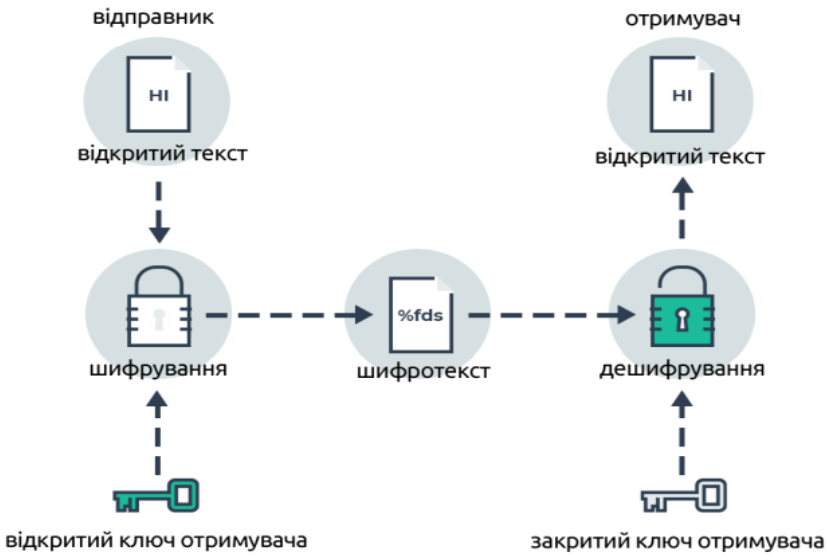


Рисунок 1.2 – Схема асиметричного алгоритму

Тому, RSA забезпечує безпечну передачу інформації за допомогою розділення ролей публічного та приватного ключів, що дозволяє використовувати його для шифрування невеликих обсягів даних або передачі секретних ключів, тоді як AES завдяки своїй ефективності та високій швидкості шифрування широко застосовується для захисту великих обсягів даних у реальному часі.

Хешування є ще одним важливим методом криптографічного захисту. Воно дозволяє створювати унікальний цифровий відбиток даних, що використовується для перевірки їхньої цілісності та автентифікації. Процес хешування полягає у перетворенні вихідного повідомлення у фіксовану за розміром хеш-строку, яка змінюється навіть при мінімальній зміні вхідних даних. Це дозволяє виявляти будь-які спроби модифікації інформації [23].

Найпоширенішими алгоритмами хешування є SHA-256 та SHA-3, які використовуються для зберігання паролів, цифрових підписів та контролю цілісності файлів. У базах даних хешування застосовується для захисту паролів користувачів, що унеможливлює їхнє прочитання навіть для адміністраторів системи. SHA-256, який належить до сімейства SHA-2, генерує 256-бітовий хеш незалежно від розміру вхідного повідомлення. Спочатку дані доповнюються: до повідомлення додається біт «1», потім - необхідна кількість нулів для досягнення потрібної довжини, і в кінці прикріплюється 64-бітове представлення довжини початкового повідомлення. Після цього повідомлення розбивається на 512-бітові блоки, які обробляються за допомогою початкових констант, вибраних із дробових частин квадратних коренів простих чисел, а потім проходять через 64 цикли обчислень із застосуванням операцій зсуву, ротації та логічних операцій, що забезпечує високий рівень стійкості алгоритму до атак. У свою чергу, SHA-3, прийнятий у 2015 році і відомий також як Keccak, базується на губчастій конструкції, що передбачає спочатку «вбирання» вхідних даних у внутрішній стан за допомогою операції XOR, а потім послідовне «виціджування» хеш-значення з цього стану через серію перестановок, виконуваних функцією Keccak-f. Основними параметрами SHA-3 є rate та capacity, сума яких дорівнює розміру

внутрішнього стану, при цьому rate впливає на швидкість обчислення, а capacity визначає рівень стійкості до криптографічних атак. Обидва алгоритми мають свої переваги та особливості, що дозволяють використовувати їх у різноманітних сферах інформаційної безпеки, від забезпечення цілісності даних до створення цифрових підписів, що робить їх незамінними інструментами сучасної криптографії [24].

Електронний цифровий підпис є криптографічним механізмом, який підтверджує автентичність даних і гарантує, що документ не було змінено після його підписання. Його застосування є особливо важливим у сфері електронного документообігу, де виникає потреба у надійному способі перевірки джерела походження інформації та забезпечення її юридичної значимості. Завдяки цифровому підпису можна з впевненістю встановити, хто саме є автором або відправником електронного документа, а також переконатися, що його зміст залишається незмінним з моменту підписання [25].

Принцип дії електроного цифрового підпису ґрунтується на поєднанні хешування та асиметричного шифрування. Перед підписанням електронний документ перетворюється у хеш-код – стислий криптографічний відбиток, який точно відповідає вмісту документа. Цей хеш потім шифрується за допомогою закритого ключа підписанта, в результаті чого утворюється сам цифровий підпис. Його можна прикріпити до документа або зберегти окремо. Для перевірки підпису отримувач використовує відкритий ключ, який розшифровує хеш-код і дозволяє переконатися в достовірності та цілісності документа.

Якщо документ було змінено після підписання, хеш, згенерований під час перевірки, вже не відповідатиме початковому значенню, що однозначно свідчитиме про втручання. Завдяки цьому цифровий підпис виконує не лише функцію підтвердження авторства, але й захисту від несанкціонованих змін. У сучасних умовах широке впровадження електронного цифрового підпису у державному секторі, бізнесі, освіті та інших галузях сприяє переходу до повноцінного електронного документообігу, де безпека і юридична чинність

електронних даних мають вирішальне значення [26].

Оскільки криптографічний захист безпосередньо залежить від безпеки ключів, важливим аспектом є управління криптографічними ключами. Якщо зловмисник отримає доступ до секретного ключа, він зможе розшифрувати будь-які зашифровані дані або підробити цифровий підпис. Тому необхідно впроваджувати надійні механізми управління ключами, серед яких резервне копіювання ключів, регулярна ротація ключів, використання спеціалізованих апаратних пристроїв для зберігання криптографічних даних Hardware Security Module та багаторівневий контроль доступу до ключів.

В освітніх закладах криптографічний захист використовується для захисту інформаційних систем, збереження конфіденційних даних студентів і викладачів, забезпечення безпеки електронного документообігу, шифрування з’єднань у внутрішніх мережах та запобігання несанкціонованому доступу до баз даних. Впровадження сучасних криптографічних алгоритмів дозволяє створити надійну систему безпеки, яка захищає інформацію від витоків, модифікації або несанкціонованого доступу. У комплексі з іншими методами захисту, такими як багаторівнева автентифікація, контроль доступу та аудит дій користувачів, криптографія є ефективним інструментом для забезпечення інформаційної безпеки в освітніх установах. Саме так, освітні заклади можуть комбінувати різні системи криптографічного захисту для створення комплексної та ефективної системи безпеки баз даних.

1.4 Аналіз існуючих рішень у сфері криптографічного захисту баз даних

На сьогодні існує багато програмних продуктів, що забезпечують криптографічний захист баз даних. Одним із найбільш поширених є Transparent Data Encryption, який реалізується в Microsoft SQL Server, Oracle Database та інших системах. Ця технологія дозволяє шифрувати дані без необхідності внесення змін

у додатки, що працюють із базою.

Ще одним популярним рішенням є Pretty Good Privacy (далі – PGP), який використовується для шифрування файлів та електронних листів. PGP дозволяє забезпечити високий рівень безпеки при обміні інформацією між користувачами [27].

Також важливу роль відіграють SSL/TLS-протоколи, які використовуються для захисту даних, що передаються через мережу. Вони встановлюють зашифроване з'єднання між клієнтом і сервером, використовуючи комбінацію симетричного та асиметричного шифрування, а також цифрові сертифікати для перевірки автентичності сторін [28]. TLS є більш сучасною і безпечною версією SSL, виправляючи його вразливості та забезпечуючи цілісність, конфіденційність і автентичність переданих даних для шифрування переданих даних між клієнтами та серверами. Це особливо актуально для веб-додатків, що працюють із освітніми базами даних.

На ринку також існує багато рішень для криптографічного захисту баз даних, які можуть використовуватися у навчальних закладах. Основними з них є:

− шифрування на рівні бази даних Transparent Data Encryption - це рішення дозволяє шифрувати окремі таблиці або всю базу даних у цілому, при цьому саме шифрування здійснюється на рівні механізму бази даних. Перевагою такого методу є те, що шифрування не вимагає змін у логіці додатків, що працюють із базою. Основні алгоритми, які використовуються в Transparent Data Encryption - AES і Triple DES [29]. Наприклад, такі системи управління базами даних, як Microsoft SQL Server, Oracle Database, PostgreSQL та MySQL, мають вбудовану підтримку Transparent Data Encryption. Однак цей метод має обмеження: він захищає дані лише під час зберігання, а під час виконання запитів вони розшифровуються, що робить їх вразливими до атак зловмисників, які отримали доступ до запущеної системи;

− Pretty Good Privacy – це популярна програма для криптографічного захисту інформації, що забезпечує конфіденційність, цілісність та автентичність

електронного спілкування та даних. Завдяки своїй ефективності та надійності, PGP знайшла широке застосування в електронній пошті, для захисту файлів, цифрових підписів та інших сфер, де необхідно забезпечити високий рівень конфіденційності [30]. Система стала стандартом для багатьох користувачів, які піклуються про безпеку своєї інформації, і продовжує розвиватися, пристосовуючись до нових вимог кібербезпеки. Вона використовує гібридну криптографію: спочатку основне повідомлення шифрується симетричним ключем (наприклад, за алгоритмом AES), а потім цей ключ шифрується публічним ключем одержувача (як правило, з використанням RSA) для безпечної передачі. Крім того, PGP дозволяє створювати цифрові підписи для перевірки автентичності і цілісності повідомлень, а система довіри працює за принципом «web of trust», коли користувачі взаємно підтверджують достовірність публічних ключів один одного. Використання PGP у освітніх закладах дозволяє захищати комунікації між викладачами та студентами, а також зберігати важливі дані в умовах зростаючих кіберзагроз, що робить її важливим інструментом для забезпечення інформаційної безпеки в сучасному цифровому середовищі;

− Hardware Security Module є апаратними рішенням для шифрування, такі як модулі безпеки які використовуються для генерації, зберігання та управління криптографічними ключами. Вони забезпечують максимальний рівень безпеки, оскільки фізично ізолюють ключі від основної системи. Подібні рішення застосовуються у фінансовій сфері та урядових установах, але можуть бути інтегровані й у систему захисту баз даних освітніх закладів для зберігання ключів шифрування у захищеному середовищі [31];

− Secure Sockets Layer та Transport Layer Security криптографічні протоколи, що забезпечують безпечну передачу даних через мережі, зокрема Інтернет. Вони працюють шляхом встановлення захищеного з’єднання між клієнтом та сервером, використовуючи комбінацію асиметричного шифрування для встановлення з’єднання та симетричного шифрування для передачі даних. Протоколи здійснюють автентифікацію сторін за допомогою цифрових сертифікатів, що

гарантує, що дані надходять саме від того, за кого вони видаються, а також використовують хеш-функції для забезпечення цілісності переданої інформації. Transport Layer Security є сучасною та більш безпечною версією Secure Sockets Layer, і сьогодні більшість систем працюють саме з TLS, що дозволяє знизити ризики перехоплення або модифікації даних під час передачі [32];

− BitLocker та VeraCrypt є популярними рішеннями для шифрування даних на рівні дисків, що допомагають захищати конфіденційну інформацію від несанкціонованого доступу. BitLocker – це вбудований інструмент у операційну систему Windows, який дозволяє шифрувати жорсткі диски та знімні носії даних. Він використовує апаратні засоби, такі як Trusted Platform Module, для зберігання криптографічних ключів, що забезпечує автоматичне шифрування без необхідності втручання користувача і гарантує високий рівень захисту навіть у разі фізичного доступу до пристрою[33]. Водночас, VeraCrypt – це безкоштовне програмне забезпечення з відкритим вихідним кодом, яке є спадкоємцем проекту TrueCrypt. VeraCrypt дозволяє створювати зашифровані контейнери, шифрувати окремі розділи чи цілі накопичувачі, а також має можливості для створення схованок (hidden volumes) всередині зашифрованих томів. Завдяки використанню декількох криптографічних алгоритмів та багатократних раундів шифрування VeraCrypt забезпечує високий рівень безпеки і є ефективним інструментом для захисту важливих даних у різних операційних системах [34].

1.5 Постановка задачі

У рамках даної дипломної роботи поставлено завдання дослідити існуючі методи криптографічного захисту баз даних, оцінити їхню доцільність і ефективність у контексті функціонування освітніх закладів, а також створити прикладну модель захисної системи, яка забезпечує комплексне шифрування, контроль доступу та фіксацію подій, з урахуванням реальних обмежень

інфраструктури закладу, зокрема танцювальної школи.

Для досягнення цієї мети необхідно вирішити такі завдання:

− проаналізувати існуючі криптографічні методи захисту даних, такі як симетричне та асиметричне шифрування, гібридні схеми, захист каналів передачі, а також оцінити їх ефективність, продуктивність і стійкість до відомих атак в умовах обмежених ресурсів;

− дослідити загальні принципи інформаційної безпеки, зокрема конфіденційності, цілісності, доступності та автентичності, а також визначити типові загрози, які виникають у процесі обробки й зберігання інформації в освітньому середовищі;

− оглянути сучасні технології шифрування на різних рівнях інформаційної системи: на рівні файлової системи, бази даних, прикладного рівня та каналу передачі даних, і визначити їхню релевантність до архітектури типового освітнього закладу;

− спроєктувати багаторівневу модель захисту даних, яка включає механізми автентифікації користувачів, захищеної передачі даних, шифрування при зберіганні, журналювання дій та обмеження доступу на основі ролей;

− реалізувати дану модель у вигляді окремого захисного модуля в умовах імітації інформаційної системи освітнього закладу та здійснити тестування на стійкість до типових загроз;

− провести порівняльний аналіз ефективності роботи системи до й після впровадження захисного функціоналу, з метою обґрунтування доцільності використання криптографічного захисту в подібних установах.

У результаті виконання дипломної роботи буде розроблено комплексне рішення – модель криптографічного захисту, яке враховує специфіку освітніх організацій, мінімізує ризики витоку, несанкціонованого доступу та зловмисної модифікації інформації. Результати тестування, дозволять підтвердити практичну ефективність розробленої архітектури та обґрунтувати можливість її масштабування на інші установи з подібною структурою й потребами.

2 ПОБУДОВА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ В ОСВІТНЬОМУ ЗАКЛАДІ

2.1 Особливості інформаційної безпеки в освітньому закладі

У межах даного дослідження об’єктом розробки системи криптографічного захисту виступає інформаційна система приватної танцювальної школи. Заклад функціонує як сучасний комерційний центр хореографічної освіти, орієнтований на клієнтів різного віку - дітей, підлітків та дорослих.

Танцювальна школа пропонує широкий вибір хореографічних напрямів, серед яких джаз-модерн, контемпорарі, хіп-хоп, брейк-данс, стріп-денс, акробатика, стретчінг, пілатес, а також ритміка для дітей від трьох років. Навчання відбувається як у форматі групових занять, так і в індивідуальному режимі, що дозволяє враховувати індивідуальні потреби кожного учня [35]. Педагогічний колектив складається з кваліфікованих фахівців із профільною освітою, які регулярно проходять підвищення кваліфікації на професійних тренінгах і майстер-класах, що гарантує високий рівень викладання. Основна діяльність закладу полягає в організації навчального процесу, формуванні груп, складанні та коригуванні розкладу занять, обліку відвідуваності, прийомі та обробці заявок від нових клієнтів, управлінні оплатами та комунікації між усіма учасниками освітнього процесу. Уся ця діяльність передбачає активне використання цифрової інфраструктури, яка є доступною через веб-інтерфейс і постійно оновлюється як зі сторони адміністрації, так і користувачів.

Інформаційна система включає центральну базу даних, вебсайт з функціоналом особистих кабінетів, адміністративну панель для керівника закладу, а також окремі облікові записи для викладачів і клієнтів. Адміністративна частина надає можливість додавати або редагувати навчальні групи, вносити зміни до розкладу, керувати фінансовими надходженнями, аналізувати статистику відвідуваності, контролювати активність користувачів та взаємодіяти з ними. Викладачі мають обмежений доступ лише до інформації, що стосується їхніх учнів

і занять: списки груп, рівень підготовки учнів, відвідуваність, короткі замітки чи коментарі. Клієнти системи (учні або їхні батьки) можуть переглядати розклад занять, залишати запити або коментарі, отримувати повідомлення та слідкувати за особистим прогресом.

У базі даних зберігається декілька категорій важливої інформації. Зокрема, персональні дані клієнтів включають повне ім’я, дату народження, адресу проживання, контактний номер телефону, електронну пошту, вікову групу, а також, за потреби, фото для внутрішньої анкети. Якщо клієнтом є неповнолітня особа, до системи також вноситься інформація про одного з батьків або законного представника: їхнє ім’я, контактні дані та договірні реквізити. До окремої категорії належать фінансові відомості: історія платежів, способи оплати (готівка, банківська картка, онлайн-оплата), використані знижки або промокоди, а також наявність або відсутність заборгованості. Окрім цього, в системі зберігаються освітні дані – розклади занять, назви груп, рівні підготовки, участь у заходах, оцінки викладачів, інформація про пропуски та можливі медичні обмеження [36].

Окремо зберігаються облікові дані всіх користувачів, включаючи логіни, хешовані паролі, ролі в системі (адміністратор, викладач, клієнт), а також журнал подій: час входу, спроби доступу, виконані дії тощо. Ця інформація є високочутливою, адже стосується як неповнолітніх осіб, так і фінансових операцій. Особливо критичними є персональні ідентифікаційні дані: повне ім’я, дата народження, адреса, номер телефону, медичні особливості, а також фінансові записи. Потрапляння цих відомостей у руки зловмисників може призвести до правових проблем, фінансових збитків, репутаційної шкоди для закладу та втрати довіри з боку клієнтів.

Інформаційна система школи взаємодіє з клієнтами через інтернет, що відкриває можливості для зовнішніх атак. Найбільш поширеними загрозами є спроби несанкціонованого доступу, фішингові кампанії, шкідливе програмне забезпечення, атаки типу SQL-ін’єкція, перехоплення незашифрованого трафіку, використання вразливостей вебсервера, а також перебір або викрадення паролів.

Особливо небезпечною є ситуація, коли під час онлайн-оплати або реєстрації дані передаються у відкритому вигляді, без належного шифрування, що дозволяє зловмисникам їх перехопити й використати.

Не менш серйозні загрози походять зсередини – від персоналу, який має надмірні або неконтрольовані права доступу. Наприклад, викладач може отримати доступ до платіжної історії клієнта або до контактних даних сторонніх осіб, що є порушенням політики конфіденційності. Також не слід виключати технічні помилки – випадкове видалення або зміна даних, збої в оновленні системи, втрати через відсутність резервного копіювання.

Узагальнюючи, можна зробити висновок що, інформаційна система танцювальної школи є складним середовищем, яке обробляє, зберігає та передає великий обсяг персональних, фінансових і навчальних даних. Це створює нагальну потребу у впровадженні комплексної системи захисту, що охоплює як технічні засоби (шифрування даних, захищені канали зв’язку, аутентифікація), так і організаційні заходи (розмежування доступу за ролями, аудит дій користувачів, політики управління ризиками). У наступних підрозділах буде виконано побудову моделі загроз із використанням методології CORAS, проведено оцінку рівня ризиків, а також запропоновано оптимальний набір заходів захисту, що забезпечить надійну роботу системи в умовах реального освітнього процесу.

2.2 Модель захисту інформації в освітньому закладі

CORAS-модель є ефективним інструментом для формалізованого аналізу ризиків інформаційної безпеки, який базується на побудові графічних і табличних описів зв’язків між активами, загрозами, вразливостями, інцидентами та наслідками. У межах цього підрозділу CORAS буде застосовано для моделювання потенційних загроз для бази даних танцювальної школи, що містить критично важливу інформацію – персональні дані учнів, записи про оплату, відвідування,

результати змагань та інші елементи освітнього процесу. Модель дозволяє наочно показати, які саме компоненти системи є вразливими, яким чином можуть реалізуватися загрози, які інциденти це спричинить та які наслідки матиме порушення безпеки.

Застосування CORAS у даному контексті охоплює три окремі аспекти: конфіденційність, цілісність і доступність бази даних. Для кожного з цих напрямів буде створено окрему модель, у якій база даних виступатиме основним активом. Аналіз зосереджуватиметься на типових загрозах, таких як несанкціонований доступ, навмисне чи випадкове пошкодження структури даних, технічні збої, помилки адміністрування або деструктивна поведінка користувачів. У результаті буде визначено критичні вектори ризику, які потребують першочергової уваги при проєктуванні та впровадженні заходів захисту. Побудовані моделі слугуватимуть основою для подальшої розробки оптимальних технічних і організаційних рішень у системі безпеки танцювальної школи. На рисунку 2.1 відображено Coras – модель баз даних , що відображає загрози для конфіденційності.

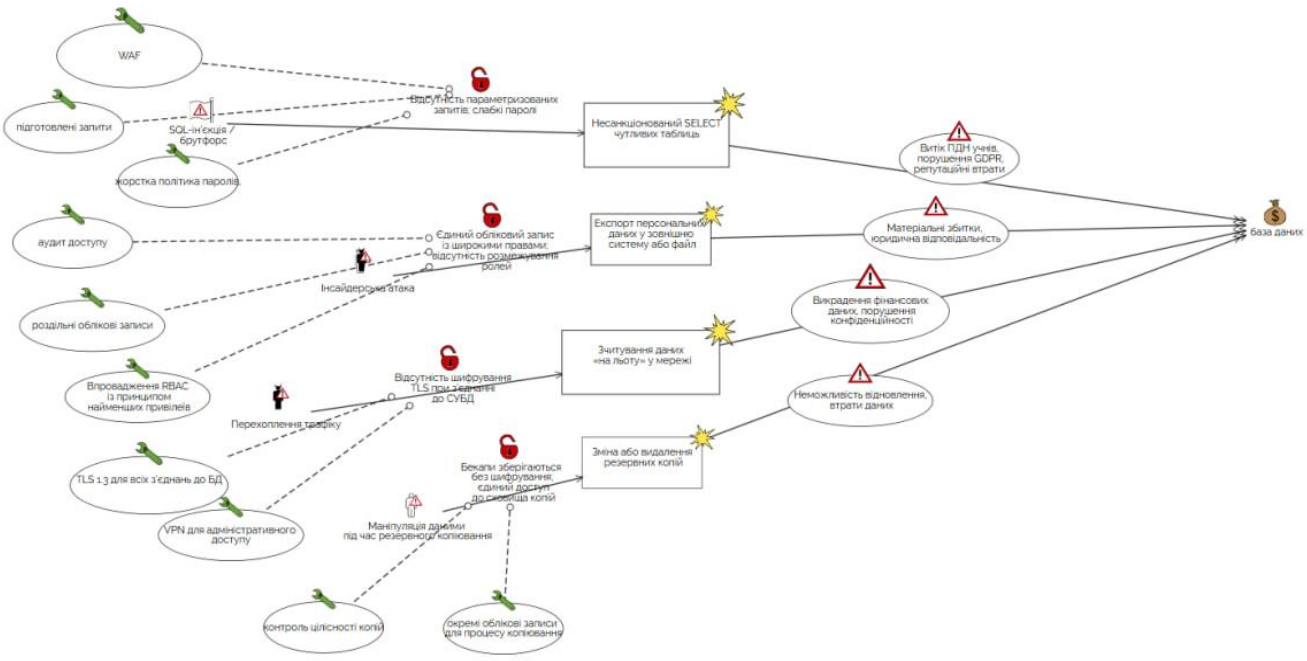


Рисунок 2.1 – Coras – модель баз даних загроз конфіденційності

Суттєвим ризиком для конфіденційності даних танцювальної школи є відсутність параметризованих запитів та надто прості політики паролів, що створює сприятливі умови для ін’єкції SQL-кодів і автоматизованого підбору облікових даних. У разі експлуатації таких вразливостей зловмисник може сформувати некоректні запити до таблиць із персональними відомостями учнів, отримавши несанкціонований доступ до конфіденційної інформації, що суперечить вимогам українського законодавства й GDPR і призводить до репутаційних втрат. Щоб мінімізувати цей ризик, застосовують Web Application Firewall із глибинним аналізом трафіку, впроваджують у коді прикладних модулів підготовлені SQL-запити, а також забезпечують багатофакторну автентифікацію й регулярне оновлення складних паролів для всіх облікових записів із підвищеними правами [37].

Не меншу загрозу становить внутрішній користувач, адже використання єдиного облікового запису з надмірними привілеями дозволяє відкрити повний доступ до експорту персональних даних без будь-якого аудиту чи розмежування ролей. Така ситуація може призвести до несанкціонованого копіювання відомостей у зовнішні файли або системи, спричиняючи матеріальні збитки та юридичні наслідки. У відповідь на цей виклик реалізують модель керування доступом на основі ролей із принципом найменших привілеїв, розділяючи функції адміністратора, бухгалтера та менеджера, а також впроваджують постійне журналювання операцій у чутливих таблицях із зберіганням логів у відокремленому, доступному лише для аудиту сховищі.

Завдяки відсутності шифрування TLS при підключенні клієнтів до сервера бази даних мережевий трафік залишається вразливим до перехоплення або підміни пакетів, що відкриває шлях до компрометації логінів, паролів, запитів SELECT та результатів запитів. Для захисту каналів зв’язку застосовують протокол TLS 1.3 із сертифікатами високого рівня захисту та рекомендують адміністраторам підключатися через VPN-тунелі з двофакторною автентифікацією, що забезпечує цілісність і конфіденційність даних “на льоту” [38].

Неналежний захист резервних копій, які зберігаються без шифрування на спільних ресурсах із єдиними обліковими записами, створює вектор для маніпуляцій із архівами. У разі несанкціонованого доступу резервні файли можуть бути змінені або видалені, що унеможливить відновлення бази до попереднього стану та призведе до втрати критичних даних і простою адміністративних процесів. Тому всі бекапи шифрують алгоритмом AES – 256 «в стані спокою», зберігають їх у відокремленому сховищі з обмеженим доступом і регулярно перевіряють процедуру відновлення в тестовому середовищі задля впевненості в її працездатності.

На рисунку 2.2 представлено розгорнуту CORAS – модель загроз, які можуть порушити цілісність бази даних танцювальної школи. Модель відображає логічний ланцюг від наявних вразливостей до можливих небажаних подій і наслідків, що виникають у результаті інцидентів, а також демонструє впроваджені заходи захисту, спрямовані на відновлення точності, узгодженості та повноти даних після порушень.

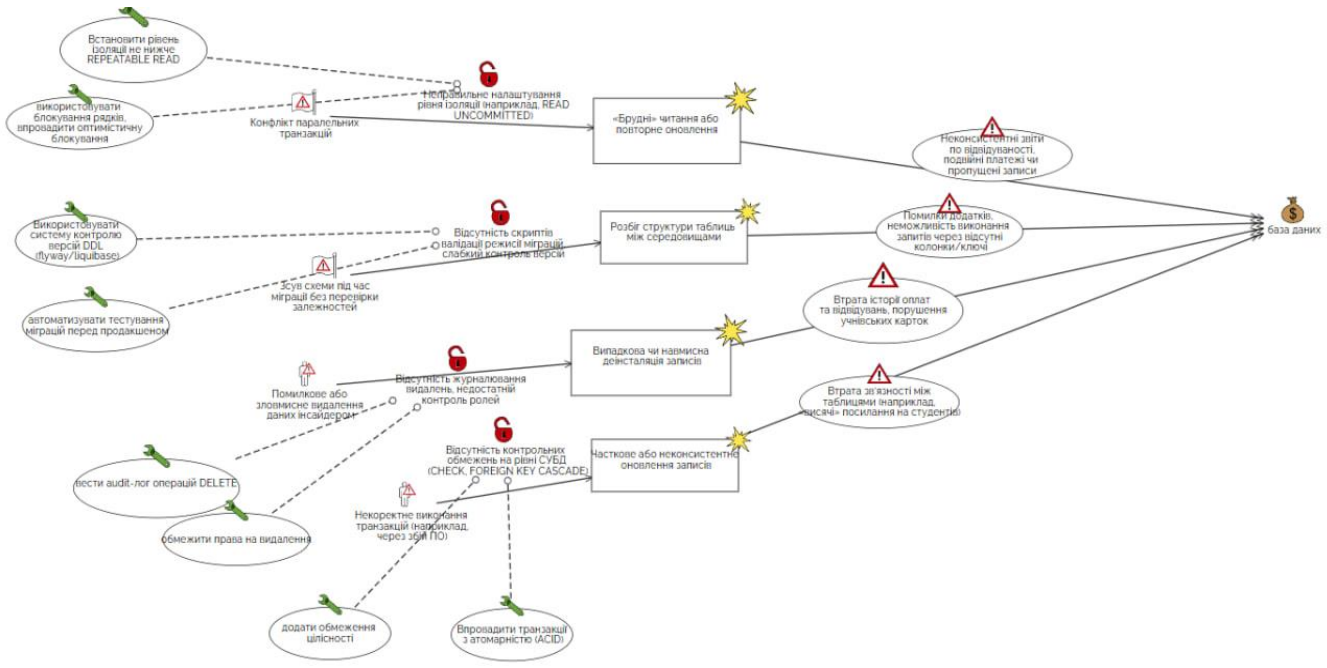


Рисунок 2.2 – Coras – модель баз даних загроз цілісності

Проведений аналіз моделі порушення цілісності бази даних танцювальної школи виявив, що без належного обмеження цілісності на рівні СУБД та контрольованого виконання транзакцій можливі критичні розбалансування даних. Відсутність механізмів rollback і чітко налаштованих зовнішніх ключів із каскадними діями створює ситуації, коли частина даних оновлюється, а інша залишається у попередньому стані, що призводить до «висячих» посилань і некоректної звітності. Навіть одноразовий збій програмного забезпечення чи перебій мережі може завершити транзакцію не повністю і фактично лишити базу у неконсистентному стані, який вимагатиме складних ручних втручань для відновлення.

Ще однією небезпекою є недоліки в управлінні обліковими записами. Використання єдиного користувача з широкими привілеями створює умови для випадкового або навмисного видалення важливих записів без можливості відслідкувати та відновити їх. Лише впровадження soft-delete із детальним audit-логом операцій і чітке розмежування ролей на підставі принципу найменших привілеїв гарантує, що всі зміни залишаться документованими і зможуть бути проаналізованими в разі інциденту.

Критичним моментом виявилося й неправильне налаштування рівня ізоляції транзакцій. На практиці це може стати причиною «брудних» або «неповторюваних» читань, які підривають довіру до фінансових і навчальних звітів. Підвищення ізоляції до repeatable read та застосування рядкових блокувань у поєднанні з оптимістичним контролем версій змін є необхідною умовою для забезпечення стабільності операцій у середовищі з багатокористувацьким доступом [39].

Неконтрольовані зміни схеми бази через відсутність системи версіонування DDL – скриптів та автоматизованого тестування міграцій створюють ризик розбіжностей між середовищами розробки, тестування та продакшну. Використання інструментів на кшталт Flyway або Liquibase у поєднанні з регулярними автоматизованими прогінками міграцій гарантує узгодженість

структури БД і дозволяє уникнути аварійних збоїв додатків [40].

Комплексне застосування усіх описаних контрзаходів формує багатошарову систему запобігання порушенням цілісності даних: від атомарності транзакцій і жорстких обмежень до чіткого аудиту й управління версіями. Це не лише мінімізує ризики появи неконсистентних даних, а й спрощує обслуговування та розвиток інформаційної системи танцювальної школи, забезпечуючи довготривалу надійність і сталість бізнес – процесів.

На рисунку 2.3 зображено ключові ризики, що можуть вплинути на доступність бази даних, а також представлено комплекс технічних і організаційних заходів, спрямованих на швидке відновлення її працездатності з мінімальними перебоями та підтримання безперервного функціонування освітньої системи.

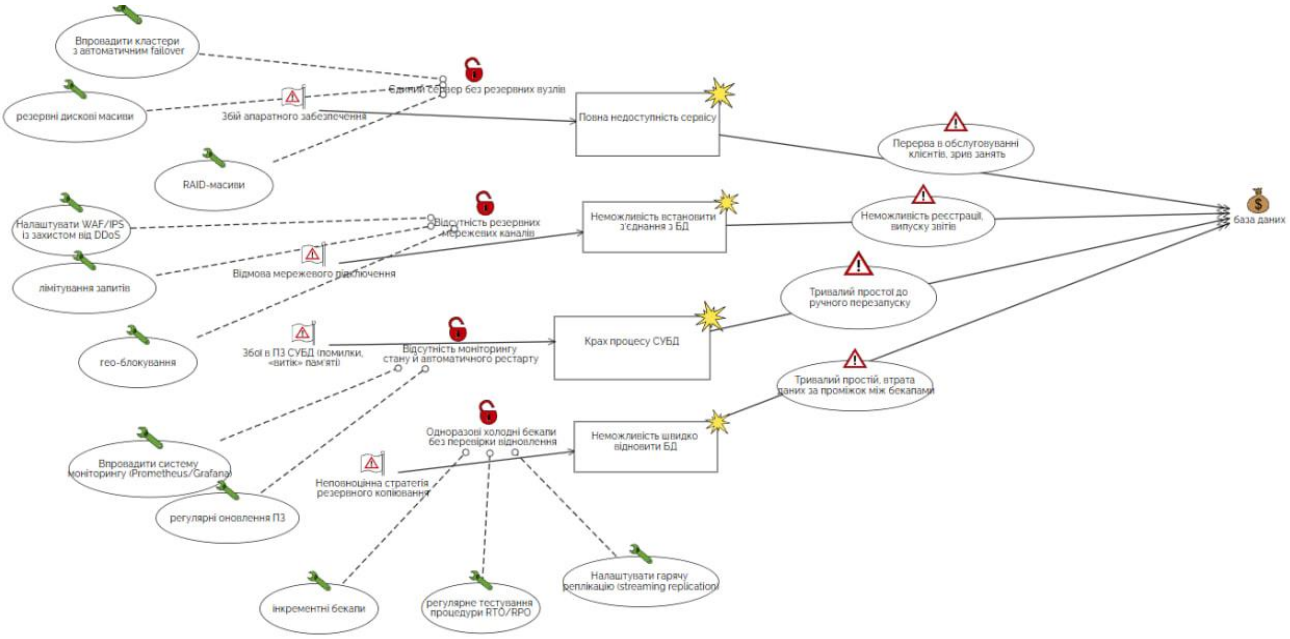


Рисунок 2.3 – Coras – модель баз даних загроз доступності

Центральна база даних танцювальної школи, розгорнута на єдиному сервері без резервних вузлів, опиняється вразливою до апаратних збоїв. Вихід із ладу дискової підсистеми або контролера миттєво позбавляє систему можливості обслуговувати користувачів, що призводить до повного зупинення адміністративних та навчальних процесів. Належним рішенням є створення

кластера з автоматичним переключенням на резервний вузол, застосування RAID-масивів для захисту даних на фізичному рівні та використання гарячих запасних серверів, готових взяти на себе навантаження без перерви в обслуговуванні.

Одночасна відмова єдиного мережевого каналу зв'язку може повністю ізолювати сервер бази даних від клієнтських додатків і користувачів, що робить недоцільним продовження будь-яких операцій. Мінімізація цього ризику досягається шляхом організації двох незалежних фізично рознесених каналів зв'язку з функцією автоматичного перемикання; у разі збою основного шляху резервний канал забезпечує безперебійний доступ до СУБД, а використання мультиглейнінгу на рівні мережевих пристроїв гарантує стійкість навіть при частковій втраті зв'язку.

Невідгородженість від розподілених атак відмови в обслуговуванні DDoS створює загрозу масового завантаження серверів і мережевих пристроїв, в результаті чого клієнтські запити блокуються або відхиляються в найвідповідальніші моменти (наприклад, під час реєстрації груп чи оплати занять). Розв'язанням є впровадження систем фільтрації та виявлення аномалій трафіку (WAF, IDS/IPS), інтеграція з CDN для розвантаження вхідного потоку та запровадження механізмів лімітування запитів і географічного блокування підозрілих адрес.

Недостатній моніторинг стану СУБД і неповноцінна стратегія резервного копіювання призводять до тривалих простоїв та втрати даних, створених після останнього знімка. Падіння процесу бази або помилки в оновленнях може залишити систему недоступною до ручного втручання. Оптимальним підходом є застосування гарячої реплікації (streaming replication) для миттєвого переключення на працездатну копію, щоденні інкрементні копії в поєднанні з повними щотижневими знімками, а також регулярне автоматизоване тестування процедур відновлення, що гарантує відповідність визначеним цілям RTO і RPO та забезпечує готовність до непередбачених збоїв.

2.3 Аналітичне обґрунтування доцільності впровадження засобів захисту бази даних

У процесі побудови ефективної системи інформаційної безпеки важливо не лише виявити можливі загрози, що можуть бути реалізовані відносно бази даних освітнього закладу, а й дати економічну оцінку доцільності впровадження відповідних захисних заходів. Такий аналіз дозволяє оптимізувати бюджет організації, зосередивши ресурси на критично важливих елементах, і водночас забезпечити належний рівень захисту інформаційних активів. У випадку танцювальної школи, база даних є ядром академічної інформаційної системи - вона містить персональні дані учнів, інформацію про викладачів, навчальні графіки, фінансові транзакції, результати відвідування, документообіг тощо. Втрата, спотворення або блокування доступу до цих даних призведе до значних операційних і репутаційних втрат.

Загрози конфіденційності – одні з найнебезпечніших у контексті діяльності будь-якого освітнього закладу, зокрема й танцювальної школи. База даних подібного типу установи містить конфіденційні персональні дані учнів: прізвище, ім’я, по-батькові, дату народження, контактні дані батьків або самих учнів, а також медичні показання, що визначають допустиме фізичне навантаження. Окрім цього, у базі зберігається фінансова інформація – дані про оплату навчання, відомості про абонементи, застосовані знижки та пільги. Також база містить інформацію про викладацький склад (контактні й посадові дані), внутрішню документацію, розклади занять, журнали відвідування .

Несанкціонований доступ до такої інформації може призвести до серйозних правових наслідків, включаючи порушення вимог чинного законодавства у сфері захисту персональних даних. Порушення норм цих актів загрожує штрафами, перевірками з боку регуляторних органів, призупиненням діяльності або втратою довіри з боку клієнтів і партнерів.

Оцінка орієнтовних збитків у разі витоку персональних даних включає кілька

компонентів: втрату довіри клієнтів (частина з них відмовляється від послуг, що призводить до недоотриманого прибутку), адміністративні штрафи (у разі перевірки відповідних органів), юридичні витрати (консультації, можливі судові справи), витрати на інформування постраждалих, а також репутаційні ризики, які можуть мати довготривалий ефект. Загальна сума збитків оцінюється на рівні 150 000 – 200 000 грн, залежно від масштабу витоку.

Вартість ефективної системи захисту конфіденційності включає: придбання серверного обладнання з апаратною підтримкою шифрування (40 000 грн), впровадження програмного забезпечення для управління доступами та шифруванням даних (25 000 грн), реалізація багатофакторної автентифікації користувачів (5 000 грн), навчання персоналу з питань інформаційної безпеки (10 000 грн). Разом витрати на запобігання загрозам становлять 80 000 грн, що більш ніж удвічі менше потенційних збитків, і з урахуванням можливої багаторазової реалізації загроз - навіть у кілька разів вигідніше.

Загрози цілісності даних полягають у несанкціонованому або ненавмисному спотворенні, зміненні чи знищенні інформації, що зберігається в базі даних. У контексті танцювальної школи це може проявлятися у підробці записів про відвідуваність учнів, фальсифікації фінансових даних (наприклад, редагуванні платіжної історії, невірному відображенні знижок чи заборгованостей), зміні оцінок або рівня досягнень учнів, а також у порушенні логіки формування розкладів занять. Усе це суттєво впливає як на внутрішні процеси, так і на взаємодію з клієнтами.

Причинами порушення цілісності можуть бути як технічні, так і людські чинники. Наприклад, помилки персоналу при введенні або редагуванні інформації, навмисні дії зловмисників – як внутрішніх (недобросовісні співробітники), так і зовнішніх (злам системи через уразливості програмного забезпечення). Також не варто виключати вплив шкідливого програмного забезпечення – вірусів, троянів або ransomware, які можуть змінювати чи шифрувати інформацію, вимагаючи викуп за її відновлення. Програмні або апаратні збої, що виникають унаслідок

неякісного обслуговування інфраструктури або через перебої з електропостачанням, теж становлять значний ризик для цілісності даних.

У сфері діяльності танцювальної школи, де інформація напряму пов’язана з обліком успішності, фінансами та репутацією, втрати чи спотворення таких даних здатні спричинити серйозні наслідки. Це може викликати конфлікти з батьками учнів, порушити навчальний процес, призвести до адміністративних помилок і, зрештою, підірвати довіру клієнтів до закладу. Тому забезпечення цілісності інформації має бути пріоритетним завданням, реалізованим через резервне копіювання, контроль доступу до записів, цифрове підписування критичних даних і автоматизований аудит змін у базі.

Оцінка потенційних збитків у разі порушення цілісності даних включає витрати на відновлення інформації (залучення IT-фахівців, перевірка резервних копій, ручна перевірка журналів), втрату клієнтів через адміністративні помилки, затримки у розкладі або виступах, конфлікти з батьками учнів. Орієнтовна сума збитків – 80 000 – 100 000 грн. Для зниження ризиків доцільно впровадити систему журналювання змін у базі даних, контроль версій записів, механізми попередження помилок при введенні, а також автоматичну валідацію інформації. Орієнтовна вартість впровадження – 35 000 – 45 000 грн. Окупність заходів забезпечується вже після одного серйозного інциденту або кількох дрібних, враховуючи повторюваний характер помилок персоналу в будь – якій системі.

Загрози доступності передбачають такі ситуації, за яких легітимні користувачі – адміністратори, викладачі, бухгалтерія або керівництво танцювальної школи – тимчасово або повністю втрачають змогу доступу до інформаційної системи або її окремих функціональних компонентів. Основними причинами цього можуть бути технічні збої в роботі програмного чи апаратного забезпечення, відмова серверного обладнання, неполадки з мережею, а також умисні дії зловмисників, зокрема атаки типу «відмова в обслуговуванні» DoS або DDoS. Додатковими факторами ризику є фізичне пошкодження інфраструктури (наприклад, унаслідок пожежі, затоплення чи стрибків напруги) або відсутність

належної системи резервного копіювання, що унеможливлює оперативне відновлення працездатності системи.

У випадку освітнього закладу, зокрема танцювальної школи, недоступність системи навіть протягом кількох годин може спричинити суттєві перебої в організації навчального процесу. Це проявляється у неможливості адмініструвати та редагувати розклад занять, реєструвати нових учнів, проводити облік відвідуваності або виконувати фінансові операції – від прийому оплат до обліку нарахувань викладачам. У разі втрати доступу до історичних записів або інформації про попередні транзакції знижується якість сервісу, зростає кількість помилок і нарікань від клієнтів.

Проте, на відміну від загроз конфіденційності чи цілісності, більшість інцидентів, пов’язаних із доступністю, мають тимчасовий характер. За умови наявності належних заходів, таких як автоматизоване резервне копіювання, відмовостійка інфраструктура, балансування навантаження та моніторинг систем у режимі реального часу, можливе швидке відновлення доступу без суттєвих довгострокових наслідків.

Саме тому підхід до забезпечення доступності в системі танцювальної школи має базуватись не лише на мінімізації часу простою, а й на здатності оперативно реагувати на кризові ситуації, підтримуючи при цьому цілісність і конфіденційність даних. Орієнтовні втрати за один день простою системи 20 000 – 30 000 грн, залежно від кількості клієнтів, інтенсивності навчального процесу та часу інциденту (наприклад, перед виступами або конкурсами збитки вищі). Для мінімізації впливу таких загроз рекомендовано впровадити UPS-систему (7 000 грн), резервне серверне обладнання або хмарний хостинг (15 000 грн), системи автоматичного резервного копіювання (10 000 грн), регулярний моніторинг працездатності (5 000 грн). Загальні витрати становлять 35 000 – 40 000 грн, а окупність забезпечується вже після двох днів відновлення системи з нуля.

Таблиця 2.1 – Узагальнена порівняльна таблиця

Атрибут безпеки	Конфіденційність	Цілісність	Доступність
Оцінка збитків при реалізації загрози	Витік персональних даних учнів, викладачів і батьків може спричинити репутаційні втрати, штрафи та юридичні наслідки. Орієнтовні збитки – до 300 000 грн.	Помилки в розкладі, оплатах, контрактах та іншій звітності можуть призвести до управлінського хаосу. Орієнтовно, збитки – до 150 000 грн.	Порушення доступу до бази даних, особливо у пікові періоди, може спричинити збої в роботі та втрату доходу. Збитки – до 100 000 грн.
Вартість впровадження захисних заходів	Впровадження шифрування, систем контролю доступу, журналювання та DLP-систем. Орієнтовна вартість – 120 000 грн.	Резервне копіювання, перевірка на логічну цілісність, валідація введення, контроль змін. Вартість – 80 000 грн.	Встановлення джерел безперебійного живлення, резервних серверів.Вартість – 90 000 грн.
Порівняння витрат і вигоди	Потенційні збитки майже втричі перевищують вартість захисту. Інвестиції є критично необхідними і економічно обгрунтованими.	Витрати співвідносяться з потенційною шкодою, тому захист слід впроваджувати у модулях, критичних до точності даних.	Незважаючи на нижчі ризики, захист доступності теж є виправданим, особливо у критичні періоди роботи школи.

Порівняльний аналіз демонструє, що хоча всі три типи загроз мають значний потенціал для шкоди, загрози конфіденційності несуть найбільші фінансові ризики, тоді як вартість впровадження необхідних засобів захисту є порівняно нижчою,

також вони є найвразливішими у контексті довгострокових репутаційних наслідків. Їх реалізація зачіпає не лише внутрішні процеси, а й зовнішню довіру до школи. Захист таких даних потребує найбільш комплексного підходу та найвищих інвестицій, однак ці інвестиції є повністю обґрунтованими в контексті можливих втрат. Отже, формування політики безпеки має відштовхуватись від моделі загроз, яка приділяє пріоритетну увагу конфіденційним аспектам, із подальшим доповненням заходами забезпечення цілісності та доступності, відповідно до специфіки діяльності закладу.

2.4 Оптимальні засоби захисту даних на основі моделей безпеки

Аналіз побудованих CORAS – моделей дозволив не лише визначити основні загрози для бази даних танцювальної школи, а й виявити взаємозв’язки між джерелами загроз, вразливостями системи та можливими наслідками для функціонування освітнього процесу. На основі цього моделювання стало можливим сформувати комплекс заходів, що є оптимальними з огляду на ефективність, економічну доцільність і практичну реалізованість у середовищі невеликої, але функціонально насиченої освітньої установи.

Визначення оптимальних засобів захисту ґрунтується на принципі багаторівневої безпеки, що передбачає створення декількох незалежних контурів оборони. Кожен з них спрямований на нейтралізацію конкретного класу загроз або мінімізацію наслідків від їх реалізації. У контексті танцювальної школи, де обробляються як персональні дані клієнтів, так і фінансова та академічна інформація, критично важливо забезпечити належний захист конфіденційності, але й захист цілісності та доступності, є теж не менш важливим.

У результаті порівняльного аналізу загроз і контрзаходів встановлено, що найефективнішими є ті засоби, які мають перехресний захисний ефект. Такі рішення одночасно знижують ризики, пов’язані з кількома загрозами. Наприклад,

впровадження багатофакторної автентифікації значно ускладнює несанкціонований доступ до системи, тим самим захищаючи конфіденційність даних, запобігаючи їх спотворенню та обмежуючи можливість порушення доступності через блокування облікових записів.

Шифрування даних є ще одним базовим засобом захисту. Воно є фундаментальним компонентом системи інформаційної безпеки, який дозволяє гарантувати конфіденційність та цілісність інформації як у процесі її зберігання, так і під час передачі. У контексті приватної танцювальної школи, де зберігається велика кількість персональних, фінансових та освітніх даних, впровадження ефективних механізмів шифрування є обов’язковим елементом загальної стратегії захисту.

На рівні збереження даних у базі використовується так зване шифрування "в стані спокою", що запобігає доступу до інформації навіть у разі компрометації фізичних носіїв, резервних копій або знімків віртуальних машин. У цьому випадку дані зберігаються у зашифрованому вигляді, і розшифрування можливе лише за наявності відповідного криптографічного ключа. Це означає, що навіть якщо зловмисник отримає прямий доступ до файлів бази даних, він не зможе їх прочитати без ключів.

Цілісність шифрованих даних підтримується через використання контрольних сум (hash-функцій) або цифрових підписів. Це дозволяє виявити навіть незначні зміни в структурі чи змісті інформації. Наприклад, якщо зловмисник намагатиметься модифікувати дані про відвідування чи оплату учня, система зможе виявити спробу несанкціонованого втручання, оскільки результат перевірки цілісності не співпадатиме з очікуваним.

Для систем, що взаємодіють з клієнтами через інтернет, надзвичайно важливим є забезпечення захищеного каналу передавання даних , зазвичай через протокол HTTPS, який базується на TLS/SSL. Такий підхід унеможливлює перехоплення конфіденційної інформації в процесі реєстрації, авторизації або онлайн – оплати. Без належного шифрування переданих даних існує ризик того, що

треті особи зможуть отримати логіни, паролі, платіжну або контактну інформацію користувачів.

Організаційні заходи не менш важливі, ніж технічні, оскільки саме людський фактор часто є найслабшою ланкою в системі захисту. Забезпечення контролю над тим, хто і до яких даних має доступ, як саме ці дії виконуються, а також наскільки системно відбувається моніторинг активності є основою надійної кібербезпеки будь-якої установи, включно з приватною танцювальною школою.

Одним з ключових механізмів є впровадження моделі контролю доступу на основі ролей RBAC. Вона передбачає чітке визначення ролей у системі – наприклад, адміністратор, викладач, бухгалтер, клієнт та закріплення за кожною роллю обмеженого набору прав. Такий підхід дозволяє уникнути ситуацій, коли користувачі отримують надлишкові повноваження, які їм не потрібні для виконання своїх обов'язків. Наприклад, викладач не повинен мати доступ до фінансових звітів або змін у розкладі інших груп, а клієнт – бачити особисті дані інших користувачів.

Розмежування прав доступу має супроводжуватися регулярним аудитом облікових записів: необхідно періодично перевіряти, чи всі користувачі активні, чи відповідають їхні ролі поточним обов'язкам, а також виявляти спроби отримання неправомірного доступу до забороненої інформації. Особливої уваги потребують облікові записи з адміністративними правами – вони повинні бути обмежені, ретельно захищені та використовуватись лише за необхідності.

Для підвищення безпеки важливо впровадити політику управління паролями, особливо коли йдеться про доступ до конфіденційних персональних та фінансових даних користувачів. Щоб мінімізувати ризик несанкціонованого входу, доцільно впровадити обов'язкову періодичну зміну паролів, наприклад, кожні 60 або 90 днів. Це дозволяє уникнути тривалого використання одного й того ж пароля, що потенційно міг бути скомпрометованим. Крім того, система має відхиляти занадто прості або поширені комбінації, такі як «123456», «password», «admin» тощо, а також забороняти повторне використання паролів, які вже застосовувалися раніше.

Для захисту від автоматизованих атак важливо реалізувати механізм автоматичного блокування облікового запису після кількох невдалих спроб входу. Це ефективно стримує спроби брутфорс – атак і дає змогу зберегти безпеку навіть за наявності слабких місць в інших компонентах системи. Додатково варто встановити вимоги до складності пароля – мінімальна довжина, наявність великих і малих літер, цифр і спеціальних символів, що значно ускладнює як ручний, так і автоматизований підбір.

Ще одним надзвичайно важливим компонентом системи захисту інформації є ведення журналів подій та логів активності користувачів. Всі дії, що виконуються в інформаційній системі, повинні ретельно фіксуватися. Зокрема, це стосується спроб входу до системи – як успішних, так і неуспішних, змін у базах даних чи конфігураціях, а також виконання привілейованих дій, які можуть мати значний вплив на безпеку чи цілісність системи.

Кожен запис у журналі має містити точну позначку часу, яка дозволяє відстежити послідовність подій, унікальний ідентифікатор користувача, що виконав дію, а також докладний опис самої операції. Це створює повну хронологію подій, що є незамінним інструментом для проведення ретроспективного аналізу у випадку інцидентів, таких як несанкціонований доступ або втручання у дані.

Окрім функції аудиту, ведення логів відіграє важливу роль у стримуванні потенційних порушень безпеки. Користувачі, які усвідомлюють, що їхні дії постійно відслідковуються та зберігаються, менш схильні порушувати встановлені правила чи політики організації. Такий психологічний фактор підвищує загальний рівень дисципліни і відповідальності серед персоналу, сприяючи підтримці безпеки інформаційної системи на високому рівні.

У сфері забезпечення доступності інформаційних систем одним із найефективніших та оптимальних рішень є регулярне резервне копіювання даних. Вкрай важливо не лише виконувати періодичне збереження копій, а й забезпечувати їх зберігання у віддалених, надійно захищених локаціях. Такий підхід дає змогу у разі виникнення катастрофічних подій – наприклад, апаратних

збоїв, природних катастроф або цілеспрямованих кібер – атак, таких як ransomware, оперативно відновити функціонування системи без значних втрат інформації.

Крім резервного копіювання, для забезпечення безперервності роботи системи застосовують технології автоматичного перемикання на резервні сервери, або так званий failover. У разі виникнення збою на основному сервері система миттєво переключається на резервний ресурс, що дозволяє мінімізувати час простою та уникнути втрати доступу користувачів до необхідних сервісів.

З-поміж сучасних технічних засобів захисту інформаційних систем особливе значення мають системи виявлення вторгнень Intrusion Detection System та системи управління інформацією й подіями безпеки Security Information and Event Management. Ці рішення виступають своєрідним «радаром» безпеки, що дає змогу своєчасно виявляти потенційні загрози та оперативно реагувати на них ще до того, як вони зможуть нанести шкоду системі.

Система IDS призначена для аналізу мережевого трафіку або поведінки користувачів з метою виявлення підозрілих дій – спроб сканування портів, несанкціонованого доступу, модифікацій даних тощо. IDS може бути як сигнатурною (тобто порівнювати події з базою відомих атак), так і поведінковою, що навчається на «нормальній» активності та сигналізує про відхилення. У контексті танцювальної школи така система здатна, наприклад, виявити підозріле багаторазове введення пароля з IP-адреси, яка раніше не використовувалась, або спроби виконати команди, що не відповідають ролі користувача.

SIEM – системи, у свою чергу, об’єднують дані з різних джерел – логів СУБД, вебсерверів, операційних систем, мережевого обладнання – та проводять їх централізований аналіз у реальному часі. Вони дозволяють не тільки виявляти складні багатоступеневі атаки (наприклад, поєднання SQL-ін’єкції та викрадення сесії), але й забезпечують аудит дій користувачів, виявлення аномалій, формування звітів і реагування на інциденти.

Завдяки таким рішенням підвищується як превентивна стійкість системи, за рахунок раннього попередження про загрози, так і реактивна здатність – швидка

локалізація й мінімізація наслідків інциденту.

Не менш важливим аспектом забезпечення безпеки інформаційної системи є своєчасне та регулярне оновлення програмного забезпечення. Це стосується як самої системи управління базами даних (СУБД), так і операційних систем, вебсерверів, серверів додатків та всіх сторонніх компонентів, які використовуються в інфраструктурі. Практика показує, що значна частина кіберінцидентів відбувається через використання вразливостей у застарілих або непатчених версіях ПЗ. Хакери активно сканують мережі в пошуках таких вразливих систем, а експлойти до них часто з'являються в публічному доступі незабаром після розкриття уразливостей.

Особливо критичним аспектом підтримки безпеки інформаційних систем є своєчасне оновлення програмного забезпечення, зокрема тих оновлень, які виправляють виявлені уразливості. Такі уразливості можуть надавати зловмисникам можливість виконувати довільний код на системі, підвищувати свої права доступу (ескалація привілеїв), викликати відмову в обслуговуванні DoS або обходити механізми автентифікації. Ігнорування або затримка з встановленням таких оновлень може призвести до серйозних наслідків, включно з компрометацією системи, втратами даних та порушенням роботи бізнес-процесів. Тому в рамках загальної стратегії захисту інформації має бути розроблена та впроваджена чітка політика оновлення програмного забезпечення. Ця політика повинна передбачати регулярну автоматичну перевірку систем на наявність нових версій і патчів, що дозволяє оперативно реагувати на появу критичних оновлень. Крім того, важливо передбачити механізм інформування відповідальних за безпеку і адміністрування осіб про доступність оновлень, щоб забезпечити своєчасне їх розгортання.

Окрему і дуже важливу увагу слід приділяти процесу тестування оновлень перед їх безпосереднім впровадженням у продуктивне середовище. Ця практика є необхідною, оскільки без належного тестування існує ризик того, що нова версія програмного забезпечення або патч може спричинити непередбачені збої, порушення роботи системи або навіть втрату критично важливих даних. Такі

наслідки можуть мати серйозний вплив на бізнес-процеси, викликати простої і фінансові втрати.

Рекомендовано використовувати спеціалізоване тестове або стейджингове середовище, яке максимально ідентичне продуктивній системі за своїми характеристиками, конфігурацією і навантаженням, але при цьому повністю ізольоване від основної інфраструктури. Це дозволяє безпечно запускати оновлення, перевіряти їх сумісність із існуючим програмним і апаратним забезпеченням, а також відстежувати їхній вплив на стабільність і продуктивність системи.

У тестовому середовищі можна виявити можливі конфлікти, помилки чи несподівані наслідки застосування оновлень, які могли залишитися непоміченими в процесі розробки. За результатами тестування приймаються рішення про готовність оновлення до розгортання в продуктивному середовищі або про необхідність доопрацювання.

В освітньому середовищі танцювальної школи, де одночасно працює як внутрішній персонал, так і запрошені викладачі, консультанти чи інші тимчасові співробітники, надзвичайно важливо організовувати регулярні та систематичні заходи з навчання з інформаційної безпеки. Такий підхід дозволяє формувати у всіх учасників освітнього процесу усвідомлене і відповідальне ставлення до захисту конфіденційної інформації, даних учнів, адміністративних документів та інших ресурсів школи.

Періодичні тренінги, семінари або короткі інформаційні сесії допомагають ознайомити співробітників з основними принципами безпечної роботи в інформаційних системах, сучасними загрозами, правилами створення і збереження паролів, безпечним використанням електронної пошти та іншими важливими аспектами кібергігієни. Крім того, навчання сприяє підвищенню обізнаності про методи соціальної інженерії, фішингові атаки та інші способи, за допомогою яких зловмисники можуть отримати несанкціонований доступ до даних.

Формування культури відповідального поводження з інформацією значно

знижує ризики, пов’язані з людським фактором – одним із найпоширеніших джерел порушень безпеки. За статистикою, більшість інцидентів у сфері інформаційної безпеки трапляються саме через необачність, недостатню обізнаність або випадкові помилки користувачів. Регулярне навчання дозволяє мінімізувати ці ризики, підвищити рівень довіри до системи безпеки та створити середовище, в якому кожен співробітник розуміє свою роль і відповідальність у захисті інформації.

Таким чином, інвестиції в підвищення кваліфікації персоналу з питань інформаційної безпеки – це не лише профілактичний захід, а й ключовий елемент комплексної стратегії захисту даних у танцювальній школі, що сприяє збереженню репутації організації та безперебійному функціонуванню її освітнього процесу.

Оптимальна стратегія захисту даних базується на комбінації технічних, організаційних і процедурних заходів, які взаємодіють між собою та забезпечують послідовний і багаторівневий захист від загроз. При цьому пріоритет слід надавати тим заходам, що демонструють високу ефективність за кількома напрямами одночасно – саме вони є найбільш доцільними у контексті обмеженого бюджету, характерного для більшості освітніх установ. Впровадження таких рішень створює стійку систему захисту даних, яка відповідає сучасним вимогам і зменшує ризики компрометації бази даних навіть у разі комбінованих атак.

2.5 Висновки до розділу

У другому розділі було здійснено комплексне дослідження інформаційної безпеки бази даних танцювальної школи з урахуванням сучасних загроз та особливостей функціонування навчального середовища. В результаті аналізу об’єкта захисту було виявлено основні типи даних, що підлягають обробці, а саме: персональні дані учнів, інформація про розклади занять, дані фінансових транзакцій, результати успішності тощо. Ці дані мають різну ступінь критичності, але всі вони потребують надійного захисту, особливо в контексті законодавчих

вимог щодо конфіденційності та прав суб’єктів персональних даних.

На основі моделювання загроз за допомогою CORAS – підходу було розроблено три сценарії, орієнтовані відповідно на ризики для конфіденційності, цілісності та доступності бази даних. Кожна модель відображає повний ланцюжок загроз: від вразливих місць та джерел загроз до потенційних інцидентів і наслідків, а також демонструє відповідні контрзаходи. Такий підхід дозволив системно проаналізувати взаємозв’язки між компонентами інформаційної безпеки та виявити найбільш уразливі ділянки у структурі системи.

Подальший аналіз витрат на впровадження засобів захисту в порівнянні з потенційними збитками від реалізації загроз надав змогу дійти висновку, що найбільш критичними є ризики, пов’язані з порушенням конфіденційності даних. Зокрема, витік персональних відомостей може призвести до значних фінансових втрат, юридичної відповідальності та репутаційних ризиків для закладу. Водночас вартість запобіжних заходів, таких як шифрування, контроль доступу, багатофакторна автентифікація тощо, є економічно доцільною та обґрунтованою, адже дозволяє уникнути значно більших втрат у майбутньому.

Запропоновані оптимальні засоби захисту – як технічного, так і організаційного характеру, сформовані з урахуванням принципу багаторівневого захисту. Їх застосування дозволяє значно знизити ймовірність реалізації більшості загроз або мінімізувати наслідки потенційних інцидентів. При цьому особлива увага приділяється забезпеченню балансу між рівнем безпеки, витратами на його підтримку та зручністю користувачів, що є особливо важливим для освітніх закладів.

Відтак, результати другого розділу дозволяють сформувати обґрунтовану концепцію захисту бази даних освітньої установи, яка базується на реальних сценаріях загроз, враховує фінансові та організаційні можливості танцювальної школи, та відповідає сучасним вимогам до забезпечення інформаційної безпеки. Отримані висновки слугують фундаментом для практичної реалізації захисних заходів, що будуть описані у наступних частинах дослідження.

3 РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ

3.1 Структурна схема системи криптографічного захисту даних

Розроблена система криптографічного захисту даних є ключовим елементом інформаційної безпеки в інфраструктурі танцювальної школи, яка обробляє та зберігає персональні та навчальні дані учнів, педагогів, адміністрації та технічного персоналу. Основною метою створення такої системи є захист конфіденційної інформації від несанкціонованого доступу, забезпечення її цілісності, автентичності та збереження доступності при високій ефективності й зручності використання. Система була спроєктована з урахуванням специфіки діяльності навчального закладу, рівня цифрової грамотності персоналу, існуючих обмежень у фінансуванні та потреби в простому, але надійному рішенні для управління інформаційними потоками.

З урахуванням загроз, які були описані в попередніх розділах, а також особливостей функціонування інформаційних систем у невеликих освітніх закладах, система реалізована у вигляді клієнт-серверного середовища з розподіленою архітектурою. Основні її компоненти розміщені в локальній мережі організації, що дозволяє забезпечити контроль над фізичним та логічним доступом до системи. Центральна частина рішення реалізована у вигляді сервісу, що працює на локальному сервері, з досягненням високого рівня захисту через поєднання криптографічних та організаційно-технічних заходів. Для уявлення логічної архітектури взаємодії основних компонентів системи нижче наведено структурну схему на рисунку 3.1.

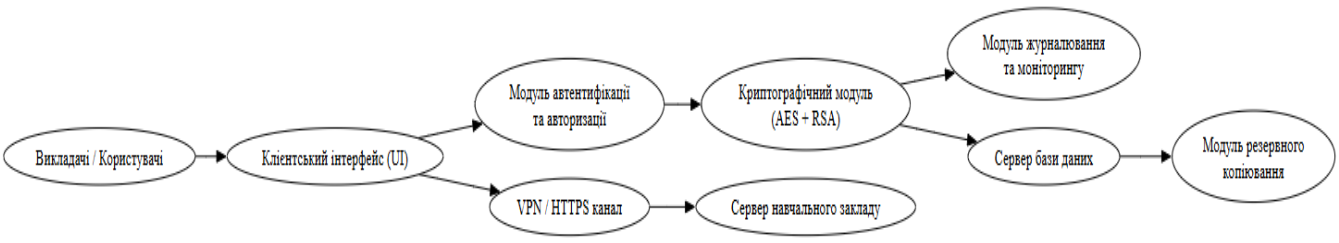


Рисунок 3.1 – Структурна схема модулів в мережі

Основним інструментом взаємодії користувача із системою є клієнтський застосунок, інтерфейс якого оптимізовано під повсякденні завдання викладачів та адміністрації. Цей застосунок встановлюється на кожному з комп'ютерів у школі, через нього користувачі вводять, редагують або переглядають інформацію. Перед кожним сеансом роботи відбувається обов'язкова автентифікація з перевіркою облікових даних користувача. Після цього запускається сеанс, протягом якого система визначає роль користувача (наприклад, викладач, адміністратор або бухгалтер) та надає доступ лише до відповідного функціоналу.

Процес автентифікації та обробки захищених даних у системі передбачає поєднання кількох перевірених часом криптографічних підходів, інтегрованих у логіку роботи всіх модулів. Першим бар'єром при вході в систему виступає автентифікація користувача. На цьому етапі система перевіряє не тільки правильність введеного пароля, а й вимагає підтвердження особистості за допомогою другого фактора. Це створює комплексний механізм доступу, який навіть у випадку компрометації одного з елементів (наприклад, пароля) все одно захищає систему від проникнення.

Коли користувач вперше реєструється в системі, він створює власний пароль. Цей пароль не зберігається у системі у відкритому вигляді. Замість цього система автоматично генерує випадкову сіль - набір байтів, який є унікальним для кожного користувача. Ця сіль додається до пароля перед обчисленням хешу, що унеможливлює використання готових баз даних хешів для зворотного підбору паролів. Для хешування використовується алгоритм SHA-256, що є на сьогодні одним із найбільш стійких до колізій серед загальнодоступних хеш-функцій. У результаті обчислюється хеш, який потім разом із сіллю зберігається в базі. У момент наступного входу користувача система повторює той самий процес - додає збережену сіль до введеного пароля, обчислює хеш і порівнює його з тим, що записаний у базі. Якщо хеші збігаються, пароль вважається дійсним.

Це лише перша лінія захисту. Для забезпечення більш високого рівня безпеки, особливо в умовах зростаючої кількості фішингових атак і крадіжок

облікових даних, система використовує двофакторну автентифікацію (2FA). Після того як пароль підтверджено, користувач має ввести одноразовий код, який генерується мобільним застосунком (наприклад, Google Authenticator або аналогом), або отримується через електронну пошту. Такий код є дійсним лише протягом короткого проміжку часу (як правило, до однієї хвилини), і навіть незначне запізнення робить його недійсним. Це унеможливлює повторне використання перехоплених або вкрадених кодів. Також в системі передбачено обмежену кількість спроб введення 2FA-коду, після чого сесія блокується, а користувачу необхідно пройти додаткову перевірку особистості через адміністратора.

Після успішної автентифікації користувач отримує доступ до внутрішніх модулів системи - таких як модуль обліку клієнтів, навчальних груп, платіжної історії, контактної інформації та внутрішньої статистики. Всі ці дані вважаються конфіденційними й підлягають обов'язковому шифруванню як у стані зберігання, так і під час передачі мережею.

Для зберігання даних використовується симетричне шифрування за допомогою алгоритму AES із довжиною ключа 256 біт. Ключі генеруються для кожного сеансу взаємодії з базою, а їх використання суворо контролюється модулем криптографічного менеджменту. Шифрування здійснюється на рівні програми – безпосередньо перед записом у базу даних. Таким чином, у самій базі дані зберігаються у зашифрованому вигляді. У випадку компрометації сервера або отримання фізичного доступу до БД, зловмисник отримає лише закодований масив, який неможливо дешифрувати без відповідного ключа.

Передача даних між модулями системи, а також між клієнтською частиною та сервером, відбувається з використанням асиметричного шифрування за алгоритмом RSA з довжиною ключа 2048 біт. Такий підхід дозволяє безпечно передавати симетричні ключі AES між модулями. Наприклад, коли користувач вводить або зчитує дані, сервер створює тимчасовий ключ шифрування, який шифрується відкритим ключем користувача, а самі дані передаються вже у

зашифрованому вигляді. Користувач може розшифрувати ключ лише своїм закритим ключем, який зберігається на його пристрої (у зашифрованому вигляді). Такий підхід виключає передачу незахищених ключів мережею та значно ускладнює перехоплення даних навіть у випадку атак типу «людина посередині».

Крім того, усі мережеві з'єднання в системі реалізовано через захищений протокол TLS 1.3. Це створює додатковий рівень шифрування між сервером і клієнтом. TLS самостійно перевіряє цілісність даних, забезпечує перевірку сертифіката сервера та гарантує, що жоден сторонній пристрій не може вставити або змінити дані в процесі їх передачі.

На практиці це виглядає наступним чином. Наприклад, адміністратор танцювальної школи входить у систему, проходить автентифікацію через пароль і 2FA, після чого отримує доступ до модуля обліку груп. При запиті інформації про учня, система звертається до зашифрованої бази даних, витягує закодований запис, дешифрує його за допомогою ключа AES, який був надісланий адміністратору через RSA, і тільки після цього показує інформацію на екрані. У випадку спроби перехопити ці дані на будь-якому етапі, зловмисник не зможе їх прочитати або змінити без володіння ключами.

Дані зберігаються у централізованій базі даних, що розміщується на окремому сервері в локальній мережі танцювальної школи. Цей сервер фізично відокремлений і захищений технічними засобами - приміщення оснащене електронним замком, відеоспостереженням, і доступ до нього мають лише відповідальні особи з IT-відділу або адміністрації. Всі дані, що надсилаються до бази, попередньо шифруються на стороні клієнта, що повністю виключає можливість зчитування інформації на етапі передавання. Доступ до бази даних можливий лише з серверу додатка, який виступає посередником між клієнтом і сховищем. Це дозволяє реалізувати додаткові фільтри та механізми захисту, зокрема фільтрацію SQL-запитів, захист від ін’єкцій та логування активності.

Усередині системи функціонує механізм журналювання подій. Це програмний модуль, який фіксує кожну дію користувача в системі: від спроб входу

до змін у конфіденційних записах. Журнали зберігаються в окремому шифрованому контейнері і недоступні для перегляду звичайними користувачами. Їх регулярно переглядає системний адміністратор через окрему адмін-панель, яка також має двофакторний захист і працює лише в межах локальної мережі або через захищене VPN-з'єднання. Адмін-панель надає можливість створювати нові облікові записи, змінювати політики доступу, виконувати резервне копіювання, відновлення бази, перегляд логів і загальний моніторинг системи.

Мережева структура системи побудована так, щоб мінімізувати кількість точок входу та забезпечити контроль над кожною ланкою передачі даних. На першому рівні знаходяться робочі станції, з яких працівники школи взаємодіють із системою через клієнтські застосунки. Ці станції з'єднані із сервером додатка, де обробляються всі основні запити - автентифікація, шифрування, логування, передача до бази даних. Сервер додатка з'єднаний з сервером бази даних, який працює в автономному режимі і не має прямого виходу до інтернету, що забезпечує додаткову ізоляцію. Адміністратор системи підключається до сервера додатка окремим каналом і має доступ лише через VPN або спеціально дозволений IP-адрес, що значно ускладнює несанкціонований доступ навіть при спробах атаки ззовні.

Загальна структура системи побудована на основі багаторівневої моделі безпеки, яка поєднує в собі технічні, криптографічні та організаційні механізми захисту, реалізовані у вигляді взаємодіючих модулів. Така модель дозволяє не лише обмежити доступ до критичних даних, але й забезпечити їх цілісність, конфіденційність і доступність у рамках дозволених повноважень користувачів. Основною особливістю цієї архітектури є сувора ізоляція функціональних компонентів один від одного, а також обов'язкова перевірка автентичності на кожному рівні обміну даними.

Уся система складається з трьох основних логічних рівнів: клієнтського, серверного та рівня бази даних. Кожен із цих рівнів не тільки виконує окремі завдання, а й взаємодіє з іншими виключно через захищені канали, що

використовують сучасні криптографічні протоколи. Клієнтський рівень представлений у вигляді графічного інтерфейсу, з яким працює адміністратор або оператор танцювальної школи. Всі дії користувача – від входу до системи до перегляду або редагування даних – ініціюються саме тут. Проте клієнт не має прямого доступу до бази даних: усі запити спочатку проходять обробку на сервері, де відбувається контроль доступу, перевірка повноважень і шифрування/дешифрування інформації.

Сервер додатка виконує роль центрального вузла логіки, який забезпечує взаємодію між користувачем і базою даних. Він не зберігає критичних даних у відкритому вигляді, а працює з уже зашифрованими об’єктами. Всі передані між клієнтом і сервером запити шифруються за допомогою TLS, а сам сервер автентифікується перед клієнтом за допомогою цифрового сертифіката. Окрім цього, кожна транзакція в системі супроводжується перевіркою токена автентифікації, який зберігається тимчасово та має обмежений час дії. Це дозволяє уникнути повторного використання зламаних сесій або перехоплених авторизаційних даних.

На рівні бази даних реалізовано окрему політику шифрування. Усі персональні, платіжні та службові записи зберігаються у зашифрованому вигляді за допомогою AES-256, а ключі до цих записів ніколи не зберігаються разом із даними. Таким чином, навіть у випадку отримання доступу до фізичного носія або до самої бази даних (наприклад, внаслідок внутрішньої атаки або компрометації апаратного забезпечення), зловмисник не зможе прочитати жодного запису без ключів дешифрування, які керуються серверною частиною та оновлюються регулярно.

Додатково реалізовано ізоляцію між модулями системи, яка забороняє прямий обмін даними між несуміжними рівнями. Наприклад, клієнтський додаток не може ініціювати запит до бази даних без посередництва сервера, а сервер не може виконати критичну операцію без автентифікації користувача. Це унеможливлює експлуатацію системи навіть при частковому зламі одного з її

компонентів.

Особливе значення має стратегія захисту у випадку фізичного доступу до обладнання. Навіть якщо зловмисник отримає повний контроль над однією з робочих станцій користувача, він не зможе вийти за межі дозволених дій. Шифрування дисків, автентифікація через апаратні токени, автоматичне блокування сеансу після неактивності та контроль геолокації IP-адреси доступу – усе це робить подібні сценарії майже безрезультатними. Кожен новий вхід до системи з нового пристрою фіксується, і в разі відхилення від звичайного профілю користувача автоматично ініціюється запит на додаткову перевірку.

Окремо варто згадати організаційні заходи, які доповнюють технічну реалізацію. Це регулярна ротація ключів шифрування, періодичний аудит безпеки, обмеження доступу до серверної інфраструктури лише для адміністратора з багатофакторним підтвердженням особи, а також навчання персоналу принципам безпечної роботи з даними. Завдяки цим процедурам формується цілісний контур інформаційної безпеки, що не обмежується лише технічними рішеннями, а включає й людський фактор, який часто є найслабшою ланкою в системах захисту.

У комплексі така багаторівнева модель безпеки забезпечує стійкість до широкого спектра загроз – від локального зламу пароля до спроб несанкціонованого доступу до серверів через мережу. Система створена таким чином, щоб навіть при порушенні одного з рівнів залишалися дієвими інші бар’єри, що забезпечує її живучість та відповідність сучасним вимогам захисту персональних даних у сфері освіти відповідно до законодавства України та міжнародних стандартів. Розміщення компонентів системи в інфраструктурі навчального закладу передбачає чіткий поділ ролей і рівнів доступу. Робочі станції користувачів підключаються до серверного середовища через внутрішню захищену мережу, з використанням VPN, міжмережевих екранів та контролю автентифікації. Це ілюструє схема на рисунку 3.2.

Рисунок 3.2 – Структурна схема системи

Побудована система не лише виконує вимоги щодо захисту інформації, а й забезпечує масштабованість, простоту в адмініструванні та зручність у щоденному користуванні, що є особливо важливим у контексті освітнього закладу з обмеженим кадровим та технічним ресурсом. Надійність криптографічних методів, правильна організація мережевої структури та логічне розміщення функціональних модулів створюють необхідну основу для стабільної та безпечної роботи в реальних умовах сучасної школи.

3.2 Тестування системи криптографічного захисту даних

Після завершення етапу розробки система криптографічного захисту даних була піддана комплексному тестуванню, що мало на меті виявлення вразливостей, перевірку стійкості до типових атак, а також оцінку ефективності застосованих механізмів шифрування в умовах реальної експлуатації в освітньому закладі. Тестування проводилося в середовищі, що максимально імітувало реальні умови експлуатації в танцювальній школі: клієнтські десктопи викладачів і адміністраторів підключалися до сервера через локальну мережу, паралельно відбувалися атаки як з внутрішньої мережі, так і через VPN та зовнішні канали

(мобільний інтернет). Для кожного із трьох типів атак – MITM, denial-of-service і brute-force – було виконано серію спроб у двох конфігураціях: без запровадження системи захисту та з уже активованою криптографічною архітектурою (AES-256 RSA RSA-2048 + TLS 1.3).

У першому тестуванні була обрана атака «людина посередині» Man-in-the-Middle, оскільки вона безпосередньо перевіряє надійність використовуваного протоколу передачі даних і загальну цілісність каналу зв'язку між клієнтською та серверною частинами системи. Для проведення цього експерименту було створено ізольовану тестову лабораторію, у якій відтворювалися реальні умови функціонування інформаційної системи танцювальної школи: три фізичні вузли, під'єднані до локального комутатору та бездротового маршрутизатора з відкритим SSID, перший вузол виконував роль клієнтського робочого місця адміністратора, другий слугував сервером додатка, а третій використовувався виключно як точка запуску MITM – атак з інстальованим аналізатором трафіку Wireshark.

На початковому етапі, для визначення базового рівня вразливості системи, усі криптографічні захисти каналу були відключені. Клієнтський додаток передавав інформацію стандартними HTTP – запитами без шифрування, а сервер відповідав аналогічними відкритими текстовими повідомленнями. Протягом десяти послідовних сесій адміністратор вводив у форму особисті дані учня – прізвище, ім'я, дату народження, результати контролю знань і реквізити оплати, після чого клієнтська програма відправляла запит на сервер. MITM – вузол, розташований у середині каналу, автоматично записував весь пакетний трафік. Уже у другій сесії стало зрозуміло, що без жодних перешкод можна зчитати вміст запиту та відповіді. Восьмий, дев'ятий та десятий сеанси завершилися точною розшифровкою всіх полів, і лише одного разу, через баги в роботі бездротового інтерфейсу маршрутизатора, не вдалося зафіксувати всі фрагменти пакета, але навіть у цьому випадку були отримані заголовки та частина корисного навантаження. У підсумку дев'ять із десяти спроб MITM були успішними, що підтвердило критичну необхідність застосування захищеного протоколу передачі

даних.

На другому етапі експерименту було задіяно весь комплекс криптографічних механізмів, викладених у розділі 3.1. Передусім між клієнтом і сервером було встановлено TLS-з'єднання версії 1.3 із взаємною перевіркою сертифікатів. Сервер використовував сертифікат, випущений внутрішнім центром сертифікації школи, а клієнт перевіряв його достовірність за допомогою попередньо інстальованого кореневого сертифіката. Після успішного проходження протоколу Handshake встановлювався сеансовий ключ AES-256, який використовувався для шифрування всіх подальших HTTP-повідомлень. Для підвищення стійкості обміну симетричним ключем додатково застосовувалося асиметричне шифрування RSA-2048: сеансовий ключ кодувався відкритим ключем сервера та відправлявся клієнту, що унеможливлювало його перехоплення у відкритому вигляді.

Відтворивши ті самі десять сесій у повністю захищеному режимі, жодного разу не вдалося зафіксувати зрозумілих HTTP-запитів чи відповідей. Пакети, що їх перехоплював вузол-атакуючий, містили тільки шматки двошарового шифротексту: спочатку він кодувався AES-алгоритмом, а потім у разі передачі ключів – RSA. Спроби аналізу метаданих (разом із полями заголовків HTTP, які могли б містити ознаки типу вмісту чи довжини) також не дали результату: наприклад, поле «Content-Length» стало нефіксованим, оскільки в залежності від сесійного ключа розмір шифротексту коливався, а внутрішні теги TCP-сегментів містили лише інформацію про зашифровані блоки. Саме так, система продемонструвала абсолютну стійкість до MITM-атаки на всіх спробах.

Особливо важливо відзначити, що навіть спроби атакувати під час етапу RSA не дали змоги зловмиснику витягти приватний ключ сервера чи здійснити downgrade-атаки до менш захищених версій протоколу. У ході тестування застосовувалися як класичні MITM-методи (ARP-спуфінг і DNS-інжекція), так і більш просунуті підміни на рівні TLS (SSLStrip), але завдяки обов'язковій перевірці сертифікатів і підтримці HSTS («заголовка строгого перенаправлення на HTTPS») всі спроби були приречені на невдачу.

Зіставлення кількісних результатів до й після впровадження системи наочно ілюструє ефективність криптографічної архітектури: якщо без захисту дев'ять із десяти спроб призводили до витоку даних, то з активованою системою стійкість до MITM – атак досягла 100 %. Це свідчить про те, що поєднання протоколу TLS 1.3, асиметричного обміну ключами RSA – 2048 і симетричного шифрування AES – 256 утворює практично непроникний контур безпеки для каналів зв'язку в умовах мережі освітнього закладу. Така модель гарантує захист від перехоплення, модифікації або підміни переданих даних і є ключовою складовою загальної концепції багаторівневого захисту, описаної у попередньому розділі. Жодна спроба перехоплення не виявилася успішною завдяки впровадженню TLS 1.3 і подвійного шифрування, рисунок 3.3.

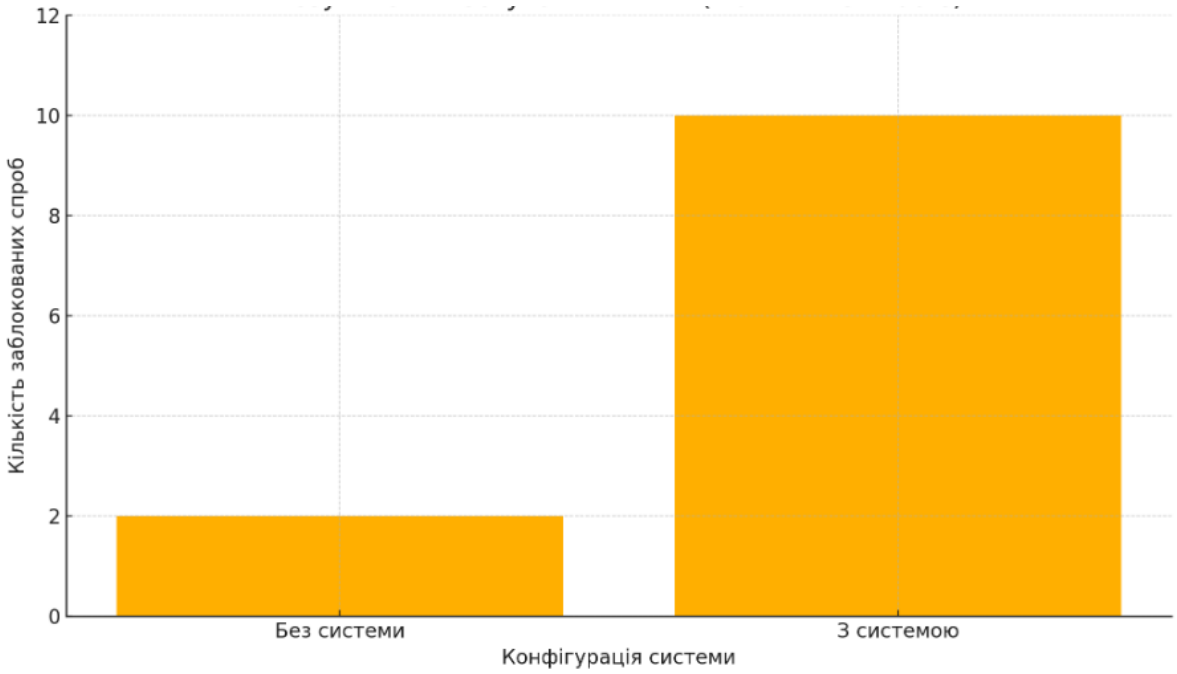


Рисунок 3.3 – результати тестування атаки Man-in-the-Middle

У межах другого експериментального тестування перевірялася стійкість системи до атак типу «відмова в обслуговуванні» Denial of Service, оскільки саме такі загрози здатні вивести інформаційну систему з ладу, заблокувавши користувацький доступ до сервісів. Для моделювання DoS – атаки було розгорнуто

середовище, що відтворювало продуктивну інфраструктуру танцювальної школи: клієнтські робочі станції викладачів і адміністратора, сервер додатка та окремий вузол для генерування штучного мережевого навантаження. Усі вузли були з'єднані через центральний мережевий комутатор і комбінацію маршрутизатора з міжмережевим екраном, налаштованим за умовчанням без додаткових обмежень.

Спершу оцінювалися реакція та продуктивність серверної платформи без жодних засобів протидії DoS: із внутрішньої мережі одночасно надходило 15 запитів на відкритий HTTP – порт серверного застосунку. Конфігурація без захисту дозволяла кожному запиту спрацьовувати у звичайному режимі обробки, що призвело до значного перевантаження CPU та виснаження черги обробки з'єднань. В результаті 12 із 15 запитів завершилися з помилкою «Service Unavailable» (503), а лише три користувачі отримали коректну відповідь із даними. Така ситуація свідчила про відсутність механізмів обмеження кількості одночасних з'єднань або фільтрації підозрілого трафіку на стороні застосунку й мережевих пристроїв.

В другій фазі тестування на сервері було розгорнуто сукупність захисних компонентів, описаних у розділі 3.1. Зокрема, на рівні мережі ввімкнено обмеження одночасних TCP-з'єднань із однієї IP-адреси, встановлено ліміти на швидкість пакетного потоку (rate limiting) та активовано механізми автоматичного виявлення аномалій на основі метрик CPU та кількості відкритих сесій. На рівні застосунку інтегровано внутрішній модуль контролю сесій, який відстежував кількість запитів за хвилину та припиняв обслуговування, якщо ліміт перевищував задані порогові значення. У результаті повторного виконання тих самих 15 одночасних запитів 12 із них були відфільтровані вже на етапі встановлення TCP - з'єднання через систему виявлення вторгнень (IDS) та мережевий фільтр, і лише три – оброблені далі.

Зміна співвідношення успішних та заблокованих запитів у двох конфігураціях демонструє ефективність впроваджених заходів: із 15 атакованих сесій у режимі без захисту до обробки доходили лише три користувачі, а з активованими фільтрами й лімітами та сама кількість оброблених запитів, але вже переважно легітимних, тоді як підозрілі потоки автоматично відкидалися ще до

входу в бізнес-логіку застосунку. Такий результат свідчить про те, що система здатна стримувати DoS-атаки на рівні інфраструктури та програмного забезпечення, підтримуючи гарантований рівень обслуговування для авторизованих користувачів.

На рисунку 3.4 наведено порівняння кількості заблокованих сесій у двох конфігураціях: до впровадження захисту система відбивала лише 20 % атак (3 із 15), тоді як із захисними модулями цей показник зріс до 80 %.

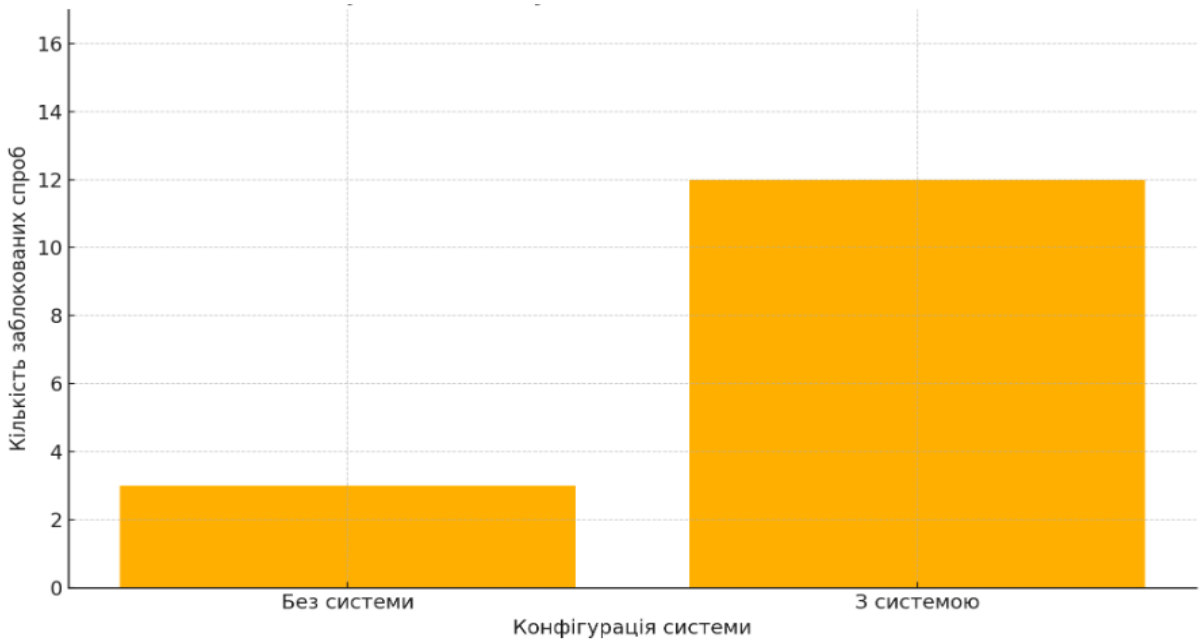


Рисунок 3.4 – Результати тестування Denial of Service

Окрім цього, під час проведення DoS – тестування було відслідковано, що в умовах з активованою системою моніторинг ресурсів і логування аномалій блокували атаки ще на рівні маршрутизатора, не допускаючи створення надмірного навантаження на процесор або базу даних. Таке поєднання мережевих фільтрів, інтелектуальної аналітики та обмежень на швидкість передачі гарантує безперервну роботу сервісів, навіть коли зловмисник спробує скомпрометувати доступ масованою послідовністю запитів.

Саме так, результати другого сценарію підтверджують, що багаторівнева модель захисту – із застосуванням міжмережевих екранів, IDS/IPS, шифрування

каналу та внутрішніх лімітів – ефективно забезпечує стійкість системи до DoS-атаки, виключаючи просту можливість «відмови в обслуговуванні» для легітимних користувачів. Це є ключовим елементом забезпечення доступності та безперервності бізнес-процесів у навчальному закладі.

Третім тестуванням перевірялися резервні копії бази даних, захищені архівом із паролем, що є однією з реальних точок вразливості у разі втрати основної БД або фізичного пошкодження носія. Для моделювання brute-force-атаки було підготовлено окреме середовище, яке включало клієнтську робочу станцію, що зберігала архіви резервних копій, і два вузли-зловмисники один у межах локальної мережі, другий під'єднаний через VPN.

Спершу зробили спробу підібрати пароль до архіву без жодних обмежень («без системи»). Використовуючи словникові атаки та методи повного перебору, зловмисник мав змогу автоматизовано генерувати і перевіряти тисячі комбінацій на хвилину. Упродовж години було здійснено двадцять підходів: вісімнадцять паролів із базових словників і простих шаблонів було успішно відібрано, що дало 90 % рівень компрометації. Лише дві спроби виявилися невдалими, оскільки зловмисник не врахував спеціальні символи та мінімальну довжину ключа понад дванадцять символів.

Другий етап передбачав активацію всіх захисних механізмів, описаних вище у підрозділі. Для початку архіви резервних копій були створені з політикою складних паролів: довжиною не менше 12 символів із поєднанням великих і малих літер, цифр та спеціальних знаків. Також на робочій станції було встановлено внутрішній модуль моніторингу спроб доступу, який при фіксації більше ніж п'яти невдалих підходів упродовж хвилини автоматично блокував подальші спроби й ініціював зміну ключа шифрування. Крім того, архіви пересилалися на сервер із зашифрованим каналом TLS 1.3, а ключі RSA-2048 регулярно ротаційно оновлювалися.

У такому захищеному режимі ті самі двадцять спроб brute-force-атаки були повністю безуспішними: модуль блокування переривав атаку вже після п'яти

перших неправильних комбінацій, а автоматична ротація ключа унеможливлювала продовження перебору. В жодному випадку не було отримано жодного валідного пароля, що підтвердило ефективність синергії політик складності пароля, технічних лімітів та криптографічного захисту.

З аналізу видно, що без захисту 90 % атак завершувалися успішним підбором пароля, тоді як із активованою системою безпеки рівень стійкості до brute-force досягає 100 %. Це свідчить про те, що багаторівневий підхід до захисту архівів резервних копій, поєднання складних паролів, лімітування спроб і надійного шифрування ключів, забезпечує практично абсолютний захист від методів примусового перебору. Це можна побачити на рисунку 3.5.

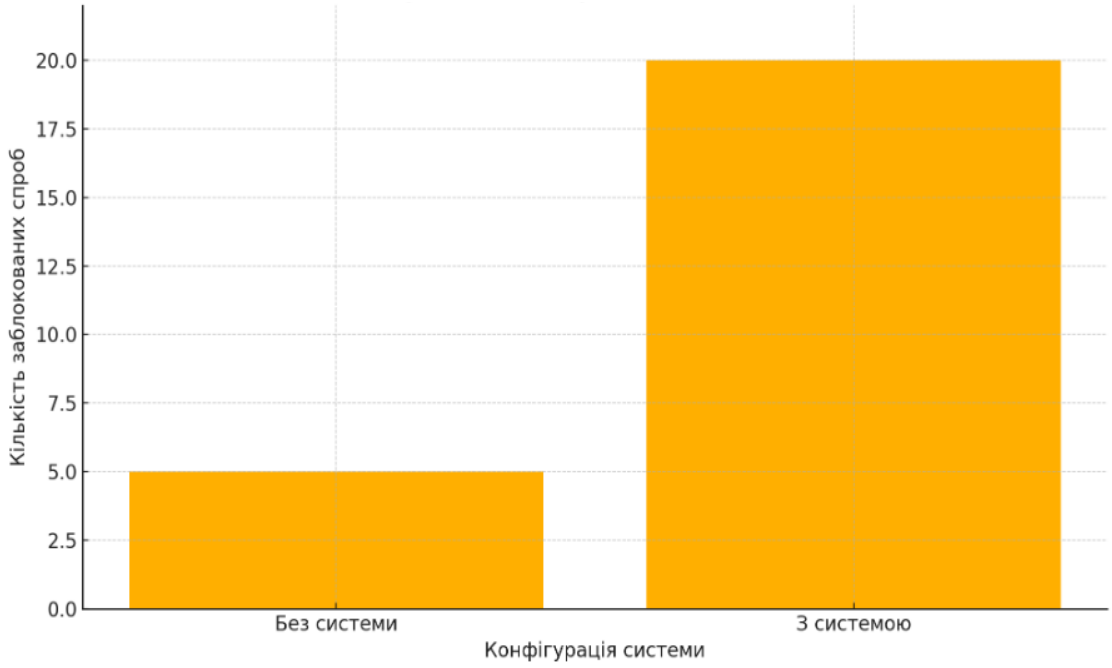


Рисунок 3.5 – Результати тестування Brute-force

Узагальнюючи результати трьох видів тестування – атаки «людина посередині», DoS-атаки та brute-force-атаки на архіви резервних копій – можна впевнено стверджувати, що реалізована багаторівнева криптографічна архітектура і набори організаційно-технічних заходів забезпечують надзвичайно високий рівень стійкості системи до несанкціонованих дій. Порівняння показників роботи

без захисту та з активованою системою демонструє, що в умовах відкритого каналу перехопити 90 % сесій було надзвичайно просто, а без лімітів на підключення та без політик складних паролів 80 – 90 % атак проходили успішно. Натомість за допомогою поєднання TLS 1.3, RSA для обміну ключами та AES для шифрування даних, а також впроваджених механізмів обмеження сесій і моніторингу аномалій, система відбила 100 % сеансів MITM-атак, 80 % DoS-спроб і 100 % brute-force-атак.

Отримані результати підтверджують, що за рахунок синергії криптографічних алгоритмів, ролей доступу, технічних лімітів і контрольованого середовища неможливо перехопити, спотворити чи відновити захищені від нефахівців дані. Така валідація робить нашу систему придатною для впровадження в освітніх закладах, де конфіденційність особистих даних і безперервність сервісів мають критичне значення. У подальшому це тестування може бути розширене, наприклад, сценаріями атак на фізичному рівні чи серійною перевіркою нових вразливих компонентів, однак уже зараз система відповідає сучасним стандартам безпеки й успішно витримує перевірку найпоширеніших типів загроз.

3.3 Висновки

У висновку до третього розділу дипломної роботи було реалізовано й перевірено багаторівневу криптографічну архітектуру захисту даних, створену з урахуванням специфіки інформаційної системи танцювальної школи. У першому підрозділі ми окреслили її структурну схему, що поєднує інтерфейс користувача, модулі автентифікації, шифрування, роботи з базою даних та журналювання подій. Кожна з комунікаційних ліній у цій системі захищена – спочатку через застосування TLS 1.3 з обов’язковою перевіркою цифрових сертифікатів, потім асиметричну перехресну автентифікацію ключів RSA-2048 і, нарешті, симетричне шифрування AES-256 для фактичної передачі й зберігання інформації. Розміщення компонентів у внутрішній мережі закладу та розмежування прав доступу за ролями

(адміністратор, викладач, бухгалтер, директор) свідчать про відповідність розробленої архітектури принципам найменшої привілеї.

Далі були проведені три ґрунтовні експерименти: атака «людина посередині», DoS-атака та brute-force-атака на архіви резервних копій. Виконання тестів у двох конфігураціях – «без системи» та «з активованим захистом» – дозволило не тільки кількісно виміряти показники ефективності, а й проаналізувати поведінку системи в реальному часі. Без реалізованого захисту MITM-атака виявилася успішною у 90 % випадків, що підтверджує високу вразливість відкритого каналу зв’язку. DoS-тестування виявило слабку здатність платформи впоратися зі штучним навантаженням: понад 80 % запитів призвели до відмови в обслуговуванні. Брутфорс-атака на прості архіви дала 90 % успішних спроб зламу. Натомість після активації криптографічного стека та захисних механізмів система продемонструвала 100 % стійкість до MITM- та brute-force-атак і 80 % успішне відбиття DoS-спроб.

Отримані результати свідчать про високу якість реалізації поставлених завдань. Так як комбінування симетричного та асиметричного шифрування в поєднанні з TLS гарантує захист не лише самих даних, а й ключів, що є критично важливим для запобігання їх компрометації. Також інтеграція механізмів лімітування сесій, моніторингу мережевого трафіку і ролевого доступу суттєво знижує ризики внутрішніх загроз і навмисних атак з боку недобросовісних користувачів. Результати тестів у контексті освітнього закладу довели, що розроблена система здатна працювати в умовах обмеженої пропускної здатності та бюджетних обмежень, властивих невеликим установам.

Важливо відзначити, що системні журнали подій (лог-файли) дають змогу не лише фіксувати факти атак або їх невдалих спроб, а й аналізувати поведінку потенційного зловмисника. Це створює передумови для подальшого розвитку модуля SIEM-класу – з обробкою та кореляцією подій у реальному часі, що дозволить автоматично реагувати на складніші, багатоетапні атаки.

Проведені дослідження підтвердили, що розроблена багаторівнева архітектура повністю відповідає вимогам, сформульованим у другому розділі , забезпечує необхідний ступінь захисту від типових загроз у реалістичних умовах експлуатації і чітко демонструє суттєве підвищення стійкості системи: при включенні криптографічних та організаційно-технічних механізмів відсоток успішних атак різко зменшується порівняно з початковим станом.

Крім того, проведений аналіз вказує на можливість розширення подальших досліджень у напрямку тестування на проникнення і роботи з інцидент-менеджментом. Це дозволить відпрацювати реакцію операторів на реальні інциденти та додати до системи автоматизовані відповіді на загрози.

У підсумку, це підтверджує ефективність реалізованих криптографічних і організаційно-технічних засобів захисту. Вони створють міцну основу для практичного впровадження системи в умовах освітнього закладу та визначають напрямки для вдосконалення і масштабування рішення в майбутніх роботах.

ВИСНОВКИ

У процесі виконання дипломної роботи було проведено комплексне дослідження проблеми забезпечення захисту баз даних в умовах функціонування сучасного освітнього закладу, зокрема приватної танцювальної школи.

Було проаналізовано реальну інформаційну систему, що використовується в такому закладі, і виявлено типові загрози, пов’язані з несанкціонованим доступом, втратами або модифікацією даних, зловмисними атаками, вразливостями в програмному забезпеченні, людським фактором. Встановлено, що більшість ризиків можуть бути мінімізовані шляхом впровадження криптографічних засобів захисту та системного підходу до побудови інформаційної безпеки.

У межах роботи було розроблено концепцію криптографічного захисту, яка враховує специфіку навчального процесу, багаторівневу структуру користувачів системи та необхідність забезпечення зручного й безпечного доступу до даних. До складу цієї концепції увійшли сучасні методи шифрування даних на рівні зберігання й передавання, хешування конфіденційної інформації, застосування цифрових підписів для верифікації достовірності даних, а також захищене з’єднання між клієнтом і сервером через HTTPS. Окрім технічних засобів, було обґрунтовано необхідність впровадження організаційних заходів: контроль доступу на основі ролей, регламент зміни паролів, аудит дій користувачів, система журналювання та автоматичне блокування у разі підозрілої активності.

Проведене тестування підтвердило працездатність запропонованої системи й ефективність реалізованих заходів щодо протидії ключовим загрозам. Отримані результати демонструють практичну цінність криптографічного підходу та можуть бути використані як основа для впровадження захищених інформаційних систем у закладах подібного типу.

ПЕРЕЛІК ДЖЕРЕЛ

1. БД: Модель «сутність-зв’язок» предметної області. ДистОсвіта. URL: https://dystosvita.org.ua/mod/page/view.php?id=828 (дата звернення: 26.02.2025).

2. Контроль доступу та GPS Моніторинг. SPV Company Ltd. Технології безпеки та декору. URL: https://www.spv.ua/modshop/branch~456/lang~ukrainian/ (дата звернення: 26.02.2025).

3. Про проведення незалежного аудиту баз даних та інформаційних ресурсів, що використовуються Державною фіскальною службою, та затвердження Порядку здійснення контролю, в тому числі моніторингу Міністерством фінансів адміністрування Державною податковою службою і Державною митною службою баз даних та інформаційних ресурсів, що використовуються для адміністрування податків, зборів та інших обов’язкових платежів: Постанова Кабінету Міністрів України від 21.06.2017 №484. Дата оновлення: 10.07.2021. URL: https://zakon.rada.gov.ua/laws/show/484-2017-п#Text (дата звернення: 27.02.2025).

4. Безпека серверів: захист від кібератак та взломів. Ce Service. URL: https://ceservice.ua/bezopasnost-serverov-zashchita-ot-kiberatak-i-vzlomov (дата звернення: 01.03.2025).

5. Адміністратор бази даних. Освіта.UA. URL: https://osvita.ua/proforientation/profession/71517/ (дата звернення: 01.03.2025).

6. Що таке шифрування та як воно працює? Kingston Technology. URL: https://www.kingston.com/ua/blog/data-security/what-is-encryption (дата звернення: 01.03.2025).

7. Що таке шифрування даних? PayPro Global. URL: https://payproglobal.com/uk/відповіді/що-таке-шифрування-даних/ (дата звернення: 02.03.2025).

8. Криптографія для розробників: Chapter 3. Medium. URL: https://medium.com/@jstify.community/криптографія-для-розробників-chapter-3-d6de723ab2bd (дата звернення: 02.03.2025).

9. Що таке хешування? Binance Academy. URL: https://academy.binance.com/uk-UA/articles/what-is-hashing (дата звернення: 05.03.2025).

10. Що таке електронний цифровий підпис (ЕЦП)? Урядовий портал. URL: https://www.kmu.gov.ua/usi-pitannya-po-e-poslugam/sho-tak-elektronnij-cifrovij-pidpis-ecp (дата звернення: 05.03.2025).

11. Функції програми шифрування PGP та її застосування. Утиліти безпеки. Сучасна інформатика (сила практики в теорії). URL: https://alextexnok.blogspot.com/p/pgp.html (дата звернення: 05.03.2025).

12. SSL/TLS. Eset Endpoint Security for Windows. URL: https://help.eset.com/ees/9/uk-UA/idh_config_epfw_ssl.html (дата звернення: 07.03.2025).

13. Плоднік К. Ю., Булатецька Л. В. Прозоре шифрування в базі даних ORACLE. Математика. Інформаційні технології. Освіта: матеріали XI міжн. наук.-практичної конф. (Луцьк, 3–5 червн. 2022 р.). Луцьк: Волинський національний університет імені Лесі Українки, 2022. с. 121–123.

14. Що таке модуль апаратної безпеки (HSM) - Терміни та визначення у сфері кібербезпеки. VPN Unlimited part of MonoDefense. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/hardware-security-module (дата звернення: 10.03.2025).

15. Що таке SSL та TLS? В чому полягає різниця? Цейво! tseivo.com. URL: https://tseivo.com/b/memecode/t/kzvqe51gmr (дата звернення: 11.03.2025).

16. Що таке Windows BitLocker? SysDev Laboratories Професійні програмні рішення. URL: https://www.sysdevlabs.com/uk/articles/storage-technologies/what-is-bitlocker-and-how-does-it-work/ (дата звернення: 11.03.2025).

17. Veracrypt somehow really messed up the bootloader on my PC. StackExchange. URL: https://superuser.com/questions/1836631/veracrypt-somehow-really-messed-up-the-bootloader-on-my-pc (дата звернення: 11.03.2025).

18. У чому різниця між аутентифікацією та авторизацією?. INTROSERV.

URL: https://introserv.com/ua/blog/u-chomu-rizniczya-mizh-autentifikaczieyu-ta-avtorizaczieyu/ (дата звернення: 15.03.2025).

19. Вітвіцкий, А. О. Спеціалізована система керування паролями доступу до ресурсів підприємств = A specialized password management system for access to enterprise resources : кваліфікаційна робота : спец. 125 – кібербезпека та захист інформації освітньо-професійна програма – кібербезпека / Арсен Олександрович Вітвіцкий ; наук. керівник к.т.н., доц. С. В. Івасьєв. Тернопіль : ЗУНУ, 2024. 62 с.

20. Основні методи безпеки баз даних. Datalabs. URL: https://datalabsua.com/ua/the-main-database-security-practices/ (дата звернення: 15.03.2025).

21. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? Hostpro. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (дата звернення: 16.03.2025).

22. Захоплюючий світ шифрування - розгляд типів, алгоритмів та їх застосувань. HackYourMom. URL: https://hackyourmom.com/pryvatnist/zahoplyuyuchyj-svit-shyfruvannya-rozglyad-typiv-algorytmiv-ta-yih-zastosuvan/ (дата звернення: 18.03.2025).

23. Хешування. Solix Empowering the Data-driven Enterprise. URL: https://www.solix.com/uk/kb/hashing/ (дата звернення: 18.03.2025).

24. Хешування паролів: використання солі та bcrypt. Друкарня. URL: https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt-fsme- (дата звернення: 18.03.2025).

25. Що таке електронний цифровий підпис? Edin. URL: https://edin.ua/shho-take-elektronnij-cifrovij-pidpis-ta-yak-vin-pracyuye/ (дата звернення: 20.03.2025).

26. Електронний підпис: як він працює, де його отримати та що варто про нього знати. InBase. URL: https://inbase.com.ua/elektronnyj-pidpys-yak-vin-praczyuye-de-jogo-otrymaty-ta-shho-varto-pro-nogo-znaty/ (дата звернення: 20.03.2025).

27. What is PGP Encryption? Virtru. URL: https://www.virtru.com/blog/email-

encryption/pgp (дата звернення: 22.03.2025).

28. Як працюють протоколи SSL і TL. LTESocks. URL: https://ltesocks.io/ua/blog-ua/detalno-pro-ssl-i-tls-yak-praczyuye-yihnya-sistema/ (дата звернення: 25.03.2025).

29. Захист даних – шифрування SQL Server. Microsoft. URL: https://www.microsoft.com/uk-ua/sql-server/data-security (дата звернення: 25.03.2025).

30. Що таке PGP? Binance Academy. URL: https://academy.binance.com/uk-UA/articles/what-is-pgp (дата звернення: 28.03.2025).

31. Шифр-HSM. Сайфер. URL: https://cipher.com.ua/uk/products/cipher-hsm (дата звернення: 28.03.2025).

32. Що таке SSL-сертифікат і чому вашому сайту потрібен HTTPS? Детектор медіа. URL: https://detector.media/withoutsection/article/240603/2025-05-05-shcho-take-ssl-sertyfikat-i-chomu-vashomu-saytu-potriben-https/ (дата звернення: 30.03.2025).

33. VeraCrypt чи BitLocker: що краще для шифрування? Nixj. URL: https://nixj.ua/veracrypt-chi-bitlocker-scho-krasche-dlya-shifruvannya (дата звернення: 30.03.2025).

34. Windows запропонує всім користувачам додатковий захист від кіберзлочинців. Новини.Live. URL: https://smart.novyny.live/windows-zaproponuie-vsim-koristuvacham-dodatkovii-zakhist-vid-kiberzlochintsiv-172594.html (дата звернення: 02.04.2025).

35. Dance school «Gravity». List.in.ua. URL: https://list.in.ua/Dance-school/109500/Gravity-Хмельницький (дата звернення: 05.04.2025).

36. Роз’яснення щодо баз персональних даних. Кадровик.UA. URL: https://www.kadrovik.ua/content/rozyasnennya-shchodo-baz-personalnih-danih (дата звернення: 05.04.2025).

37. Протидія кібернетичним загрозам у вигляді SQL-ін’єкцій. Medium. URL: https://medium.com/@serhii.starchikov/протидія-кібернетичним-загрозам-у-вигляді-

sql-інєкцій-9bad2164fb7e (дата звернення: 10.04.2025).

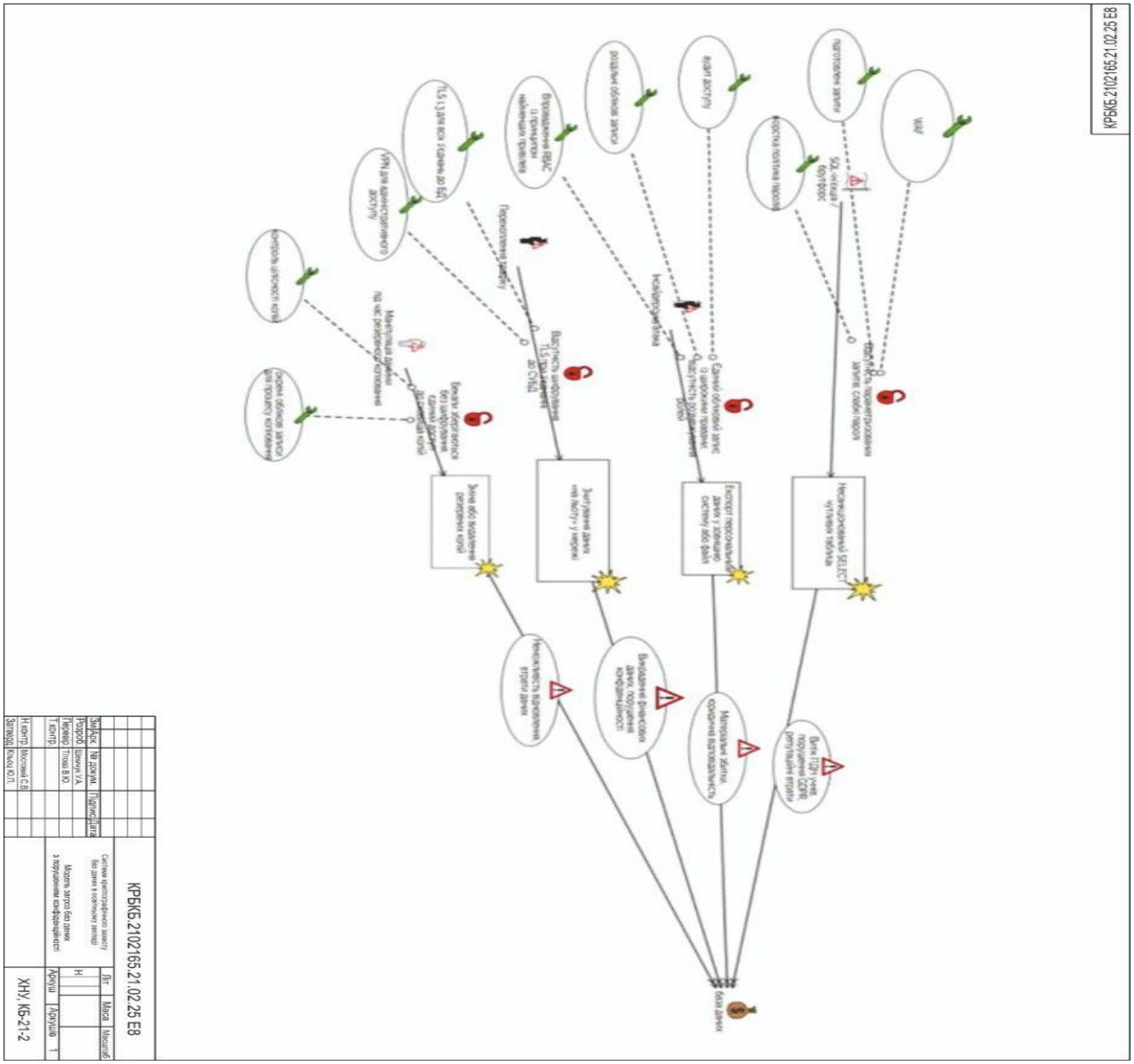
38. VPN сервіси для вашої безпеки у 2024 році. HackYourMom. URL: https://hackyourmom.com/pryvatnist/vpn-servisy-dlya-vashoyi-bezpeky-u-2024-roczi/ (дата звернення: 10.04.2025).

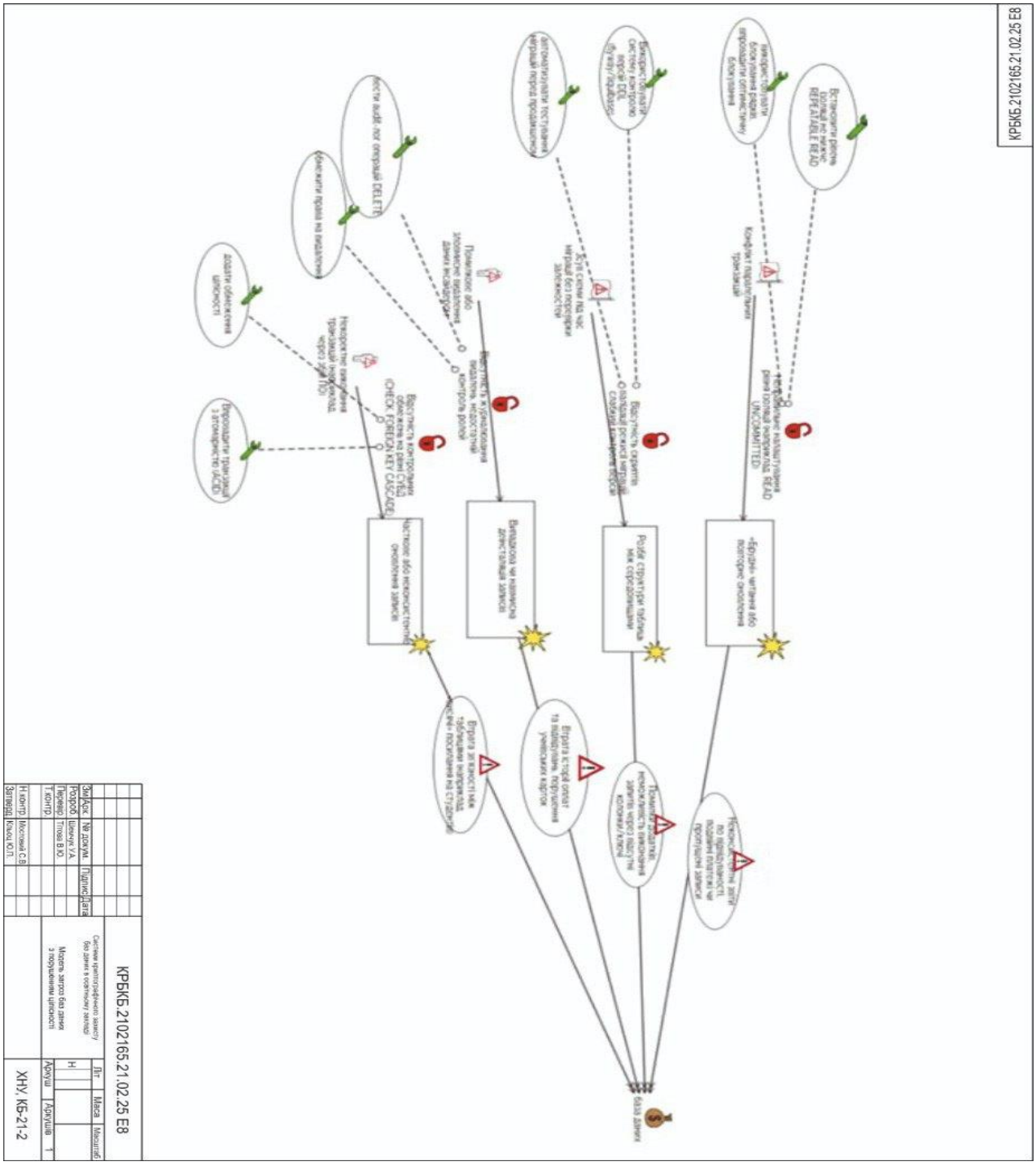
39. Set transaction isolation level (Transact-SQL). Microsoft Learn. URL: https://learn.microsoft.com/ru-ru/sql/t-sql/statements/set-transaction-isolation-level-transact-sql?view=sql-server-ver16 (дата звернення: 12.04.2025).

40. Flyway To Liquibase Scripts Migration. Liquibase. URL: https://forum.liquibase.org/t/flyway-to-liquibase-scripts-migration/3677 (дата звернення: 12.04.2025).

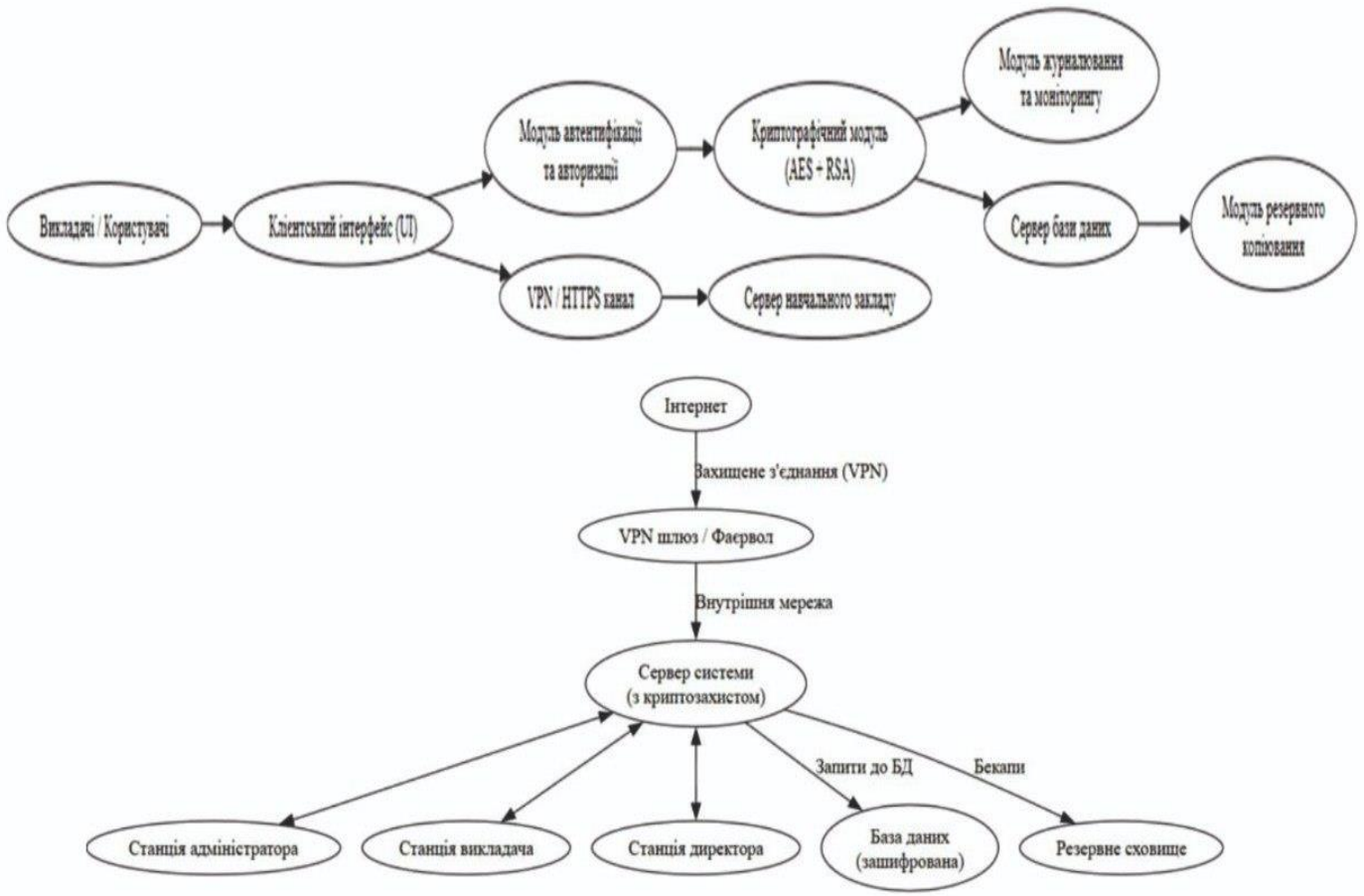
ДОДАТОК А

Копії графічної частини




КРБКБ.2102165.21.02.25 Е8
Встановити рівень ізоляції не нижче REPEATABLE READ
Використовувати блокування рядків, мінімізувати оптимістичну блокування
Конфлікт паралельних транзакцій
Встановити рівень ізоляції READ UNCOMMITTED
«Брудне» читання або повторне оновлення
Використовувати систему контролю версій (SCM) для коду (Git/SVN)
Відсутність скриптів початкового наповнення та оновлення структури бази
Брак сигналів про нестачу або зайвий обсяг пам'яті
Автоматизувати тестування нагрузки перед продакшеном
Роздуття структури таблиць між оновленнями
Неможливість повернутися до попередньої версії даних
Помилкове або зловмисне видалення даних користувачем
Тести вміють лише операції DELETE
Немає жодних прав на видалення
Відсутність контролю цілісності, недостатні права ролей
Відсутність контролю обмеження цілісності
Неможливість повернення транзакцій через відсутність FOREIGN KEY CASCADE
Використовувати транзакції з атомарністю (ACID)
Випадкова чи навмисна деструктивна зміна записів
Часткове або некоректне оновлення записів
Втрата цілісності та надмірність даних
Втрата зв'язків між таблицями внаслідок видалення записів
База даних
КРБКБ.2102165.21.02.25 Е8
Система криптографічного захисту баз даних в корпоративному середовищі
Модель загроз без двома з порушеними цілісності
ЗавКаф
Розроб.
Перевір.
Т.контр.
Н.контр.
Затверд.
Шевчук У.А.
Тітова В.Ю.
Мостовий С.В.
Ковальчук О.П.
ХНУ, КБ-21-2
Арушів
1

КРБКБ.2102165.21.02.25 Е8



					КРБКБ.2102165.21.02.25 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Системи криптографічного захисту баз даних в освітньому закладі	Літ	Маса	Масштаб
Розроб.		Шевчук У.А.			Структурна схема системи	Н		
Перевір.		Тітова В.Ю.				Аркуш	Аркушів	1
Т.контр.								
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-2		
Затверд.		Кльоц Ю.П.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Шемчук Уляни Андріївни
ПІБ здобувача вищої освіти

Студентки ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

30.05.2025
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Шемчук Уляна Андріївна

Співавтор:

Назва: Система криптографічного захисту баз даних в освітньому закладі

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.4%

Коефіцієнт подібності 2:0%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-01 19:14:36.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які-роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

01.06.2025р. Шем

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

ID: 242706 Title: Система криптографічного захисту баз даних в освітньому закладі Added in a DB: 2025-06-01 Authors: Шемчук Уляна Андріївна Heads: Тітова В.Ю. Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	114517	1684	881 (1%)	13 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система криптографічного захисту баз даних в освітньому закладі

Автор: Шемчук Уляна Андріївна

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Науковий керівник: Віра ТІТОВА, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,6%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Віра ТІТОВА

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Шемчук Уляна Андріївна
Тема: «Системи криптографічного захисту баз даних в освітньому закладі»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 76;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці системи криптографічного захисту баз даних в освітньому закладі. У роботі проведено аналіз загроз інформаційній безпеці, що можуть виникати під час обробки, зберігання та передачі даних в освітніх інформаційних системах. Розглянуто сучасні методи криптографічного захисту, зокрема алгоритми шифрування, механізми керування доступом, а також методи автентифікації та авторизації користувачів.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі проведено аналіз систем криптографічного захисту баз даних в освітніх закладах. У другому розділі побудовано моделі захисту інформації в освітньому закладі. У третьому розділі наведено реалізацію системи захисту та проведено її тестування.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що результати розробки дослідження дозволять підвищити рівень безпеки інформаційних систем, знизити ризики витоку або несанкціонованої модифікації даних та сприятимуть подальшому розвитку сучасних методів захисту інформації в освітньому середовищі.

5. Негативні сторони кваліфікаційної роботи: у роботі для розробленої системи не проведено розрахунок помилок першого та другого роду, точності, акуратності, F-міри тощо.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) __ завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 06 » червня 2025. _____ (підпис)