МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ СЕРВЕРІВ БАЗ ДАНИХ»

Виконав здобувач 4 курсу
Рівень «бакалавр»
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Панкін Нікіта Миколайович

Керівник: д.т.н., професор
Соколов Артем Вікторович

Рецензент: к.т.н., доцент
Кухаренко Сергій Вікторович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Панкіну Нікіті Миколайовичу

1. Тема роботи: «Організація захисту інформації серверів баз даних»
Керівник роботи: професор, д.т.н. Соколов Артем Вікторович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «15» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області	02.10.2024	
2	Проєктування веб-застосунку	04.12.2024	
3	Вибір програмних засобів для реалізації поставлених задач	28.01.2025	
4	Розробка клієнтської частини	14.02.2025	
5	Розробка серверної частини	15.03.2025	
6	Тестування функціональності сайту	26.04.2025	
7	Оформлення звітної частини	08.05.2025	

Здобувач _____
(підпис) (ім’я та прізвище)

Керівник роботи _____
(підпис) (ім’я та прізвище)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Організація захисту інформації серверів баз даних» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 2 рисунки, 4 таблиці та 21 літературних джерела за переліком посилань. Робота виконана на 44 сторінках загального тексту, з яких 36 сторінки основного тексту.

Метою роботи є аналіз загроз інформаційній безпеці серверів баз даних, дослідження методів і засобів їхнього захисту, а також розробка та впровадження моделі захисту інформації в конкретному серверному середовищі. У дослідженні систематизовано класифікацію серверів баз даних, проаналізовано основні кіберзагрози, такі як SQL-ін’єкції, атаки на автентифікацію, інсайдерські загрози та атаки на відмову в обслуговуванні, а також розглянуто нормативно-правові засади захисту інформації в Україні та світі, включаючи GDPR, ISO/IEC 27001 та національні закони. У практичній частині розроблено модель захисту інформації для серверів баз даних, впроваджено та протестовано її на прикладі PostgreSQL в хмарному середовищі AWS, оцінено ефективність запропонованих заходів через симуляцію атак, аналіз журналів і перевірку відповідності нормативним вимогам.

Результати роботи можуть бути використані для підвищення безпеки серверів баз даних в організаціях, оптимізації захисту чутливих даних і забезпечення відповідності нормативним вимогам.

Можливими напрямами подальших досліджень є вдосконалення автоматизованих систем моніторингу, розробка адаптивних моделей захисту для нових типів кіберзагроз, зокрема з використанням штучного інтелекту, та гармонізація національних стандартів із міжнародними.

Ключові слова: КІБЕРБЕЗПЕКА, СЕРВЕРИ БАЗ ДАНИХ, ШИФРУВАННЯ, КОНТРОЛЬ ДОСТУПУ, АУДИТ, SQL-ІН’ЄКЦІЇ, ХМАРНІ ТЕХНОЛОГІЇ, РЕЗЕРВНЕ КОПІЮВАННЯ, GDPR, ISO/IEC 27001.

ABSTRACT

The qualification thesis on the topic "Organization of Information Protection for Database Servers" for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 2 figures, 4 tables, and 21 literary sources in the list of references. The work is completed on 44 pages of total text, of which 36 pages are the main text.

The aim of the work is to analyze threats to the information security of database servers, study methods and tools for their protection, and develop and implement an information protection model in a specific server environment. The study systematizes the classification of database servers, analyzes major cyber threats such as SQL injections, authentication attacks, insider threats, and denial-of-service attacks, and reviews the regulatory and legal framework for information protection in Ukraine and globally, including GDPR, ISO/IEC 27001, and national laws. In the practical part, an information protection model for database servers was developed, implemented, and tested using the example of PostgreSQL in the AWS cloud environment, with the effectiveness of the proposed measures evaluated through attack simulations, log analysis, and compliance with regulatory requirements.

The results of the work can be used to enhance the security of database servers in organizations, optimize the protection of sensitive data, and ensure compliance with regulatory requirements. They are valuable for database administrators, cybersecurity specialists, and information system developers.

Possible directions for further research include improving automated monitoring systems, developing adaptive protection models for new types of cyber threats, particularly using artificial intelligence, and harmonizing national standards with international ones.

Keywords: CYBERSECURITY, DATABASE SERVERS, ENCRYPTION, ACCESS CONTROL, AUDIT, SQL INJECTIONS, CLOUD TECHNOLOGIES, BACKUP, GDPR, ISO/IEC 27001.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному цифровому світі сервери баз даних є ключовими компонентами інформаційних систем, що забезпечують зберігання, обробку та управління чутливою інформацією, такою як персональні дані, фінансові записи чи комерційні таємниці. Зростання кількості та складності кібератак, зокрема SQL-ін’єкцій, атак на автентифікацію, інсайдерських загроз і програм-вимагачів, робить захист серверів баз даних критично важливим завданням. Традиційні методи безпеки, такі як базові антивіруси чи слабкі політики доступу, часто виявляються недостатніми для протидії сучасним загрозам, які постійно еволюціонують. Технічні, програмні та організаційні заходи захисту, включаючи шифрування, контроль доступу, аудит і навчання персоналу, відіграють ключову роль у забезпеченні конфіденційності, цілісності та доступності даних. Актуальність теми зумовлена необхідністю розробки комплексних моделей захисту серверів баз даних, які враховують специфіку їхньої архітектури, типи даних і нормативні вимоги, а також зростанням важливості кібербезпеки в умовах цифрової трансформації.

Мета дослідження – розробка теоретичних основ і практичних рекомендацій щодо організації захисту інформації серверів баз даних для забезпечення їхньої безпеки, зниження ризиків кібератак і відповідності нормативним вимогам. Для досягнення мети поставлено такі завдання:

- систематизувати теоретичні основи захисту серверів баз даних, включаючи їх класифікацію за типом даних, архітектурою та рівнем критичності.
- проаналізувати основні загрози інформаційній безпеці серверів баз даних, такі як SQL-ін’єкції, атаки на автентифікацію та інсайдерські загрози.
- вивчити нормативно-правові засади захисту інформації в Україні та світі, включаючи GDPR, ISO/IEC 27001 і українське законодавство.
- провести аналіз технічних засобів захисту, таких як шифрування, брандмауери та системи моніторингу.

- дослідити програмні методи забезпечення безпеки, включаючи параметризовані запити, аудит і оновлення програмного забезпечення.
- описати організаційні заходи захисту, такі як політики безпеки, навчання персоналу та планування реагування на інциденти.
- розробити модель захисту інформації для серверів баз даних на основі оцінки ризиків і багаторівневого підходу.
- впровадити та протестувати систему захисту на прикладі серверного середовища PostgreSQL в AWS.
- оцінити ефективність запропонованих заходів захисту за критеріями стійкості до атак, якості аудиту та відповідності нормативним вимогам.

Об’єкт дослідження – процеси забезпечення інформаційної безпеки серверів баз даних, що включають захист від кіберзагроз, забезпечення конфіденційності, цілісності та доступності даних у різних серверних середовищах.

Предмет дослідження – технічні, програмні та організаційні методи і засоби захисту серверів баз даних, включаючи шифрування, контроль доступу, аудит, резервне копіювання та політики безпеки, що застосовуються для протидії кіберзагрозам.

Практичне значення отриманих результатів. Результати дослідження мають практичну цінність для організацій, які використовують сервери баз даних для обробки чутливої інформації. Запропонована модель захисту, що включає шифрування, контроль доступу, аудит і резервне копіювання, дозволяє знизити ризики кібератак і забезпечити відповідність міжнародним і національним стандартам, таким як GDPR і ДСТУ ISO/IEC 27001. Рекомендації щодо впровадження системи захисту на прикладі PostgreSQL в AWS можуть бути використані IT-фахівцями та адміністраторами баз даних для створення надійних і адаптивних систем безпеки. Результати також сприяють підвищенню обізнаності про кіберзагрози та зниженню впливу людського фактора через навчання персоналу, що є важливим для підтримки довіри до інформаційних систем.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ СЕРВЕРІВ БАЗ ДАНИХ

1.1 Поняття та класифікація серверів баз даних у контексті кібербезпеки

Сервер баз даних є ключовим компонентом інформаційних систем, призначеним для централізованого зберігання, обробки, управління та надання доступу до даних у структурованому, напівструктурованому або неструктурованому вигляді. Це може бути спеціалізоване програмне забезпечення, що працює на фізичному чи віртуальному сервері, або комплексна апаратно-програмна система, яка включає серверне обладнання, операційні системи та системи управління базами даних.

У контексті кібербезпеки сервери баз даних мають критично важливе значення, оскільки вони часто містять чутливу інформацію, таку як персональні дані користувачів, фінансові записи, комерційні таємниці, інтелектуальну власність або державні секрети. Захист серверів баз даних є складним завданням, яке спрямоване на забезпечення конфіденційності, тобто захисту від несанкціонованого доступу, цілісності, тобто запобігання неавторизованим змінам даних, та доступності, тобто гарантії безперебійного доступу до даних для легітимних користувачів. Ці принципи є основою кібербезпеки серверів баз даних і формують фундамент для розробки стратегій їхнього захисту.

Сервер баз даних виконує низку важливих функцій, що роблять його центральним елементом інформаційної інфраструктури. Він обробляє запити від клієнтських додатків, виконує транзакції, забезпечує цілісність даних, підтримує механізми автентифікації та авторизації, а також керує процесами резервного копіювання та відновлення даних [1].

У сучасних умовах сервери баз даних можуть бути розгорнуті в різних середовищах: локально, тобто на власних серверах організації, у хмарних платформах, таких як Amazon Relational Database Service, Google Cloud SQL чи Microsoft Azure SQL, або в гібридних конфігураціях, що поєднують локальні та хмарні ресурси. Кожне з цих середовищ створює унікальні виклики для кібербезпеки. Наприклад, локальні сервери потребують фізичного захисту

серверних приміщень і мережевої інфраструктури, тоді як хмарні сервери стикаються з ризиками, пов’язаними з неправильною конфігурацією хмарного середовища, слабкими політиками доступу або вразливостями в програмних інтерфейсах.

Кібербезпека серверів баз даних набуває особливої актуальності через зростання кількості та складності кібератак, спрямованих на отримання доступу до даних. Зловмисники використовують різноманітні методи атак, включаючи SQL-ін’єкції, спроби підбору паролів або використання вкрадених облікових даних, експлуатацію вразливостей у системах управління базами даних, фішинг, атаки типу "людина посередині" або атаки на відмову в обслуговуванні. Крім того, значну загрозу становлять інсайдерські атаки, коли співробітники чи підрядники зловживають своїм доступом до даних.

Для протидії цим загрозам застосовуються комплексні заходи безпеки, такі як шифрування даних у спокої та під час передачі, впровадження моделей контролю доступу на основі ролей або атрибутів, регулярне оновлення програмного забезпечення для усунення вразливостей, моніторинг активності користувачів, використання систем виявлення та запобігання вторгненням, а також створення надійних планів резервного копіювання та відновлення даних.

Класифікація серверів баз даних у контексті кібербезпеки дозволяє систематизувати підходи до їхнього захисту, враховуючи різноманітність їхніх типів, архітектур і функціонального призначення [2]. Основні критерії класифікації включають:

1. Тип даних - сервери можуть обробляти структуровані дані, такі як реляційні бази даних (наприклад, MySQL, PostgreSQL, Oracle Database), напівструктуровані дані, такі як NoSQL бази (наприклад, MongoDB, Cassandra, DynamoDB), або неструктуровані дані, такі як файлові чи об’єктні сховища (наприклад, Amazon S3). Реляційні бази даних часто стають мішенню SQL-ін’єкцій, тоді як NoSQL бази вразливі до атак через слабкі конфігурації програмних інтерфейсів або недостатній контроль доступу.

2. Архітектура - сервери поділяються на локальні, розгорнуті в межах організації, хмарні, розміщені на платформах Amazon Web Services, Microsoft Azure чи Google Cloud, та гібридні, що поєднують локальні та хмарні ресурси. Локальні сервери потребують фізичного захисту обладнання, тоді як хмарні сервери вимагають уваги до безпеки мережевих з'єднань, конфігурації хмарного середовища та захисту даних у транзиті.

3. Призначення - сервери можуть бути транзакційними, призначеними для обробки великої кількості коротких транзакцій (Online Transaction Processing), аналітичними, що використовуються для аналізу великих обсягів даних (Online Analytical Processing), або універсальними. Транзакційні сервери частіше зазнають атак на доступність, таких як атаки на відмову в обслуговуванні, тоді як аналітичні сервери є мішенню для викрадення великих масивів даних.

4. Рівень критичності - сервери, що містять конфіденційні дані, наприклад, медичні, фінансові чи державні, потребують посилених заходів безпеки, таких як шифрування на рівні бази даних, багатофакторна автентифікація, аудит дій користувачів і захист від витоку даних.

5. Технологічна платформа - сервери базуються на різних системах управління базами даних, таких як Oracle Database, Microsoft SQL Server, MySQL, PostgreSQL, MongoDB, Cassandra тощо. Кожна платформа має власний набір вразливостей, які необхідно враховувати при розробці стратегії захисту. Наприклад, застарілі версії MySQL можуть бути вразливими до відомих експлойтів, а MongoDB – до атак через неправильно налаштовані права доступу.

Для забезпечення безпеки серверів баз даних необхідно враховувати їхню специфіку та потенційні загрози. Наприклад, реляційні бази даних потребують захисту від SQL-ін'єкцій шляхом використання параметризованих запитів, валідації вхідних даних і фільтрації запитів. NoSQL бази даних, які часто використовують RESTful або GraphQL інтерфейси, вимагають уваги до безпеки програмних інтерфейсів і захисту від атак на основі неправильно налаштованих доступів.

Хмарні сервери потребують правильного налаштування політик безпеки, таких як обмеження доступу за IP-адресами, використання віртуальних приватних хмар і шифрування даних у транзиті. Локальні сервери, у свою чергу, потребують фізичного захисту серверних приміщень, контролю доступу до обладнання та захисту від атак на локальну мережу [4].

Моніторинг і аудит активності серверів є ще одним важливим аспектом безпеки. Системи моніторингу дозволяють виявляти підозрілі дії, такі як масові запити до бази даних, спроби несанкціонованого доступу або аномальна поведінка користувачів. Аудит дій користувачів, включаючи журнали доступу та змін, допомагає не лише виявляти інциденти, але й аналізувати їх для запобігання майбутнім атакам [4]. Крім того, впровадження принципів мінімальних привілеїв, коли користувачі та додатки отримують доступ лише до необхідних даних і функцій, значно знижує ризик зловживань.

Резервне копіювання даних і розробка планів відновлення після атак є невід’ємною частиною стратегії захисту. Регулярне створення зашифрованих резервних копій, їх зберігання в ізольованих середовищах і тестування процедур відновлення дозволяють мінімізувати втрати в разі кібератак, таких як атаки програм-вимагачів [5]. Крім того, важливо проводити регулярне навчання персоналу з питань кібербезпеки, оскільки людський фактор часто є слабкою ланкою в системі захисту.

Загалом, класифікація серверів баз даних за типом даних, архітектурою, призначенням, рівнем критичності та технологічною платформою дозволяє розробити диференційовані стратегії захисту, що враховують специфіку кожної системи. У сучасному світі, де кіберзагрози постійно еволюціонують, захист серверів баз даних вимагає комплексного підходу, що поєднує технічні заходи, такі як шифрування та моніторинг, організаційні заходи, такі як навчання персоналу, та адміністративні заходи, такі як розробка політик безпеки. Забезпечення безпеки серверів баз даних не лише захищає цінну інформацію, але й сприяє підтримці довіри користувачів, клієнтів і партнерів, а також відповідності міжнародним і

національним нормативним вимогам, таким як Загальний регламент захисту даних, стандарти безпеки медичних даних чи стандарти безпеки платіжних систем.

1.2 Основні загрози інформаційній безпеці серверів баз даних

Інформаційна безпека серверів баз даних є критично важливим аспектом сучасних інформаційних систем, оскільки вони зберігають чутливу інформацію, таку як персональні дані, фінансові записи, комерційні таємниці чи державні секрети. Сервери баз даних є привабливою мішенню для зловмисників через їхню цінність і потенційні вразливості, які можуть бути використані для компрометації даних. Загрози інформаційній безпеці серверів баз даних охоплюють широкий спектр атак, які можуть порушити конфіденційність, цілісність або доступність даних. Ці загрози виникають як через зовнішні атаки, так і через внутрішні недоліки, такі як помилки конфігурації чи недостатній контроль доступу [2].

Однією з найпоширеніших загроз є використання вразливостей у програмному забезпеченні систем управління базами даних. Зловмисники можуть експлуатувати застарілі версії програмного забезпечення, які містять відомі вразливості, для отримання несанкціонованого доступу до даних. Наприклад, якщо адміністратор не оновлює систему управління базами даних, хакери можуть скористатися відомими експлойтами для проникнення в систему. Крім того, неправильно налаштовані сервери, особливо в хмарних середовищах, часто стають жертвами атак через відкриті порти або слабкі паролі. Такі помилки конфігурації дозволяють зловмисникам отримати доступ до бази даних без значних зусиль [6].

Ще одним серйозним ризиком є атаки, спрямовані на маніпуляцію запитами до бази даних. Наприклад, зловмисники можуть вводити шкідливий код у запити, щоб отримати доступ до даних, змінити їх або навіть видалити. Такі атаки часто спрямовані на реляційні бази даних, але також можуть стосуватися баз даних NoSQL, якщо їхні інтерфейси недостатньо захищені. Крім того, атаки на автентифікацію, такі як підбір паролів або використання вкрадених облікових даних, дозволяють зловмисникам отримати доступ до системи під виглядом

легітимного користувача. Ці методи часто поєднуються з соціальною інженерією, наприклад, фішингом, для отримання доступу до облікових даних адміністраторів чи користувачів.

Інсайдерські загрози також становлять значний ризик. Співробітники чи підрядники, які мають доступ до серверів баз даних, можуть навмисно або ненавмисно спричинити витік даних. Наприклад, необережне поводження з даними або зловживання привілеями доступу може призвести до компрометації інформації. Атаки на доступність, спрямовані на порушення роботи серверів, також є поширеними [7].

Такі атаки можуть блокувати доступ до даних для легітимних користувачів, що особливо критично для транзакційних систем, де безперервна доступність є ключовою вимогою.

Для наочності основні категорії загроз інформаційній безпеці серверів баз даних узагальнено в таблиці 1.1, яка представлена нижче.

Таблиця 1.1 – Основні загрози безпеці серверів баз даних

Тип загрози	Опис	Вплив на безпеку
Експлуатація вразливостей	Використання відомих вразливостей у застарілих версіях СУБД	Несанкціонований доступ, витік даних
Помилки конфігурації	Неправильне налаштування серверів, відкриті порти, слабкі паролі	Несанкціонований доступ, компрометація даних
Маніпуляція запитами	Введення шкідливого коду в запити до бази даних	Витік, зміна або видалення даних
Атаки на автентифікацію	Підбір паролів, використання вкрадених облікових даних	Несанкціонований доступ, компрометація даних

Продовження таблиці 1.1

Тип загрози	Опис	Вплив на безпеку
Інсайдерські загрози	Зловживання доступом співробітниками чи підрядниками	Витік даних, порушення цілісності
Атаки на доступність	Блокування доступу до сервера через перевантаження	Порушення доступності, зупинка роботи системи

Як видно з таблиці, кожна загроза має специфічний вплив на безпеку, що вимагає індивідуального підходу до захисту. Наприклад, для захисту від експлуатації вразливостей необхідно регулярно оновлювати програмне забезпечення та застосовувати патчі безпеки. Помилки конфігурації можна мінімізувати шляхом ретельного налаштування серверів і використання автоматизованих інструментів для перевірки безпеки. Для запобігання маніпуляціям запитами до бази даних застосовуються методи валідації вхідних даних і параметризовані запити. Атаки на автентифікацію вимагають впровадження складних паролів, багатофакторної автентифікації та моніторингу підозрілих спроб входу.

Інсайдерські загрози потребують особливого підходу, включаючи впровадження принципу мінімальних привілеїв, коли користувачі отримують доступ лише до необхідних даних, а також регулярний аудит дій користувачів. Для захисту від атак на доступність необхідно використовувати системи захисту від перевантаження, такі як обмеження трафіку чи розподілені системи, а також створювати плани відновлення після атак. Крім того, шифрування даних у спокої та під час передачі є обов’язковим для захисту від витоку інформації, особливо в хмарних середовищах, де дані можуть передаватися через незахищені мережі [7].

Ще однією важливою загрозою є атаки програм-вимагачів, які шифрують дані на сервері та вимагають викуп за їхнє відновлення. Такі атаки можуть мати катастрофічні наслідки, якщо не існує актуальних резервних копій. Регулярне

створення зашифрованих резервних копій і їх ізольоване зберігання є ключовим заходом для забезпечення можливості відновлення даних. Крім того, недостатня обізнаність персоналу може сприяти успіху атак, особливо тих, що базуються на соціальній інженерії [8]. Проведення регулярних тренінгів з кібербезпеки допомагає зменшити ризик людського фактора.

Загрози інформаційній безпеці серверів баз даних є різноманітними та багатогранними, охоплюючи як технічні, так і організаційні аспекти. Для ефективного захисту необхідно застосовувати комплексний підхід, який включає технічні заходи, такі як шифрування, моніторинг і оновлення програмного забезпечення, а також організаційні заходи, такі як навчання персоналу та розробка політик безпеки.

1.3 Нормативно-правові засади захисту інформації в Україні та світі

Нормативно-правові засади захисту інформації є основою для створення ефективних механізмів забезпечення кібербезпеки, зокрема для серверів баз даних. Вони встановлюють стандарти, вимоги та процедури, які регулюють захист даних від несанкціонованого доступу, витоку, модифікації чи знищення. В Україні та світі ці засади формуються через національні законодавства, міжнародні стандарти та галузеві регуляції, які враховують специфіку інформаційних технологій і виклики кіберзагроз. Ці норми спрямовані на захист конфіденційності, цілісності та доступності даних, а також на забезпечення відповідальності організацій за порушення безпеки.

В Україні захист інформації регулюється низкою законодавчих актів, які створюють правову основу для забезпечення кібербезпеки. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" визначає принципи захисту інформації, включаючи вимоги до технічних і організаційних заходів для забезпечення безпеки даних у комп’ютерних системах, таких як сервери баз даних [9]. Закон України "Про захист персональних даних" встановлює правила обробки персональних даних, включаючи вимоги до їхнього зберігання,

передачі та захисту від несанкціонованого доступу. Цей закон є особливо актуальним для серверів баз даних, які містять персональну інформацію, таку як імена, адреси чи фінансові дані [10].

Крім того, Закон України "Про основні засади забезпечення кібербезпеки України" визначає ключові аспекти захисту інформаційних систем, включаючи критичну інфраструктуру, до якої можуть належати сервери баз даних, що обробляють дані державного значення. Цей закон встановлює вимоги до впровадження систем управління кібербезпекою, проведення аудитів безпеки та реагування на кіберінциденти [11]. Для організацій, які працюють із критичною інфраструктурою, передбачено обов’язкове впровадження сертифікованих засобів захисту інформації. Також в Україні діють галузеві стандарти, такі як ДСТУ ISO/IEC 27001, який адаптує міжнародний стандарт управління інформаційною безпекою, встановлюючи вимоги до створення, впровадження та підтримки систем управління інформаційною безпекою [12].

На міжнародному рівні захист інформації регулюється низкою стандартів і нормативних актів, які мають глобальний вплив. Одним із найвідоміших є Загальний регламент захисту даних (General Data Protection Regulation, GDPR), який діє в Європейському Союзі з 2018 року. GDPR встановлює суворі вимоги до обробки персональних даних, включаючи принципи прозорості, мінімізації даних і забезпечення безпеки. Організації, які працюють із даними громадян ЄС, зобов’язані впроваджувати технічні та організаційні заходи для захисту даних, такі як шифрування, контроль доступу та аудит. Порушення GDPR може призвести до значних штрафів, що робить цей регламент важливим для компаній, які використовують сервери баз даних для обробки даних європейських користувачів [13].

Ще одним важливим міжнародним стандартом є ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою. Цей стандарт є універсальним і застосовується в усьому світі для оцінки та вдосконалення безпеки інформаційних систем, включаючи сервери баз даних. Він передбачає оцінку ризиків, впровадження заходів безпеки та регулярний аудит [12]. Інший стандарт,

ISO/IEC 27002, доповнює ISO/IEC 27001, надаючи практичні рекомендації щодо впровадження заходів безпеки, таких як управління доступом, шифрування та моніторинг.

У США захист інформації регулюється кількома галузевими нормативними актами. Наприклад, закон HIPAA (Health Insurance Portability and Accountability Act) встановлює вимоги до захисту медичних даних, які обробляються серверами баз даних у медичних установах [15]. PCI DSS (Payment Card Industry Data Security Standard) є обов'язковим для організацій, які обробляють дані платіжних карток, і передбачає суворі вимоги до шифрування, контролю доступу та моніторингу серверів баз даних [16]. Закон CCPA (California Consumer Privacy Act) у Каліфорнії надає споживачам право контролювати свої персональні дані, що також впливає на організацію безпеки серверів баз даних [16].

Міжнародні угоди, такі як Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, також відіграють важливу роль. Ця конвенція, до якої приєдналася Україна, встановлює принципи захисту даних і сприяє гармонізації законодавства між країнами. Крім того, міжнародні організації, такі як NIST (National Institute of Standards and Technology) у США, розробляють рекомендації, наприклад NIST SP 800-53, які широко використовуються для захисту інформаційних систем, включаючи сервери баз даних [17].

Важливим аспектом є гармонізація українського законодавства з міжнародними стандартами, особливо з огляду на інтеграцію України до Європейського Союзу. Наприклад, Закон України "Про захист персональних даних" був оновлений для відповідності принципам GDPR. Це включає вимоги до повідомлення про витоки даних, забезпечення права суб'єктів даних на доступ до інформації та впровадження механізмів захисту даних на етапі проектування [10].

Нормативно-правові засади захисту інформації в Україні та світі створюють комплексну систему, яка регулює безпеку серверів баз даних. В Україні ключовими є закони про захист інформації, персональних даних і кібербезпеку, які доповнюються галузевими стандартами та міжнародними нормами. На глобальному рівні стандарти, такі як GDPR, ISO/IEC 27001, HIPAA і PCI DSS,

встановлюють високі вимоги до захисту даних, що є особливо важливим для серверів баз даних, які обробляють чутливу інформацію. Ці норми не лише забезпечують захист даних, але й сприяють підвищенню довіри користувачів і відповідності організацій міжнародним і національним вимогам.

Теоретичні основи захисту інформації серверів баз даних підкреслюють їхню ключову роль у сучасних інформаційних системах, де вони забезпечують зберігання, обробку та управління чутливими даними. Сервери баз даних класифікуються за типом даних (структуровані, напівструктуровані, неструктуровані), архітектурою (локальні, хмарні, гібридні), призначенням (транзакційні, аналітичні) та рівнем критичності, що дозволяє диференціювати підходи до їхнього захисту. Основними загрозами є SQL-ін’єкції, атаки на автентифікацію, інсайдерські загрози, атаки на відмову в обслуговуванні та помилки конфігурації, які потребують комплексного підходу до безпеки, включаючи шифрування, контроль доступу, моніторинг і резервне копіювання. Нормативно-правові засади, такі як Конституція України, Закони України "Про захист інформації в інформаційно-телекомунікаційних системах" і "Про захист персональних даних", а також міжнародні стандарти GDPR та ISO/IEC 27001, встановлюють вимоги до захисту даних і відповідальності організацій. Ці норми забезпечують правову основу для створення ефективних систем безпеки, що відповідають сучасним викликам кібербезпеки, сприяючи захисту інформації та підтримці довіри до інформаційних систем.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ СЕРВЕРІВ БАЗ ДАНИХ

2.1 Технічні засоби захисту інформації серверів баз даних

Технічні засоби захисту інформації серверів баз даних є ключовим елементом забезпечення безпеки даних, що зберігаються, обробляються та передаються в інформаційних системах. Ці засоби включають апаратні та програмні рішення, спрямовані на захист конфіденційності, цілісності та доступності даних, а також на запобігання несанкціонованому доступу, витоку інформації чи її пошкодженню. У сучасних умовах, коли сервери баз даних стають мішенню різноманітних кібератак, таких як експлуатація вразливостей, атаки на автентифікацію чи маніпуляція запитами, технічні засоби відіграють вирішальну роль у створенні багаторівневої системи захисту. Вони охоплюють широкий спектр технологій, від шифрування даних до систем моніторингу та фізичного захисту серверного обладнання.

Одним із основних технічних засобів є шифрування даних, яке застосовується як для даних у спокої, так і для даних під час передачі. Шифрування у спокої захищає інформацію, що зберігається на серверах, від несанкціонованого доступу в разі фізичного чи віртуального проникнення. Наприклад, використання алгоритмів AES-256 забезпечує високий рівень безпеки для даних, збережених у базі. Шифрування даних під час передачі, наприклад, через протоколи TLS/SSL, гарантує захист інформації, що передається між сервером і клієнтськими додатками. Це особливо важливо для хмарних серверів, де дані можуть передаватися через загальнодоступні мережі [18].

Іншим важливим засобом є системи контролю доступу, які обмежують доступ до серверів баз даних лише для авторизованих користувачів. Це включає використання складних паролів, багатофакторної автентифікації та управління доступом на основі ролей. Наприклад, системи управління базами даних, такі як MySQL чи PostgreSQL, дозволяють налаштувати детальні політики доступу, де кожен користувач має доступ лише до тих даних, які необхідні для виконання його завдань. Багатофакторна автентифікація, що поєднує паролі з біометричними даними чи одноразовими кодами, значно ускладнює несанкціонований доступ.

Моніторинг і аудит активності серверів є ще одним важливим технічним засобом. Системи моніторингу дозволяють виявляти підозрілі дії, такі як незвичайна кількість запитів до бази даних або спроби несанкціонованого доступу. Системи виявлення та запобігання вторгненням аналізують мережевий трафік і поведінку користувачів, щоб своєчасно виявити загрози. Наприклад, інструменти, такі як Splunk або ELK Stack, допомагають адміністраторам відстежувати журнали подій і виявляти аномалії. Аудит активності, включаючи журнали доступу та змін, дозволяє не лише реагувати на інциденти, але й аналізувати їх для запобігання майбутнім атакам.

Фізичний захист серверів також є важливим технічним засобом, особливо для локальних серверів. Це включає використання захищених серверних приміщень із контролем доступу, відеоспостереженням і системами захисту від пожеж чи інших фізичних загроз. Для хмарних серверів фізичний захист забезпечується постачальниками хмарних послуг, але організації повинні переконатися, що постачальник дотримується високих стандартів безпеки.

Для наочності основні технічні засоби захисту серверів баз даних узагальнено в таблиці 2.1.

Таблиця 2.1 – Технічні засоби захисту серверів баз даних

Технічний засіб	Опис	Ефект захисту
Шифрування даних	Використання алгоритмів (наприклад, AES-256, TLS/SSL) для захисту даних	Захист конфіденційності, запобігання витоку даних
Контроль доступу	Складні паролі, багатофакторна автентифікація, управління ролями	Обмеження несанкціонованого доступу
Технічний засіб	Опис	Ефект захисту
Моніторинг і аудит	Аналіз журналів подій, виявлення аномалій, системи IDS/IPS	Виявлення та запобігання загрозам

Продовження таблиці 2.1

Фізичний захист	Захищені серверні приміщення, відеоспостереження, захист від стихій	Запобігання фізичному доступу до обладнання
Резервне копіювання	Створення зашифрованих копій даних, ізольоване зберігання	Відновлення даних після атак чи збоїв
Оновлення програмного забезпечення	Встановлення патчів безпеки для усунення вразливостей	Запобігання експлуатації відомих вразливостей

Системи управління базами даних, такі як Oracle чи MongoDB, регулярно випускають оновлення, які необхідно встановлювати для забезпечення безпеки. Резервне копіювання даних є критично важливим для відновлення інформації після атак, таких як програми-вимагачі. Зашифровані резервні копії, збережені в ізольованих середовищах, дозволяють швидко відновити роботу системи без значних втрат.

Ще одним важливим аспектом є використання брандмауерів і мережевих засобів захисту. Брандмауери дозволяють обмежувати мережевий трафік до серверів баз даних, блокуючи неавторизовані підключення. Наприклад, налаштування брандмауера для дозволу доступу лише з певних IP-адрес значно знижує ризик атак. Для хмарних серверів використовуються віртуальні приватні хмари, які ізолюють сервер від загальнодоступних мереж. Крім того, системи захисту від атак на відмову в обслуговуванні, такі як Cloudflare або AWS Shield, допомагають забезпечити доступність серверів навіть під час масованих атак.

Для захисту від маніпуляцій запитами до бази даних застосовуються спеціалізовані інструменти, такі як засоби валідації вхідних даних і параметризовані запити. Ці методи особливо важливі для реляційних баз даних, які вразливі до SQL-ін’єкцій. Для NoSQL баз даних, таких як MongoDB, необхідно забезпечувати безпеку API, через які здійснюється доступ до даних. Використання інструментів аналізу коду, таких як SonarQube, допомагає виявляти вразливості в програмному забезпеченні ще на етапі розробки.

2.2 Програмні методи забезпечення безпеки баз даних

Програмні методи забезпечення безпеки баз даних є важливою складовою захисту інформації, що зберігається та обробляється на серверах. Ці методи включають програмні рішення та підходи, які інтегруються в системи управління базами даних або працюють як окремі інструменти для запобігання кіберзагрозам, таким як несанкціонований доступ, маніпуляція даними чи витік інформації. Вони спрямовані на захист конфіденційності, цілісності та доступності даних, а також на забезпечення відповідності нормативним вимогам. Програмні методи охоплюють широкий спектр технологій, від вбудованих функцій безпеки СУБД до спеціалізованих інструментів аналізу та моніторингу [19].

Одним із ключових програмних методів є управління доступом до бази даних. Сучасні СУБД, такі як MySQL, PostgreSQL, Oracle Database чи MongoDB, дозволяють налаштувати детальні політики доступу на основі ролей або атрибутів. Це дає змогу обмежити доступ до даних лише для авторизованих користувачів, які мають необхідні привілеї. Наприклад, адміністратор може налаштувати доступ так, щоб певний користувач мав права лише на читання певних таблиць, тоді як інший користувач зможе виконувати операції редагування. Для підвищення безпеки також використовується багатофакторна автентифікація, яка вимагає від користувачів підтвердження особи за допомогою додаткових засобів, таких як одноразові коди чи біометричні дані.

Ще одним важливим методом є захист від маніпуляцій запитами до бази даних, зокрема від SQL-ін’єкцій, які є поширеною загрозою для реляційних баз даних. Для цього застосовуються параметризовані запити та валідація вхідних даних. Параметризовані запити дозволяють відокремити код SQL від даних, що вводяться користувачем, що унеможливлює введення шкідливого коду. Наприклад, замість прямого включення даних у запит, СУБД використовує заповнювачі, які заповнюються перевіреними значеннями. Для NoSQL баз даних, таких як MongoDB, захист від подібних атак забезпечується через належне налаштування API та перевірку вхідних даних.

Шифрування даних є ще одним програмним методом, який широко застосовується для захисту інформації. СУБД можуть підтримувати шифрування на різних рівнях, наприклад, шифрування окремих стовпців у таблицях або цілих баз даних. Наприклад, Microsoft SQL Server підтримує функцію Transparent Data Encryption, яка автоматично шифрує дані у спокої. Для захисту даних під час передачі використовуються протоколи, такі як TLS, які забезпечують безпечний обмін інформацією між сервером і клієнтськими додатками. Це особливо важливо для хмарних баз даних, де дані передаються через загальнодоступні мережі [20].

Для наочності основні програмні методи забезпечення безпеки баз даних представлено на рисунку 2.1, який ілюструє їх взаємозв’язок і роль у захисті даних.

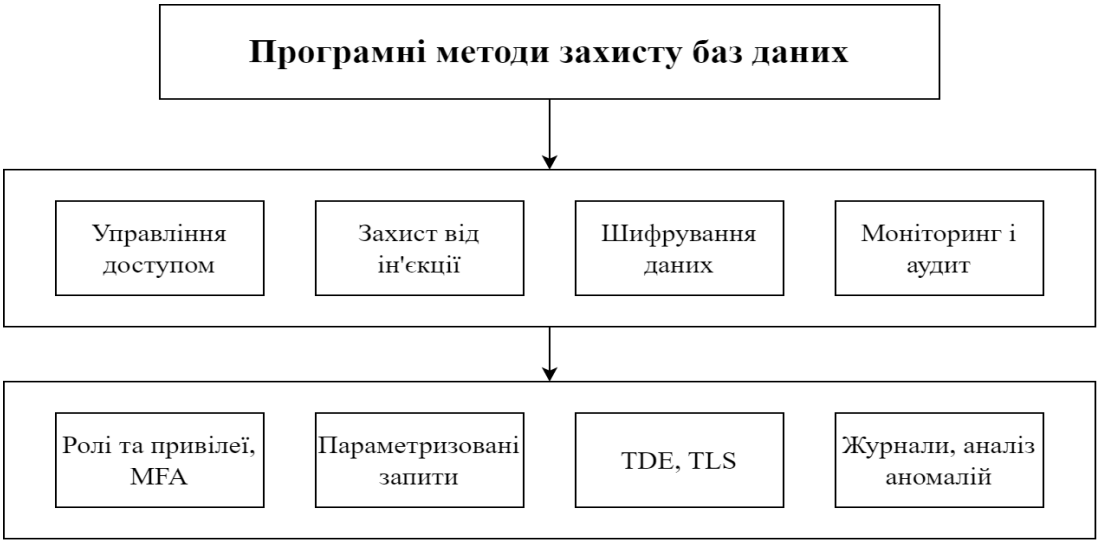

Рисунок 2.1 –Основні програмні методи забезпечення безпеки баз даних

Як видно зі схеми, кожен програмний метод відіграє унікальну роль у комплексному захисті баз даних. Моніторинг і аудит є ще одним важливим програмним методом. Системи моніторингу дозволяють відстежувати активність користувачів і виявляти підозрілі дії, такі як незвичайна кількість запитів або спроби несанкціонованого доступу. Наприклад, інструменти, такі як Oracle Audit Vault або IBM Guardium, забезпечують детальний аналіз подій у базі даних, включаючи журнали доступу та змін. Це дозволяє не лише реагувати на інциденти, але й проводити їх аналіз для вдосконалення безпеки.

Іншим важливим програмним методом є оновлення програмного забезпечення та застосування патчів безпеки. Застарілі версії СУБД можуть містити відомі вразливості, які зловмисники використовують для атак. Регулярне оновлення СУБД, таких як PostgreSQL чи MongoDB, дозволяє усунути ці вразливості та підвищити безпеку. Крім того, використання інструментів аналізу коду, таких як SonarQube, допомагає виявляти потенційні вразливості в коді додатків, які взаємодіють із базою даних, ще на етапі розробки.

Для захисту від атак на доступність, таких як атаки на відмову в обслуговуванні, застосовуються програмні методи, такі як обмеження кількості запитів (rate limiting) і використання розподілених систем. Наприклад, хмарні платформи, такі як AWS чи Azure, пропонують інструменти для автоматичного масштабування баз даних, що дозволяє підтримувати їхню доступність навіть під час високого навантаження. Також важливим є створення зашифрованих резервних копій даних, які дозволяють відновити інформацію після атак, таких як програми-вимагачі. СУБД, такі як MySQL, підтримують вбудовані інструменти для створення та управління резервними копіями.

2.3 Організаційні заходи захисту інформації на серверах

Організаційні заходи захисту інформації на серверах баз даних є важливою складовою комплексної системи кібербезпеки. Вони охоплюють процеси, політики та процедури, які спрямовані на мінімізацію ризиків, пов’язаних із людським фактором, неправильним управлінням або недостатньою координацією в організації. Ці заходи не потребують складних технічних рішень, але відіграють ключову роль у забезпеченні конфіденційності, цілісності та доступності даних. Організаційні заходи включають розробку політик безпеки, навчання персоналу, аудит і контроль доступу, а також планування реагування на інциденти [21].

Одним із основних організаційних заходів є розробка та впровадження політик безпеки інформації. Ці політики визначають правила поводження з даними, включаючи вимоги до їх зберігання, обробки та передачі. Наприклад, політика

може встановлювати, що доступ до серверів баз даних надається лише авторизованим співробітникам, а всі дії з даними мають бути задокументовані. Політики також включають принципи мінімальних привілеїв, коли користувачі отримують доступ лише до тих даних, які необхідні для виконання їхніх обов'язків. Впровадження таких політик допомагає знизити ризик інсайдерських загроз і помилок через неналежне використання доступу.

Навчання персоналу є ще одним важливим організаційним заходом. Людський фактор часто є слабкою ланкою в системі безпеки, оскільки співробітники можуть ненавмисно розкрити дані через фішинг або необережне поводження з інформацією. Регулярні тренінги з кібербезпеки, які включають навчання розпізнаванню фішингових атак, правильному використанню паролів і дотриманню політик безпеки, значно знижують ці ризики. Наприклад, співробітники повинні знати, як безпечно працювати з базами даних і уникати використання незахищених мереж для доступу до серверів.

Аудит і контроль є критично важливими для забезпечення безпеки. Регулярний аудит серверів баз даних дозволяє виявляти потенційні вразливості, такі як неправильно налаштовані права доступу або застарілі політики безпеки. Аудит включає перевірку журналів доступу, аналіз дій користувачів і оцінку відповідності нормативним вимогам, таким як Загальний регламент захисту даних. Контроль доступу передбачає періодичне оновлення облікових даних і перевірку прав користувачів, щоб забезпечити їх актуальність.

Планування реагування на інциденти є ще одним ключовим організаційним заходом. Організації повинні мати чіткий план дій на випадок кібератак, таких як витік даних або атака програми-вимагача. Цей план включає процедури виявлення інциденту, ізоляції ураженого сервера, відновлення даних із резервних копій і повідомлення зацікавлених сторін. Регулярне тестування таких планів, наприклад, через симуляцію кібератак, дозволяє переконатися в їхній ефективності [22].

Для наочності основні організаційні заходи захисту інформації на серверах баз даних узагальнено в таблиці 2.2.

Таблиця 2.2 – Організаційні заходи захисту серверів баз даних

Організаційний захід	Опис	Ефект захисту
Політики безпеки	Встановлення правил обробки даних і доступу до серверів	Зниження ризиків через чіткі інструкції
Навчання персоналу	Тренінги з кібербезпеки для співробітників	Зменшення впливу людського фактора
Аудит і контроль	Перевірка журналів, прав доступу та відповідності вимогам	Виявлення вразливостей і забезпечення відповідності
Планування реагування	Розробка планів на випадок кіберінцидентів	Швидке відновлення після атак

Як видно з таблиці, кожен захід сприяє створенню надійної системи безпеки. Наприклад, політики безпеки забезпечують єдиний підхід до захисту даних, тоді як навчання персоналу знижує ймовірність помилок. Аудит дозволяє своєчасно виявляти проблеми, а планування реагування забезпечує швидке відновлення після інцидентів.

Для ілюстрації одного з організаційних заходів, наприклад, автоматичного створення журналів аудиту, нижче наведено приклад коду на мові SQL для налаштування автоматичного логування дій користувачів у базі даних PostgreSQL.

```
-- Створення таблиці для зберігання логів аудиту
CREATE TABLE audit_log (
    log_id SERIAL PRIMARY KEY,
    user_name VARCHAR(50),
    action VARCHAR(100),
    table_name VARCHAR(50),
    action_time TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
-- Створення тригера для логування змін у таблиці users
CREATE OR REPLACE FUNCTION log_user_changes()
RETURNS TRIGGER AS $$
BEGIN
    INSERT INTO audit_log (user_name, action,
table_name)
```

```
    VALUES (current_user, TG_OP, TG_TABLE_NAME);
    RETURN NEW;
END;
$$ LANGUAGE plpgsql;
-- Прив'язка тригера до таблиці users
CREATE TRIGGER users_audit_trigger
AFTER INSERT OR UPDATE OR DELETE ON users
FOR EACH ROW EXECUTE FUNCTION log_user_changes();
```

Цей код створює таблицю для зберігання логів аудиту та налаштовує тригер, який автоматично записує дії користувачів (додавання, оновлення, видалення) у таблиці users. Такі журнали дозволяють відстежувати зміни в базі даних і виявляти підозрілі дії, що є частиною організаційного заходу аудиту.

Організаційні заходи захисту інформації на серверах баз даних, забезпечують системний підхід до безпеки. Вони включають розробку політик, навчання персоналу, аудит і контроль, а також планування реагування на інциденти. Використання таких заходів у поєднанні з технічними та програмними методами дозволяє створити надійну систему захисту, яка мінімізує ризики кіберзагроз і забезпечує відповідність нормативним вимогам.

Аналіз методів та засобів захисту серверів баз даних демонструє необхідність комплексного підходу до забезпечення їхньої безпеки, який поєднує технічні, програмні та організаційні заходи. Технічні засоби, такі як шифрування даних (AES-256, TLS/SSL), контроль доступу, брандмауери, системи моніторингу (IDS/IPS) та фізичний захист серверних приміщень, створюють надійний бар’єр проти зовнішніх і внутрішніх загроз, таких як несанкціонований доступ чи атаки на доступність. Програмні методи, включаючи параметризовані запити, аудит дій користувачів, оновлення програмного забезпечення та захист API, ефективно протидіють SQL-ін’єкціям і вразливостям у системах управління базами даних, таких як PostgreSQL чи MongoDB. Організаційні заходи, зокрема розробка політик безпеки, навчання персоналу, регулярний аудит і планування реагування на інциденти, мінімізують ризики, пов’язані з людським фактором і управлінськими недоліками. Поєднання цих підходів дозволяє створити багаторівневу систему захисту, яка забезпечує конфіденційність, цілісність і доступність даних, відповідає нормативним вимогам і знижує ймовірність успішних кібератак.

3 ПРАКТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ЗАХИСТУ СЕРВЕРІВ БАЗ ДАНИХ

3.1 Розробка моделі захисту інформації для серверів баз даних

Розробка моделі захисту інформації для серверів баз даних є фундаментальним процесом, спрямованим на забезпечення безпеки даних, що зберігаються, обробляються та передаються в інформаційних системах. Така модель являє собою структуровану систему принципів, політик, процедур і технічних засобів, які мають на меті запобігання несанкціонованому доступу, витоку даних, їх модифікації чи знищенню. Модель розробляється з урахуванням специфіки серверів баз даних, їхньої архітектури, типу даних, рівня критичності та потенційних загроз, таких як атаки на автентифікацію, маніпуляція запитами чи програми-вимагачі. Вона забезпечує конфіденційність, цілісність і доступність даних, а також відповідність нормативним вимогам, наприклад, Загальному регламенту захисту даних чи національним стандартам кібербезпеки.

Першим етапом розробки моделі є оцінка ризиків, яка передбачає аналіз потенційних загроз і вразливостей. Загрози можуть включати SQL-ін’єкції, підбір паролів, інсайдерські дії чи атаки на відмову в обслуговуванні. Вразливості можуть виникати через застаріле програмне забезпечення, слабкі паролі або неправильну конфігурацію серверів, особливо в хмарних середовищах. На основі цього аналізу визначаються ключові активи, такі як персональні дані, фінансові записи чи комерційні таємниці, які потребують захисту. Оцінка ризиків допомагає визначити пріоритетність заходів безпеки та оптимально розподілити ресурси для їх реалізації.

Наступним кроком є визначення принципів захисту, які базуються на тріаді безпеки: конфіденційність, цілісність і доступність. Конфіденційність досягається через шифрування даних і контроль доступу, що обмежує доступ до серверів лише для авторизованих користувачів. Наприклад, системи управління базами даних дозволяють налаштувати ролі з різними привілеями, щоб користувачі мали доступ лише до необхідних даних. Цілісність забезпечується через механізми перевірки даних і журнали аудиту, які фіксують усі зміни в базі. Доступність підтримується

шляхом створення резервних копій і захисту від атак, що можуть перервати роботу сервера.

Модель захисту інформації передбачає багаторівневий підхід, який охоплює фізичний, мережевий, програмний і організаційний рівні. Фізичний рівень включає захист серверних приміщень від несанкціонованого доступу за допомогою систем контролю доступу та відеоспостереження. Мережевий рівень передбачає використання брандмауерів, віртуальних приватних хмар і обмеження доступу за IP-адресами. Програмний рівень охоплює використання параметризованих запитів для захисту від SQL-ін’єкцій, шифрування даних і оновлення програмного забезпечення. Організаційний рівень включає розробку політик безпеки, навчання персоналу та регулярний аудит.

Для ілюстрації практичного аспекту моделі захисту інформації нижче наведено приклад коду на мові SQL для реалізації контролю доступу та аудиту в базі даних PostgreSQL. Цей код демонструє створення ролей із різними привілеями та налаштування автоматичного логування дій користувачів, що є важливим елементом моделі захисту.

```
    -- Створення ролей для управління доступом
    CREATE ROLE read_only;
    CREATE ROLE read_write;
    CREATE ROLE admin;
    -- Надання прав доступу для ролі read_only
    GRANT SELECT ON ALL TABLES IN SCHEMA public TO read_only;
    -- Надання прав доступу для ролі read_write
    GRANT SELECT, INSERT, UPDATE ON ALL TABLES IN SCHEMA
public TO read_write;
    -- Надання всіх прав для ролі admin
    GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO
admin;
    -- Створення користувачів і призначення ролей
    CREATE USER user_reader WITH PASSWORD
'secure_password1';
    CREATE USER user_writer WITH PASSWORD
'secure_password2';
    CREATE USER user_admin WITH PASSWORD 'secure_password3';
    GRANT read_only TO user_reader;
    GRANT read_write TO user_writer;
    GRANT admin TO user_admin;
```

```
-- Створення таблиці для зберігання логів аудиту
CREATE TABLE audit_log (
    log_id SERIAL PRIMARY KEY,
    user_name VARCHAR(50),
    action VARCHAR(100),
    table_name VARCHAR(50),
    action_time TIMESTAMP DEFAULT CURRENT_TIMESTAMP);
-- Створення функції для логування змін
CREATE OR REPLACE FUNCTION log_changes()
RETURNS TRIGGER AS $$
BEGIN
    INSERT INTO audit_log (user_name, action,
table_name)
    VALUES (current_user, TG_OP, TG_TABLE_NAME);
    RETURN NEW;
END;
$$ LANGUAGE plpgsql;
-- Прив'язка тригера до таблиці (наприклад, users)
CREATE TRIGGER audit_trigger
AFTER INSERT OR UPDATE OR DELETE ON users
FOR EACH ROW EXECUTE FUNCTION log_changes();
```

Цей код створює три ролі (read_only, read_write, admin) з різними рівнями доступу, що відповідає принципу мінімальних привілеїв. Наприклад, користувач із роллю read_only може лише переглядати дані, тоді як користувач із роллю admin має повний доступ. Тригер автоматично записує дії (додавання, оновлення, видалення) у таблиці users до таблиці audit_log, що дозволяє відстежувати зміни та виявляти підозрілі дії.

Модель захисту інформації також включає планування реагування на інциденти. Це передбачає розробку процедур виявлення кібератак, ізоляції ураженого сервера, відновлення даних із резервних копій і повідомлення зацікавлених сторін. Регулярне тестування цих процедур через симуляцію атак дозволяє перевірити ефективність моделі та виявити її слабкі місця. Наприклад, тестування може включати симуляцію атаки програми-вимагача для перевірки швидкості відновлення даних.

Для забезпечення відповідності нормативним вимогам модель має враховувати стандарти, такі як Загальний регламент захисту даних, який вимагає повідомлення про витоки даних протягом 72 годин, або національні стандарти, такі

як ДСТУ ISO/IEC 27001, що визначають вимоги до систем управління інформаційною безпекою. Впровадження таких стандартів передбачає регулярний аудит і документування всіх заходів безпеки.

Загалом, розробка моделі захисту інформації для серверів баз даних є комплексним процесом, який поєднує оцінку ризиків, визначення принципів безпеки, багаторівневий захист і використання програмних засобів, таких як наведений вище код. Ця модель забезпечує надійний захист даних, мінімізує ризики кіберзагроз і підтримує довіру до інформаційних систем, відповідаючи сучасним нормативним вимогам.

3.2 Впровадження та тестування системи захисту на прикладі конкретного серверного середовища

Впровадження та тестування системи захисту серверів баз даних є практичним етапом, який забезпечує реалізацію розробленої моделі безпеки в конкретному серверному середовищі. Цей процес включає налаштування технічних і програмних засобів, організаційних заходів, а також перевірку їхньої ефективності через тестування. Для прикладу розглянемо впровадження системи захисту на сервері баз даних PostgreSQL, розгорнутому в хмарному середовищі, наприклад, Amazon Web Services (AWS). PostgreSQL є популярною реляційною СУБД, яка широко використовується для зберігання чутливих даних, таких як персональна інформація чи фінансові записи. Система захисту має забезпечувати конфіденційність, цілісність і доступність даних, а також відповідність нормативним вимогам, таким як Загальний регламент захисту даних.

Процес впровадження починається з налаштування серверного середовища. У хмарному середовищі AWS це включає створення екземпляра Amazon RDS для PostgreSQL із ізольованою віртуальною приватною хмарою (VPC). Для забезпечення безпеки на мережевому рівні налаштовуються групи безпеки (Security Groups), які дозволяють доступ до сервера лише з певних IP-адрес. Наприклад, можна обмежити доступ до порту 5432 (стандартний порт PostgreSQL) лише для

внутрішньої мережі організації. Для захисту даних у спокої та під час передачі використовується шифрування. Amazon RDS автоматично підтримує шифрування даних у спокої за допомогою AWS Key Management Service (KMS) і шифрування підключень через TLS.

На рівні СУБД впроваджуються програмні методи захисту, такі як управління доступом і аудит. Управління доступом передбачає створення ролей із різними привілеями, щоб обмежити доступ до даних відповідно до принципу мінімальних привілеїв. Наприклад, створюються ролі для читання, запису та адміністрування, а користувачі отримують лише необхідні права. Для відстеження дій користувачів налаштовується аудит, який записує всі операції з даними в спеціальну таблицю. Це дозволяє виявляти підозрілі дії, такі як масові зап Figuresи чи спроби несанкціонованого доступу.

Для захисту від SQL-ін’єкцій використовуються параметризовані запити, які відокремлюють код SQL від даних, що вводяться користувачем. Наприклад, у додатках, які взаємодіють із PostgreSQL, застосовуються підготовлені запити через бібліотеки, такі як psycopg2 для Python. Крім того, для забезпечення доступності даних налаштовується автоматичне резервне копіювання через AWS RDS, яке створює зашифровані копії даних і зберігає їх у ізольованому сховищі. Це дозволяє швидко відновити дані в разі атаки, наприклад, програми-вимагача.

Тестування системи захисту включає перевірку її ефективності через симуляцію атак і аналіз результатів. Наприклад, тестування може охоплювати спроби SQL-ін’єкцій, підбору паролів або атак на відмову в обслуговуванні. Для цього використовуються інструменти, такі як sqlmap для тестування SQL-ін’єкцій або спеціалізовані симулятори навантаження для перевірки стійкості сервера до атак на доступність. Після тестування аналізуються журнали аудиту та звіти безпеки, щоб виявити слабкі місця та вдосконалити систему захисту.

Нижче наведено приклад коду на мові SQL для налаштування управління доступом і аудиту в PostgreSQL, що є частиною системи захисту в цьому серверному середовищі.

```
-- Створення ролей для управління доступом
```

```
    CREATE ROLE read_only;
    CREATE ROLE read_write;
CREATE ROLE admin;
    -- Надання прав доступу для ролі read_only
GRANT SELECT ON ALL TABLES IN SCHEMA public TO read_only;
    -- Надання прав доступу для ролі read_write
GRANT SELECT, INSERT, UPDATE ON ALL TABLES IN SCHEMA public
TO read_write;
    -- Надання всіх прав для ролі admin
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO admin;
    -- Створення користувачів і призначення ролей
    CREATE    USER    app_user_reader    WITH    PASSWORD
'secure_password1';
    CREATE    USER    app_user_writer    WITH    PASSWORD
'secure_password2';
CREATE USER app_admin WITH PASSWORD 'secure_password3';
    GRANT read_only TO app_user_reader;
    GRANT read_write TO app_user_writer;
GRANT admin TO app_admin;
    -- Створення таблиці для зберігання логів аудиту
    CREATE TABLE audit_log (
        log_id SERIAL PRIMARY KEY,
        user_name VARCHAR(50),
        action VARCHAR(100),
        table_name VARCHAR(50),
        action_time TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
        query_text TEXT);
    -- Створення функції для логування змін
    CREATE OR REPLACE FUNCTION log_changes()
    RETURNS TRIGGER AS $$
    BEGIN
        INSERT   INTO   audit_log   (user_name,   action,
table_name, query_text)
        VALUES   (current_user,   TG_OP,   TG_TABLE_NAME,
current_query());
        RETURN NEW;
    END;
$$ LANGUAGE plpgsql;
    -- Прив'язка тригера до таблиці (наприклад, customers)
    CREATE TRIGGER audit_trigger
    AFTER INSERT OR UPDATE OR DELETE ON customers
FOR EACH ROW EXECUTE FUNCTION log_changes();
    -- Налаштування параметрів безпеки PostgreSQL
    ALTER SYSTEM SET log_connections = 'on';
    ALTER SYSTEM SET log_disconnections = 'on';
```

```
    ALTER SYSTEM SET log_statement = 'all';
SELECT pg_reload_conf();
```

Цей код створює ролі з різними привілеями, призначає їх користувачам і налаштовує аудит дій у таблиці customers. Додатково вмикається логування всіх підключень, відключень і SQL-запитів, що дозволяє відстежувати активність на сервері. Це є частиною системи захисту, яка забезпечує контроль доступу та моніторинг.

Для наочності нижче представлено рисунок 3.1, системи захисту серверного середовища PostgreSQL в AWS, яка ілюструє взаємозв'язок основних компонентів.

Рисунок 3.1 – Система захисту серверного середовища PostgreSQL в AWS

Як видно з рисунку, система захисту включає шифрування даних, контроль доступу, аудит і резервне копіювання, що забезпечують комплексний захист. Тестування системи передбачає перевірку всіх компонентів. Наприклад, для тестування контролю доступу можна спробувати підключитися до сервера з неавторизованої IP-адреси, щоб переконатися, що група безпеки блокує доступ. Для перевірки аудиту аналізуються записи в таблиці audit_log після виконання тестових операцій. Тестування резервного копіювання включає відновлення даних із копії в ізольованому середовищі.

Впровадження та тестування системи захисту на прикладі PostgreSQL в AWS включає налаштування шифрування, контролю доступу, аудиту та резервного

копіювання, як показано в коді та схемі. Цей підхід забезпечує надійний захист даних, мінімізує ризики кіберзагроз і відповідає нормативним вимогам, підтримуючи довіру до інформаційної системи.

3.3 Оцінка ефективності запропонованих заходів захисту

Оцінка ефективності запропонованих заходів захисту серверів баз даних є критичним етапом, який дозволяє визначити, наскільки успішно реалізована система безпеки здатна протистояти кіберзагрозам і забезпечувати конфіденційність, цілісність та доступність даних. Цей процес передбачає аналіз результативності технічних, програмних і організаційних заходів, їх відповідності нормативним вимогам, а також здатності мінімізувати ризики, виявлені під час оцінки загроз. Оцінка ефективності проводиться через комбінацію кількісних і якісних методів, включаючи тестування, аудит, аналіз журналів і зіставлення з галузевими стандартами, такими як Загальний регламент захисту даних чи ISO/IEC 27001.

Першим кроком оцінки є проведення тестування системи захисту. Тестування включає симуляцію реальних кібератак, таких як SQL-ін’єкції, спроби несанкціонованого доступу чи атаки на відмову в обслуговуванні. Наприклад, для перевірки захисту від SQL-ін’єкцій можна використати інструменти, такі як sqlmap, щоб оцінити, чи здатна система блокувати шкідливі запити. Тестування контролю доступу передбачає спроби підключення з неавторизованих IP-адрес або використання невірних облікових даних, щоб перевірити ефективність брандмауерів і багатофакторної автентифікації. Тестування доступності включає симуляцію високого навантаження на сервер для оцінки стійкості до атак на відмову в обслуговуванні.

Наступним етапом є аналіз журналів аудиту та моніторингу. Журнали дозволяють оцінити, чи фіксуються всі дії користувачів, включаючи підозрілі операції, такі як масові запити чи спроби зміни даних. Наприклад, якщо система аудиту правильно налаштована, вона має записувати всі операції з таблицями бази

даних, включаючи інформацію про користувача, час і тип дії. Аналіз журналів допомагає виявити слабкі місця, такі як недостатня деталізація логів або пропущені події, і оцінити швидкість реагування системи на інциденти.

Відповідність нормативним вимогам є ще одним важливим критерієм оцінки. Заходи захисту мають відповідати стандартам, таким як Загальний регламент захисту даних, який вимагає шифрування даних, повідомлення про витоки протягом 72 годин і забезпечення прав суб'єктів даних. Порівняння з ISO/IEC 27001 дозволяє оцінити, чи відповідає система управління інформаційною безпекою міжнародним стандартам. Наприклад, стандарт вимагає регулярного аудиту, оцінки ризиків і документування всіх заходів безпеки. Відповідність цим вимогам підтверджує, що система захисту є надійною та придатною для роботи з чутливими даними.

Оцінка ефективності також включає аналіз часу відновлення після інцидентів. Наприклад, тестування резервного копіювання передбачає симуляцію втрати даних через атаку програми-вимагача та перевірку швидкості й точності відновлення даних із зашифрованих копій. Ефективна система захисту має забезпечувати мінімальний час простою та повне відновлення даних без втрати інформації. Крім того, оцінюється вплив людського фактора: чи пройшли співробітники навчання з кібербезпеки, і чи дотримуються вони політик безпеки, таких як використання складних паролів і уникнення фішингових атак.

Для узагальнення основних критеріїв оцінки ефективності запропонованих заходів захисту нижче наведено таблицю 3.1.

Таблиця 3.1 – Критерії оцінки ефективності заходів захисту

Критерій оцінки	Опис	Очікуваний результат
Стійкість до атак	Перевірка захисту від SQL-ін'єкцій, несанкціонованого доступу	Блокування всіх тестових атак
Якість аудиту та моніторингу	Аналіз журналів подій і виявлення підозрілих дій	Повна фіксація всіх операцій і аномалій

Продовження таблиці 3.1

Відповідність нормативам	Перевірка відповідності стандартам (GDPR, ISO/IEC 27001)	Відсутність порушень нормативних вимог
Час відновлення	Тестування відновлення даних із резервних копій	Швидке відновлення без втрати даних
Ефективність навчання персоналу	Оцінка знань співробітників із кібербезпеки	Зниження ризиків через людський фактор

Результати оцінки дозволяють виявити слабкі місця, наприклад, недостатню швидкість реагування на інциденти чи прогалини в навчанні персоналу. На основі цих даних система захисту вдосконалюється, наприклад, шляхом оновлення політик безпеки, додавання нових інструментів моніторингу чи посилення шифрування.

Оцінка ефективності запропонованих заходів захисту серверів баз даних є комплексним процесом, який включає тестування, аналіз журналів, перевірку відповідності нормативним вимогам і оцінку часу відновлення. Результати, допомагають переконатися, що система захисту є надійною, здатною протистояти сучасним кіберзагрозам і підтримувати довіру до інформаційної системи.

Практичні аспекти організації захисту серверів баз даних підкреслюють важливість системного підходу до забезпечення безпеки інформації. Розроблена модель захисту, заснована на оцінці ризиків і багаторівневому підході, включає шифрування, контроль доступу, аудит і резервне копіювання, що дозволяє ефективно протистояти кіберзагрозам, таким як SQL-ін’єкції, атаки на автентифікацію та програми-вимагачі. Впровадження системи захисту на прикладі PostgreSQL в хмарному середовищі AWS продемонструвало практичну реалізацію цих заходів, включаючи налаштування груп безпеки, ролей із мінімальними привілеями, автоматичного логування дій користувачів і зашифрованих резервних копій. Тестування системи через симуляцію атак і аналіз журналів аудиту підтвердило її здатність виявляти та блокувати загрози, а також забезпечувати

швидке відновлення даних. Оцінка ефективності заходів захисту за критеріями стійкості до атак, якості аудиту, відповідності нормативним вимогам (GDPR, ISO/IEC 27001) і часу відновлення показала, що запропонована система є надійною та адаптивною. Отримані результати можуть бути використані для вдосконалення безпеки серверів баз даних, зниження ризиків і забезпечення довіри до інформаційних систем.

ВИСНОВКИ

Захист інформації серверів баз даних є критично важливим завданням у сучасних інформаційних системах, враховуючи зростання кіберзагроз і цінність даних, що обробляються. Проведене дослідження дозволило системно проаналізувати теоретичні основи, методи та практичні аспекти забезпечення безпеки серверів баз даних, що дало змогу сформувати цілісне уявлення про створення ефективної системи захисту.

На теоретичному рівні встановлено, що сервери баз даних є ключовими компонентами інформаційних систем, які обробляють структуровані, напівструктуровані та неструктуровані дані. Їх класифікація за типом даних, архітектурою, призначенням і рівнем критичності дозволяє розробляти диференційовані стратегії захисту. Основними загрозами для серверів баз даних є SQL-ін’єкції, атаки на автентифікацію, інсайдерські загрози, атаки на відмову в обслуговуванні та помилки конфігурації. Нормативно-правові засади, такі як Загальний регламент захисту даних, ISO/IEC 27001 та українське законодавство (зокрема, Закони України "Про захист інформації в інформаційно-телекомунікаційних системах" і "Про захист персональних даних"), встановлюють вимоги до захисту даних і відповідальності організацій.

Аналіз методів і засобів захисту виявив, що ефективна безпека серверів баз даних базується на комплексному підході, який поєднує технічні, програмні та організаційні заходи. Технічні засоби, такі як шифрування даних (AES-256, TLS), контроль доступу, брандмауери та системи моніторингу, забезпечують захист від зовнішніх і внутрішніх загроз. Програмні методи, включаючи параметризовані запити, аудит дій користувачів і оновлення програмного забезпечення, дозволяють мінімізувати вразливості, зокрема SQL-ін’єкції та експлуатацію застарілих версій СУБД. Організаційні заходи, такі як розробка політик безпеки, навчання персоналу, регулярний аудит і планування реагування на інциденти, знижують ризики, пов’язані з людським фактором і управлінськими недоліками.

Практичні аспекти захисту серверів баз даних, розглянуті на прикладі PostgreSQL в хмарному середовищі AWS, показали важливість багаторівневої моделі захисту, яка включає оцінку ризиків, шифрування, контроль доступу, аудит і резервне копіювання. Впровадження такої моделі, як продемонстровано через код для управління ролями та логування дій, забезпечує надійний захист і можливість відстеження підозрілих активностей. Тестування системи захисту через симуляцію атак, аналіз журналів і перевірку відновлення даних підтверджує її ефективність. Оцінка ефективності заходів захисту, заснована на критеріях стійкості до атак, якості аудиту, відповідності нормативним вимогам і часу відновлення, дозволяє виявляти слабкі місця та вдосконалювати систему.

Загалом, захист серверів баз даних вимагає системного підходу, який поєднує теоретичні знання, аналіз ризиків, використання технічних і програмних засобів, а також організаційні заходи. Розроблена модель захисту, протестована в конкретному серверному середовищі, забезпечує надійний захист даних, відповідає сучасним нормативним вимогам і сприяє підтримці довіри до інформаційних систем. Подальші дослідження можуть бути спрямовані на вдосконалення автоматизованих систем моніторингу та адаптацію моделей захисту до нових типів кіберзагроз, таких як атаки з використанням штучного інтелекту.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сікора О. В., Вдовичин Т. Я., Ших Н. В. Об’єктно-орієнтований підхід до створення електронної бібліотечної системи. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Технічні науки, 2022. Том 33 (72) № 1. С. 189-194.
2. Тишик І. Я. Організація захисту інформаційних систем на основі серверів баз даних. *Сучасний захист інформації*, 2025. №1. С. 259-268.
3. Строгуш О. Процеси доступу систем автоматизованого проєктування в хмарні сервіси. *Управління розвитком складних систем*, 2025. №61. С. 128-135.
4. Тишик І. Реалізація захисту бази даних на основі «Oracle audit valut and database firewall». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2024. №2(26). С. 56-70.
5. Ваврик Т., Гобир Л. Оптимізація захисту даних: превентивні та реактивні стратегії. *Інформаційні технології та суспільство*, 2024. №4 (15). С. 21-25.
6. Сороколіт М. Аудит інформаційної безпеки в умовах автоматизації облікових даних вітчизняних підприємств. Herald of Khmelnytskyi National University. *Economic sciences*, 2025. №342(3 (2). С. 61-66.
7. Яровенко Г. М., Петренко К. Ю., Ульяновська Ю. В., Небаба Н. О., Мормуль М. Ф. Розроблення структури інформаційної бази експертної системи виявлення інсайдерських кіберзагроз у банках. *Академічні візії*, (26). DOI: http://dx.doi.org/10.5281/zenodo.10350590
8. Вакуленко О. С. Захист від ransomware (програми-вимагача) як зовнішньої загрози. *Цифрова трансформація кібербезпеки* : тези доповідей, м. Київ, 22 жовтн. 2020 р. Київ. С. 73-76.
9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 16.12.2020 № 1089-IX. *Відомості Верховної Ради України*, 1994, № 31, ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 03.03.2025).

10. Про захист персональних даних : Закон України від 23.02.2012 № 4452-VI. *Відомості Верховної Ради України*, 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.03.2025).
11. Про основні засади забезпечення кібербезпеки України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради*, 2017, № 45, ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 03.03.2025).
12. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Чинний від 2023-08-22. Вимоги (ISO/IEC 27001:2022, IDT). Вид. офіц. Київ. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398 (дата звернення: 15.03.2025).
13. Li H., Yu L., He W. The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 2019. №22(1). PP. 1-6.
14. Cohen I. G., Mello M. M. HIPAA and protecting health information in the 21st century. *Jama*, 2018. №320(3). PP. 231-232.
15. Mollashaik A. S. Understanding PCI DSS V4. 0: A Comprehensive Guide to Payment Security Compliance. *Technology (IJRCAIT)*, 2025. №8(1). PP. 1396-1405.
16. Tran V. H., et al. Dark Patterns in the Opt-Out Process and Compliance with the California Consumer Privacy Act (CCPA). In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 2025. PP. 1-25. DOI: https://doi.org/10.1145/3706598.3714138
17. Kurii Y., Opirskyy I. Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013. *NIST Spec. Publ*, 2022. №800(53). PP. 21-32.
18. Ларченко М. Сучасні проблеми криптографічного захисту баз даних М. Ларченко // *Технічні науки та технології*. 2022. № 3 (29). С. 102-113.
19. Легомінова С. В., Щавінський Ю. В., Будзинський О. В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. *Сучасний захист інформації*, 2024. №2. С. 50-58.
20. Горбатовський Д. М. Формування безпеки бази даних: криптографія та контроль доступу. *Редакційна колегія*, 2024. С. 160-164.

21. Хлапонін, Ю. І. Комплексні системи захисту інформації : конспект лекцій / Ю. І. Хлапонін, А. М.Котенко ; Київ. нац. ун-т буд-ва і архіт. - Київ : КНУБА, 2022. Конспект лекцій КНУБА. 83 с.