КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії
(назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему: Методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах

Улянченко Максим Юрійович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ

_____

„___" _____20___ року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

МЕТОДИ ТА ЗАСОБИ АДМІНІСТРУВАННЯ КОМПОНЕНТІВ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Улянченко Максим Юрійович

(прізвище, ім'я та по батькові повністю)

125 ''Кібербезпека та захист інформації''

(спеціальність)

Безпека інформаційних і комунікаційних

(освітня програма)

Група БІКСм-24

Керівник Делембовський М.М.

(прізвище та ініціали)

к.т.н., доцент

(вчене звання, науковий ступінь)

Рецензент _____

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Кафедра: кібербезпеки та комп'ютерна інженерія
Освітній рівень: магістр
Спеціальність:125 ‘‘Кібербезпека та захист інформації’’
ОПП: Безпека інформаційних та комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри
_____
„___”_____20___ року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Улянченко Максим Юрійович
(прізвище, ім’я та по батькові здобувача)

1. Тема роботи Методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах
затверджена наказом ректора КНУБА №1635/23.2/25 від «30»вересня 2025року
2. Керівник роботи
Делембовський Максим Михайлович, к.т.н., доцент
_____
(прізвище, ім’я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту_____
4. Зміст пояснювальної записки за розділами:
Р. 1. Теоретичні основи захисту інформації в розподілених комп’ютерних системах
Р. 2. Методи та засоби адміністрування компонентів захисту інформації
Р. 3. Практичне застосування методів адміністрування захисту інформації

5. Графічний матеріал за розділами:
Р. 1. Вступ
Р. 2. Теоретичні основи захисту інформації в розподілених комп’ютерних системах
Р. 3. Методи та засоби адміністрування компонентів захисту інформації
Р. 4. Практичне застосування методів адміністрування захисту інформації
Р. 5.Додатки

6. Консультанти розділів кваліфікаційної випускної роботи

Розділи	Прізвища, ініціали та посади консультанта	Перевірив	
		дата	підпис
Розділ 1.	Делембовський М.М		
Розділ 2.	Делембовський М.М		
Розділ 3.	Делембовський М.М		

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1. Теоретичні основи захисту інформації в розподілених комп'ютерних системах	
Розділ 2. Методи та засоби адміністрування компонентів захисту інформації	
Розділ 3. Практичне застосування методів адміністрування захисту інформації	
Остаточне оформлення роботи	
Направлення роботи на рецензування, перевірку на плагіат	
Попередній захист роботи на кафедрі	

8. Дата видачі завдання _____

Керівник _____ _____
(підпис) (прізвище та ініціали)

Здобувач _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Улянченко М.Ю. «Методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах».

Обсяг роботи 85 сторінок, 8 рисунків, 22 таблиці, 53 джерела посилань.

РОЗПОДІЛЕНІ КОМП'ЮТЕРНІ СИСТЕМИ, ЗАХИСТ ІНФОРМАЦІЇ, АДМІНІСТРУВАННЯ БЕЗПЕКИ, УПРАВЛІННЯ ДОСТУПОМ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, МОНІТОРИНГ ІНЦИДЕНТІВ, РЕЗЕРВУВАННЯ ДАНИХ, ОЦІНКА РИЗИКІВ.

Об'єктом роботи є розподілені комп'ютерні системи, що забезпечують обробку, зберігання та передачу інформації в корпоративних і державних структурах.

Предметом роботи є методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах.

Метою роботи є розробка науково обґрунтованих методів та рекомендацій щодо адміністрування компонентів захисту інформації в розподілених комп'ютерних системах з урахуванням сучасних загроз та технологічних вимог.

Новизна роботи полягає у комплексному підході до організації адміністрування систем керування доступом, засобів криптографічного захисту, моніторингу подій безпеки та резервування даних у розподіленому середовищі. Запропоновано узгоджену модель взаємодії компонентів захисту, що підвищує стійкість систем до кіберзагроз та забезпечує цілісність, конфіденційність і доступність інформаційних ресурсів.

Методи дослідження включають аналітичний та порівняльний аналіз наукових джерел, системний та моделювальний підходи до побудови систем захисту, методи проектування та тестування інформаційних систем, а також методи експертних оцінок і управління ризиками.

У роботі проаналізовано загрози та вразливості інформаційних ресурсів у розподілених системах, розглянуто принципи та моделі захисту інформації, а також нормативно-правове забезпечення кіберзахисту в Україні та міжнародні стандарти. Проведено огляд існуючих програмних рішень для адміністрування безпеки, спроєктовано систему адміністрування компонентів захисту для умовної організації, реалізовано та протестовано вибрані засоби захисту, виконано оцінку їх ефективності та сформовано практичні рекомендації щодо вдосконалення систем безпеки.

Результати роботи можуть бути використані під час впровадження комплексних систем захисту інформації в корпоративних і державних інформаційно-комунікаційних системах. Вони також застосовні під час розроблення політик безпеки, процедур адміністрування доступу, криптографічного захисту, моніторингу інцидентів та резервного копіювання. Значимість роботи полягає у підвищенні практичної ефективності управління безпекою розподілених комп'ютерних систем в умовах зростання кіберзагроз та ускладнення їх архітектури.

SUMMARY

Ulianchenko M.Y. "Methods and Tools for Administering Information Security Components in Distributed Computer Systems."

The thesis comprises 85 pages, 8 figures, 22 tables, and 53 references.

DISTRIBUTED COMPUTER SYSTEMS, INFORMATION SECURITY, SECURITY ADMINISTRATION, ACCESS CONTROL, CRYPTOGRAPHIC PROTECTION, INCIDENT MONITORING, DATA BACKUP, RISK ASSESSMENT.

The research object is distributed computer systems that provide information processing, storage, and transmission in corporate and government organizations.

The research subject encompasses methods and tools for administering information security components in distributed computer systems.

The research aims to develop scientifically grounded methods and recommendations for administering information security components in distributed computer systems, taking into account contemporary threats and technological requirements.

The novelty of this work lies in a comprehensive approach to organizing the administration of access control systems, cryptographic protection tools, security event monitoring, and data backup in distributed environments. An integrated model for security component interaction is proposed, which enhances system resilience against cyber threats and ensures the integrity, confidentiality, and availability of information resources.

The research methodology includes analytical and comparative analysis of scientific sources, systematic and modeling approaches to building security systems, methods of information system design and testing, as well as expert assessment and risk management techniques.

The thesis analyzes threats and vulnerabilities of information resources in distributed systems, examines principles and models of information protection, and reviews the regulatory framework for cybersecurity in Ukraine alongside international standards. An overview of existing software solutions for security administration is provided, a security component administration system is designed for a hypothetical organization, selected security tools are implemented and tested, their effectiveness is evaluated, and practical recommendations for security system improvement are formulated.

The research findings can be applied when implementing comprehensive information security systems in corporate and government information and communication systems. They are also applicable in developing security policies, access administration procedures, cryptographic protection, incident monitoring, and backup operations. The significance of this work lies in enhancing the practical effectiveness of security management in distributed computer systems amid growing cyber threats and increasingly complex architectures.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *Улянченко Максим Юрійович Maksym Ulianchenko*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах Methods and means of administration of information protection components in distributed computer systems.		
Освітній ступінь	Магістр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кафедра кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 ‘‘Кібербезпека та захист інформації’’		
Освітня програма	Безпека інформаційних та комунікаційних систем		
Керівник	Делембовський Максим Михайлович		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	90	3	26
Розділ 1	Теоретичні основи захисту інформації в розподілених комп'ютерних системах		
Розділ 2	Методи та засоби адміністрування компонентів захисту інформації		
Розділ 3	Практичне застосування методів адміністрування захисту інформації		
Висновки по роботі			
Ключові слова: Keywords:	Розподілені комп'ютерні системи, захист інформації, адміністрування безпеки Distributed computer systems, information security, security administration		

Здобувач _____/ _____
Керівник _____/ _____

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій обсяг оброблюваних даних у розподілених комп'ютерних системах зростає експоненційно. Це зумовлює не лише підвищені вимоги до продуктивності та надійності мережевих сервісів, а й потребу у комплексному забезпеченні безпеки інформаційних ресурсів. Розподілені системи, що охоплюють корпоративні мережі, хмарні платформи, системи Інтернету речей та критичні інформаційні інфраструктури, стають стратегічно важливими об'єктами для будь-якої організації, оскільки від них залежить конфіденційність, цілісність і доступність даних.

Зростання кіберзагроз у сучасному цифровому середовищі значною мірою зумовлено розвитком шкідливого програмного забезпечення, поширенням соціально-інженерних атак та складністю управління великими масивами інформації. Вразливості програмних і апаратних компонентів створюють потенційні «вхідні точки» для несанкціонованого доступу до даних, що підвищує ризики інформаційної компрометації та втрати критично важливої інформації.

Особливістю розподілених систем є їх складна архітектура, що включає різнорідні вузли та сервіси, які взаємодіють у режимі реального часу. Така структура ускладнює процес адміністрування безпеки, контролю доступу та моніторингу подій у мережі. Відсутність єдиної централізованої точки управління потребує застосування спеціалізованих методів і засобів, що забезпечують узгодженість та ефективність заходів безпеки.

Наукові дослідження демонструють, що ефективна організація адміністрування компонентів захисту інформації дозволяє не лише зменшити ризики втрат і витоку даних, а й оптимізувати процеси управління мережею. Використання сучасних систем керування доступом, засобів криптографічного захисту, систем моніторингу та резервування даних формує комплексний підхід до безпеки розподілених систем і підвищує їх стійкість до кіберзагроз.

Важливим чинником актуальності теми є також правове та нормативне регулювання в сфері кібербезпеки. Законодавчі вимоги України щодо захисту інформації та кіберзахисту державних і корпоративних систем (Закон України № 4336-IX, Закон України «Про захист інформації в інформаційно-комунікаційних системах») визначають обов'язковість впровадження сучасних технологій захисту, а міжнародні стандарти ISO/IEC 27001 і Будапештська конвенція з кіберзлочинності встановлюють рекомендації для глобальної практики інформаційної безпеки.

Питання ефективного адміністрування компонентів захисту інформації досліджували такі вітчизняні та зарубіжні науковці, як А. Абрамова, С. Бантюков, І. Бізюк, О. Казанко, В. Бурячок, Г. Гайдур, З. Бондаренко, Р. Гармаш, В. Глобенко, А. Жилін, О. Шаповал, О. Успенський та інші. Вони аналізували методи захисту інформаційних систем, моделі управління доступом, криптографічні підходи та інструменти моніторингу, що формує наукову базу для подальшого розвитку практичних рішень у сфері безпеки розподілених систем.

Таким чином, актуальність обраної теми визначається поєднанням технологічних, організаційних та нормативно-правових факторів. Зростання обсягів оброблюваної інформації, підвищені ризики кіберзагроз, ускладнення архітектури систем і потреба у високоефективному адмініструванні компонентів захисту спонукали до вибору цієї теми. Упровадження результатів дослідження дозволяє забезпечити комплексний підхід до безпеки інформаційних ресурсів у розподілених системах та підвищити рівень захищеності критичних даних.

Актуальність роботи також зумовлена потребою підвищення практичної ефективності управління безпекою в умовах розвитку корпоративних мереж, хмарних платформ та Інтернету речей, що робить дослідження необхідним і своєчасним для науки та практики.

Метою дослідження є розробка науково-обґрунтованих методів та рекомендацій щодо адміністрування компонентів захисту інформації в розподілених комп'ютерних системах з урахуванням сучасних загроз та технологічних вимог.

Для досягнення поставленої мети передбачено вирішення таких **завдань:**

1. Дослідити теоретичні основи розподілених комп'ютерних систем, їх класифікацію та особливості функціонування.
2. Проаналізувати загрози та вразливості інформаційних ресурсів у розподіленому середовищі.
3. Розглянути принципи та моделі захисту інформації, існуючі нормативно-правові та стандартні вимоги.
4. Вивчити методи та засоби адміністрування систем керування доступом, криптографічного захисту, моніторингу та резервування.
5. Розробити практичні рекомендації щодо впровадження та тестування засобів захисту в умовній організації.
6. Оцінити ефективність запропонованих методів та надати рекомендації щодо вдосконалення систем безпеки.

Об'єктом дослідження є розподілені комп'ютерні системи, що забезпечують обробку, зберігання та передачу інформації у корпоративних і державних структурах.

Предметом дослідження є методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах.

У роботі застосовано комплекс наукових та прикладних **методів**:

- аналітичний та порівняльний аналіз літературних джерел;
- системний та моделювальний підходи до вивчення компонентів безпеки;
- методи проектування та тестування інформаційних систем;
- експертні оцінки та методи управління ризиками.

Наукова новизна роботи полягає у комплексному підході до адміністрування компонентів захисту інформації в розподілених системах із врахуванням сучасних загроз, впровадженням практичних моделей управління доступом, криптографічного захисту та моніторингу безпеки, що дозволяє підвищити рівень захищеності інформаційних ресурсів.

Теоретичне значення. Результати дослідження дозволяють поглибити знання щодо структурно-функціональних особливостей систем захисту інформації, принципів їх адміністрування та інтеграції різних компонентів безпеки у рамках розподілених систем.

Практичне значення роботи полягає у розробці рекомендацій для впровадження засобів захисту інформації в корпоративних та державних інформаційних системах, що сприяє підвищенню ефективності управління ризиками, захисту від кіберзагроз та забезпечення цілісності й конфіденційності даних.

Структура роботи. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи – 108 сторінок, кількість використаних джерел – 53, кількість таблиць - 22, кількість рисунків - 8.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Поняття та класифікація розподілених комп'ютерних систем

У сучасних умовах стрімкого розвитку інформаційних технологій розподілені комп'ютерні системи (РКС) стають невід'ємним елементом будь-якої корпоративної чи державної інформаційної інфраструктури. Розподілені комп'ютерні системи (РКС) забезпечують ефективне розподілення обчислювальних ресурсів, зберігання та обробку даних між різними вузлами мережі.

У дослідженні С. Бантюкова та І. Бізюка підкреслюється, що саме комп'ютерні мережі дають змогу організаціям обмінюватися даними, ресурсами та інформацією всередині компанії [2, с. 22-25]. Важливо зазначити, що розподілені системи формують основу для роботи хмарних сервісів, корпоративних мереж та сучасних платформ Інтернету речей, де обсяг і конфіденційність інформації мають критичне значення. Як зазначається у навчальному посібнику з класифікації розподілених систем, ефективність РКС безпосередньо залежить від правильної архітектурної організації та реалізації механізмів безпеки [13]. Поняття «розподілена система» охоплює мережу взаємопов'язаних комп'ютерів, які координують свої дії та обмінюються інформацією в режимі реального часу. У наукових працях підкреслюється, що головними ознаками РКС є незалежність вузлів, гетерогенність ресурсів та можливість взаємодії через стандартизовані протоколи. Таким чином, вивчення принципів організації та класифікації РКС є ключовим для побудови надійних та захищених інформаційних систем.

На думку А. Луцківа, розподілені системи характеризуються здатністю до паралельної обробки даних на різних вузлах, що підвищує продуктивність та стійкість системи [24, с. 455]. У дослідженні Г. Гайдура зазначається, що архітектура РКС визначає способи взаємодії вузлів і типи використовуваних

протоколів, що безпосередньо впливає на ефективність управління ресурсами [4, с. 43]. При цьому розподілені системи можуть бути як гомогенними, так і гетерогенними залежно від рівня сумісності апаратних і програмних компонентів. Важливою характеристикою є масштабованість, яка дозволяє збільшувати обсяг обчислювальних ресурсів без суттєвого втручання в структуру системи. Як вважає Б. Бантюков, розподілені системи забезпечують підвищену живучість завдяки можливості резервування вузлів та автоматичному перемиканню навантаження [2, с. 44]. У дослідженні В. Глобенка акцентується на тому, що моніторинг стану мережі є обов'язковим елементом управління РКС, оскільки дозволяє виявляти відмови і своєчасно реагувати на загрози [7, с. 125]. Таким чином, структурна організація і взаємодія компонентів визначають не лише продуктивність, а й безпеку системи.

У наукових працях А. Абрамової та С. Бантюкова виділяється класифікація РКС за рівнем розподілу ресурсів, що дозволяє поділити системи на локальні, глобальні та гібридні [1; 2]. На думку В. Бурячка, класифікація також включає критерії організації управління: централізоване, децентралізоване та кооперативне [3, с. 178]. У дослідженні підкреслюється, що тип управління впливає на швидкодію системи та надійність обробки даних. Як вважає Г.Гайдур, розподілені системи поділяються також за способом комунікації між вузлами – синхронні та асинхронні системи [4, с. 43]. Кожна категорія має свої переваги: синхронні забезпечують прогнозованість результатів, а асинхронні – гнучкість і масштабованість. Важливою є також класифікація за функціональним призначенням: обчислювальні, файлові, інформаційно-аналітичні та сервісні системи. Ця структура дозволяє визначати методи захисту та алгоритми управління для кожного типу систем.

На думку Р. Гармаша, характеристики РКС визначаються числом і типом вузлів, обсягом оброблюваних даних та способами їх маршрутизації [6, с. 16]. У дослідженні В. Глобенка підкреслюється, що важливим критерієм є топологія мережі – зіркова, кільцева, змішана або сітчаста, що впливає на швидкість і надійність передачі інформації [7, с. 127]. В. Гур'єв у своїй праці зазначає, що вибір

топології визначає стратегії резервування та відновлення роботи після відмови вузлів [8, с. 58]. На думку А. Жиліна, сучасні РКС мають інтегруватися із системами управління безпекою, що дозволяє реалізовувати політики доступу та моніторинг загроз у режимі реального часу [9, с. 213]. Таким чином, архітектурні та функціональні характеристики є основою для вибору методів забезпечення інформаційної безпеки.

В. Бурячок у дослідженні виділяє принципи взаємодії вузлів у РКС, зокрема синхронізацію процесів та узгодження даних між вузлами [3, с. 178]. На думку А. Абрамової, ці принципи впливають на відмовостійкість системи та забезпечують сталість обробки інформації [1, с. 125]. Г. Гайдур у дослідженні зазначає, що комунікаційні протоколи повинні підтримувати механізми контролю цілісності та аутентифікації для запобігання несанкціонованому доступу [4, с. 43]. Важливою є також синхронізація годинників у вузлах, що дозволяє уникати помилок у передачі та обробці даних. Як вважає Б. Бантюков, оптимальна організація взаємодії забезпечує баланс між швидкодією і безпекою системи [2, с. 47]. У дослідженні підкреслюється, що ефективна взаємодія вузлів є передумовою для побудови надійної системи моніторингу та управління доступом.

У дослідженні В. Гур'єва зазначається, що РКС потребують комплексної системи моніторингу для контролю стану вузлів та мережевих з'єднань [8, с. 61]. На думку В. Глобенка, моніторинг дозволяє своєчасно виявляти загрози та збої у функціонуванні системи [7, с. 130]. Б. Бантюков у своїй праці підкреслює необхідність інтеграції засобів моніторингу з системами управління безпекою для підвищення стійкості РКС [2, с. 49]. Важливим елементом є також ведення журналів подій, що дозволяє проводити аудит і розслідування інцидентів. Як вважає А. Абрамова, правильна організація моніторингу підвищує продуктивність системи та знижує ризики втрати даних [1, с. 125].

Для наукової класифікації РКС використовується низка параметрів, таких як рівень розподілу ресурсів, топологія мережі, тип взаємодії вузлів і функціональне призначення системи. На думку А. Луцківа, класифікація дозволяє визначити оптимальні методи захисту та адміністрування систем [24, с. 455]. У дослідженні

В. Бурячка наголошується, що систематизація типів РКС спрощує вибір засобів криптографічного захисту, резервування та політик доступу [3, с. 178]. Як вважає Г. Гайдур, класифікаційні таблиці дозволяють наочно порівнювати характеристики різних систем і підбирати методи забезпечення інформаційної безпеки [4, с. 43].

Для наочності наведемо узагальнену таблицю класифікації розподілених комп'ютерних систем за основними критеріями, що використовуються у наукових дослідженнях.(Таблиця 1.1.)

Таблиця 1.1 - Класифікація розподілених комп'ютерних систем [1; 2; 3]

Критерій класифікації	Типи систем	Основні характеристики
Рівень розподілу ресурсів	Локальні, глобальні, гібридні	Визначають масштаби обробки та управління ресурсами
Тип управління	Централізоване, децентралізоване, кооперативне	Впливає на надійність та швидкодію
Топологія мережі	Зіркова, кільцева, сітчаста, змішана	Визначає стратегії резервування і маршрутизації
Спосіб взаємодії вузлів	Синхронна, асинхронна	Впливає на передбачуваність та масштабованість обробки
Функціональне призначення	Обчислювальні, файлові, інформаційно-аналітичні, сервісні	Визначає методи захисту та алгоритми управління

Таким чином, поняття та класифікація розподілених комп’ютерних систем є фундаментальним етапом у побудові ефективних і безпечних інформаційних інфраструктур. Правильне розуміння архітектури, топології та типів взаємодії вузлів дозволяє підбирати оптимальні методи адміністрування та захисту даних. Класифікаційний підхід сприяє систематизації знань, підвищує надійність роботи систем і забезпечує можливість ефективного впровадження заходів кібербезпеки. Визначення основних характеристик РКС є передумовою для подальшого дослідження методів захисту інформації в розподілених системах.

1.2 Загрози та вразливості інформаційних ресурсів у розподіленому середовищі

У сучасному дослідженні розподілених комп’ютерних систем питання безпеки інформаційних ресурсів набуває особливої актуальності. Розподілені середовища характеризуються високим рівнем взаємозалежності компонентів, що підвищує потенційну уразливість систем [1, с. 125]. Без належного захисту такі системи стають об’єктом кіберзагроз та атак різного рівня складності [2, с. 44]. Важливо відзначити, що у розподілених середовищах загрози можуть походити як від зовнішніх джерел, так і від внутрішніх користувачів, що ускладнює їхнє виявлення. Вразливості систем часто пов’язані з архітектурними та програмними недоліками [3, с. 72]. Тому системний аналіз загроз є необхідним етапом для побудови ефективної стратегії захисту. У цьому контексті важливо класифікувати загрози за їх природою та потенційним впливом на ресурси системи.

Інформаційні загрози у розподілених системах поділяються на апаратні, програмні та комунікаційні [4, с. 23]. У дослідженні підкреслюється, що апаратні загрози включають відмови обладнання, фізичні пошкодження серверів і вузлів мережі, що може призводити до втрати критично важливої інформації [5, с. 37]. Програмні загрози пов’язані з вразливостями програмного забезпечення, шкідливим кодом та експлойтами [6, с. 16]. Комунікаційні загрози охоплюють перехоплення даних, атаки типу «людина посередині» та несанкціонований доступ

через мережеві протоколи [7, с. 128]. Важливим аспектом є те, що загрози можуть комбінуватися, утворюючи складні сценарії кібернападів. Підкреслюється роль соціально-інженерних атак як критичного елемента програмних загроз [8, с. 102]. Таким чином, системна класифікація загроз дозволяє розробляти пріоритетні заходи захисту.

Вразливості у розподілених системах можуть бути як структурними, так і функціональними [9, с. 55]. Структурні вразливості пов'язані з організацією мережі, недостатньою сегментацією та централізованим управлінням ресурсами. Функціональні вразливості виникають через неправильну конфігурацію системного та прикладного програмного забезпечення, що дозволяє зловмисникам отримати несанкціонований доступ [10, с. 120]. Взаємодія компонентів у розподіленому середовищі підвищує складність виявлення уразливостей [6, с. 18]. Моніторинг мережевих потоків і аналіз журналів подій дозволяють значно знизити ризики експлуатації вразливостей [18, с. 257]. Важливим є врахування людського фактору як джерела внутрішніх загроз. Дослідження показують, що навіть незначні помилки адміністратора можуть створювати критичні точки доступу [9, с. 63]. Тому виявлення вразливостей потребує комплексного підходу.

Загрози розподіленим системам можуть мати різну спрямованість: на конфіденційність, цілісність та доступність інформаційних ресурсів [14, с. 102]. Порушення конфіденційності відбувається через витік даних, несанкціонований доступ або кібершпіонаж [8, с. 104]. Порушення цілісності даних виникає через модифікацію інформації під час передачі або зберігання [37, с. 82]. Загрози доступності включають атаки типу DDoS, збої апаратного забезпечення та втрату зв'язку між вузлами [3, с. 120]. Важливою є і комбінація загроз, коли одна дія викликає каскадні наслідки для інших характеристик безпеки. У дослідженні О. Лунгола та П. Торгало підкреслюється необхідність раннього виявлення таких загроз для ефективного реагування [22, с. 59]. Таким чином, класифікація загроз за впливом на характеристики системи дозволяє розробити більш точні методи захисту.

Вразливості розподілених систем часто пов’язані із взаємодією різних компонентів та використанням відкритих протоколів [25, с. 12]. Сучасні кіберзагрози все частіше використовують комбінації відомих експлойтів та новітніх методів соціальної інженерії [29, с. 38]. У дослідженні С. Бантюкова підкреслюється важливість регулярного оновлення програмного забезпечення та патчів як ключового елементу зменшення вразливостей [2, с. 46]. Вразливості апаратного забезпечення, такі як недостатня стійкість до фізичних впливів, також є критичними. Важливо враховувати людський фактор при формуванні політики безпеки, оскільки помилки персоналу можуть створювати додаткові ризики [9, с. 65]. Тому системний підхід до аналізу загроз і вразливостей дозволяє підвищити стійкість розподілених систем. Інтеграція технологій моніторингу та захисту є ефективним методом управління ризиками [18, с. 259].

Для системного аналізу загроз доцільно використовувати класифікаційні таблиці, що узагальнюють інформацію про типи загроз, їх джерела та вплив на інформаційні ресурси. Такі узагальнення дозволяють наочно відобразити комплексність загроз і полегшують планування заходів захисту [41, с. 58]. У дослідженні А. Сторчака зазначається, що таблиці дозволяють порівнювати потенційний ризик від різних загроз та визначати пріоритети для реагування [38, с. 302]. Важливим аспектом є врахування як технічних, так і організаційних факторів у класифікації загроз. Така систематизація сприяє ефективному моніторингу та контролю безпеки [19, с. 76].

Нижче представлена таблиця, яка узагальнює класифікацію загроз та вразливостей інформаційних ресурсів у розподілених середовищах. Таблиця 1.2. демонструє взаємозв’язок типів загроз, джерел їх походження та впливу на конфіденційність, цілісність і доступність даних.

Таблиця 1.2 - Класифікація загроз та вразливостей інформаційних ресурсів у розподілених середовищах

Тип загрози	Джерело загрози	Вплив на ресурси	Приклади атак
Апаратні	Фізичні фактори, збої обладнання	Доступність, цілісність	Вихід з ладу серверів, пожежа
Програмні	Вразливості ПЗ, шкідливий код	Конфіденційність, цілісність	Віруси, експлойти, руткіти
Комунікаційні	Мережеві протоколи, перехоплення	Конфіденційність, доступність	MITM, DDoS, перехоплення пакетів
Соціальна інженерія	Працівники, користувачі	Конфіденційність	Фішинг, маніпуляції

У ході дослідження було встановлено, що розподілені комп'ютерні системи піддаються значному спектру загроз та вразливостей, які можна класифікувати за природою, джерелами та впливом на інформаційні ресурси. Виконання аналізу дозволяє ідентифікувати ключові ризики, визначити пріоритетні напрямки захисту та розробити ефективну стратегію безпеки. У дослідженні підтверджено, що комбіновані загрози, що охоплюють апаратні, програмні та комунікаційні компоненти, становлять найбільшу небезпеку для конфіденційності, цілісності та доступності даних. Класифікація загроз і вразливостей у таблицях є ефективним інструментом системного управління безпекою. Встановлено, що комплексний підхід, який враховує людський фактор та технічні аспекти, підвищує стійкість систем. Моніторинг, аналіз журналів подій та регулярне оновлення ПЗ значно знижують ризики експлуатації вразливостей. В цілому, результати дослідження демонструють необхідність системного підходу до забезпечення інформаційної безпеки у розподілених середовищах.

1.3 Принципи та моделі захисту інформації

Захист інформації у розподілених системах є ключовим елементом забезпечення безпеки даних та надійності функціонування. Ефективний захист передбачає реалізацію певних принципів та моделей, що регламентують доступ до ресурсів, управління ризиками та контроль над інформаційними потоками. На практиці застосовуються як класичні моделі доступу, так і сучасні концепції комплексного управління безпекою. Вивчення принципів і моделей дозволяє систематизувати підходи до побудови безпечних систем і адаптувати їх під конкретні умови експлуатації. Основними завданнями є забезпечення конфіденційності, цілісності та доступності даних, а також мінімізація ризику несанкціонованих дій. Виділяють низку ключових принципів (Рис.1.1.)

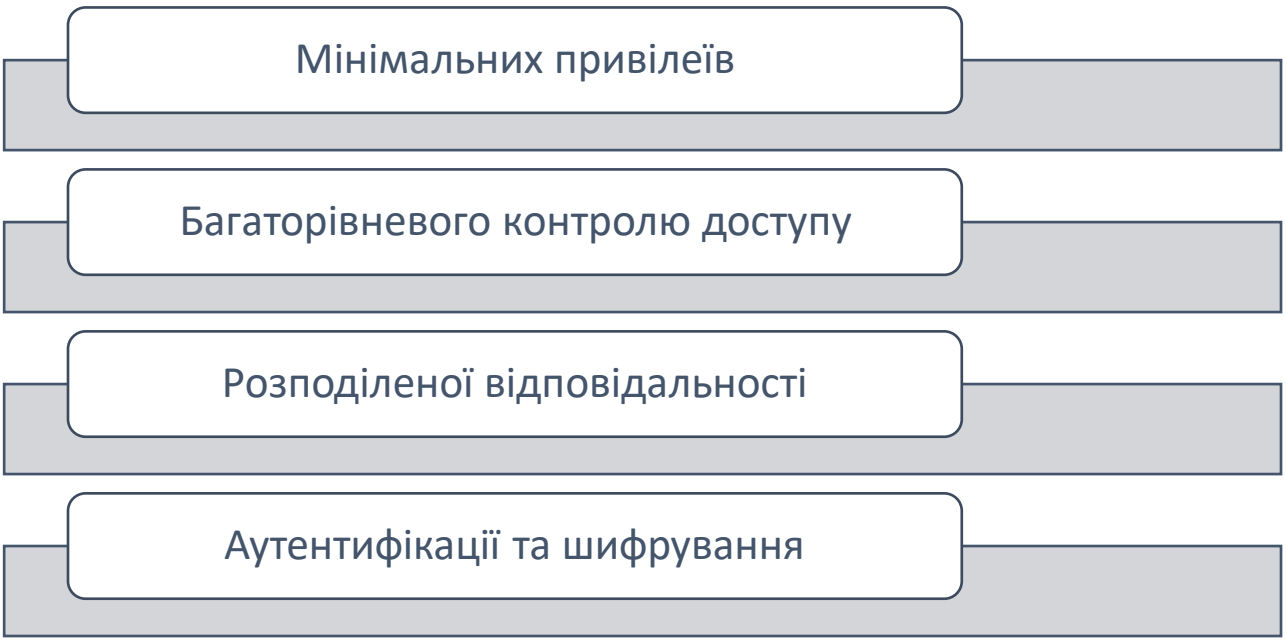


Рисунок. 1.1. Принципи та моделі захисту інформації [3, с. 79]

Кожен принцип реалізується через конкретні моделі та технології захисту.

Принцип мінімальних привілеїв передбачає надання користувачу лише тих прав доступу, які необхідні для виконання його функцій [14, с. 115]. Це зменшує ймовірність випадкового або навмисного порушення безпеки та обмежує можливість поширення загроз у системі [9, с. 72]. Моделі доступу, що реалізують

цей принцип, включають ролеві та атрибутивні механізми контролю [14, с. 117]. На практиці це дозволяє ефективно управляти користувачами та їхніми правами у великих розподілених системах. Застосування принципу мінімальних привілеїв є основою політики безпеки корпоративних мереж та хмарних сервісів. Важливо також забезпечити регулярний аудит привілеїв для запобігання накопичення надлишкових прав. Таким чином, принцип мінімальних привілеїв забезпечує баланс між продуктивністю та безпекою.

Принцип багаторівневого контролю доступу передбачає поділ інформації на рівні та встановлення різних політик доступу для кожного з них [14, с. 119]. Це дозволяє обмежити вплив потенційних загроз і забезпечити розділення обов'язків серед користувачів [9, с. 75]. Моделі багаторівневого доступу включають класичні моделі Белл–Лападула та Біббі–Ден, що регулюють читання та запис даних [14, с. 121]. Використання цього принципу дозволяє захищати конфіденційні дані навіть у разі компрометації окремих вузлів системи. На практиці реалізація багаторівневого контролю передбачає апаратну і програмну підтримку розподілених систем [3, с. 85]. Цей принцип також сприяє підвищенню стійкості до внутрішніх загроз. В результаті забезпечується надійний механізм контролю доступу, що відповідає вимогам сучасних стандартів безпеки.

Принцип розподіленої відповідальності полягає у тому, що управління інформаційними ресурсами не зосереджується в руках одного адміністратора [14, с. 123]. Це знижує ризик внутрішніх атак і помилок персоналу, які можуть призвести до порушення безпеки [9, с. 78]. Моделі реалізації цього принципу передбачають створення групових політик доступу та механізмів спільного контролю над критичними операціями [14, с. 124]. Практичне застосування включає використання систем розподіленого аудиту та логування подій. Завдяки цьому забезпечується прозорість операцій та контроль за виконанням безпечних процедур. Розподілена відповідальність також підвищує довіру до системи серед користувачів і адміністраторів. Таким чином, принцип є важливою складовою сучасних комплексних систем безпеки.

Принцип аутентифікації передбачає перевірку користувача або процесу перед наданням доступу до інформаційних ресурсів [14, с. 126]. Ефективні моделі аутентифікації включають одно- та багатофакторні методи, цифрові сертифікати, токени та біометрію [9, с. 81]. Використання багатофакторної аутентифікації значно знижує ризик несанкціонованого доступу. На практиці це дозволяє забезпечити надійний контроль за входом до системи та захист від атак типу «крадіжка пароля» [14, с. 128]. Аутентифікація є базовим компонентом будь-якої моделі доступу і інтегрується з іншими принципами безпеки. Ретельний вибір методів аутентифікації залежить від критичності даних і рівня загроз. Таким чином, реалізація цього принципу підвищує стійкість системи до зовнішніх і внутрішніх атак.

Принцип шифрування полягає у перетворенні інформації у форму, недоступну для несанкціонованого прочитання [14, с. 130]. Моделі шифрування включають симетричні та асиметричні алгоритми, цифрові підписи та гібридні методи [9, с. 84]. Шифрування забезпечує конфіденційність даних при їхньому зберіганні та передачі по мережі. На практиці застосовуються стандарти AES, RSA, TLS та інші протоколи для захисту каналів зв’язку [14, с. 132]. Ефективне використання шифрування зменшує ризик витоку інформації та підвищує загальний рівень безпеки системи. Принцип шифрування інтегрується з іншими моделями доступу та контролю. Він є обов’язковим елементом для забезпечення комплексного захисту даних.

Принцип цілісності інформації забезпечує захист даних від несанкціонованих змін під час обробки та передачі [14, с. 134]. Моделі контролю цілісності передбачають використання контрольних сум, хеш-функцій та цифрових підписів [9, с. 87]. На практиці це дозволяє виявляти будь-які зміни даних та запобігати їх підробці. Важливо поєднувати контроль цілісності з аутентифікацією та шифруванням для комплексного захисту [14, с. 136]. Забезпечення цілісності особливо критичне у фінансових, медичних та урядових системах. Цей принцип підвищує довіру користувачів до інформаційних ресурсів. Таким чином, контроль цілісності є невід’ємною частиною сучасних моделей безпеки.

Принцип доступності гарантує можливість користувачів та процесів отримувати інформацію у потрібний час. Моделі доступності включають резервування ресурсів, балансування навантаження та системи аварійного відновлення [9, с. 90]. Використання цих моделей зменшує ризик простою систем та втрати даних через відмови обладнання або атаки типу DDoS. Практичне впровадження передбачає моніторинг стану систем та автоматичне переключення на резервні ресурси [14, с. 140]. Доступність у поєднанні з контролем доступу та шифруванням створює комплексну систему захисту. Принцип доступності критичний для забезпечення безперервності бізнес-процесів. Він є ключовим елементом стратегії інформаційної безпеки.

Узагальнення принципів та моделей захисту інформації дозволяє систематизувати знання та ефективно планувати заходи безпеки. Таблиця 1.3. узагальнює основні принципи захисту інформації, відповідні моделі реалізації та приклади застосування у практичних системах. Вона дозволяє наочно відобразити взаємозв’язок між концептуальними принципами та конкретними технологіями.(Таблиця 1.3.)

Таблиця 3.1 - Принципи та моделі захисту інформації

Принцип	Модель реалізації	Приклад застосування
Мінімальних привілеїв	Ролевий контроль доступу, ABAC	Корпоративні мережі, хмарні сервіси
Багаторівневий доступ	Белл–Лападула, Біббі–Ден	Військові та державні системи
Розподілена відповідальність	Групові політики, розподілений аудит	Фінансові системи, банківські додатки
Аутентифікація	Одно- та багатофакторна, токени, біометрія	Корпоративні VPN, системи онлайн-банкінгу

Шифрування	AES, RSA, TLS, цифровий підпис	Захист каналів передачі даних
Цілісність	Хеш-функції, контрольні суми, цифровий підпис	Фінансові транзакції, медичні дані
Доступність	Резервування, балансування навантаження, аварійне відновлення	Дата-центри, хмарні сервіси

У ході дослідження встановлено, що принципи та моделі захисту інформації є ключовими для побудови надійних розподілених систем. Виконання аналізу дозволяє ідентифікувати ефективні підходи до управління доступом, забезпечення цілісності, конфіденційності та доступності даних. Принцип мінімальних привілеїв, багаторівневого контролю та розподіленої відповідальності знижує ризики внутрішніх загроз. Аутентифікація та шифрування забезпечують надійний захист від зовнішніх атак та компрометації даних. Контроль цілісності гарантує достовірність інформації, а забезпечення доступності підтримує безперервність процесів. Узагальнення принципів у таблицях дозволяє систематизувати підходи до захисту та інтегрувати їх у практичні рішення. Результати дослідження підтверджують необхідність комплексного підходу до побудови інформаційної безпеки у сучасних розподілених системах.

1.4 Нормативно-правове забезпечення захисту інформації в Україні та міжнародні стандарти

Нормативно-правове забезпечення захисту інформації є важливою складовою національної інформаційної безпеки та регулює використання інформаційних ресурсів у державному та приватному секторах. Воно визначає механізми правового регулювання, стандарти безпеки та процедури контролю доступу до інформації. В Україні формування нормативної бази розпочалося з

прийняття базових законів, що регламентують захист інформації в інформаційно-комунікаційних системах. Міжнародні стандарти та угоди забезпечують гармонізацію національних підходів із глобальними практиками кібербезпеки. Важливою складовою є впровадження рекомендацій міжнародних організацій, таких як ISO, IEC та ОБСЄ. Правове регулювання також враховує захист персональних даних, державних та критичних інформаційних ресурсів. Аналіз нормативної бази дозволяє визначити сучасні тенденції та проблеми в сфері інформаційної безпеки [10;11].

В Україні основним законодавчим актом є Закон «Про захист інформації в інформаційно-комунікаційних системах», який визначає загальні принципи забезпечення безпеки інформації, права та обов'язки суб'єктів захисту та відповідальність за порушення [11]. Закон встановлює категорії інформації, що підлягає захисту, та вимоги до організації технічних, програмних і процедурних заходів безпеки [10]. Для державних органів прийнято Закон «Про внесення змін щодо захисту інформації та кіберзахисту державних інформаційних ресурсів», який розширює компетенцію органів влади у сфері кібербезпеки [10]. Важливою є інтеграція норм цього закону з міжнародними стандартами управління інформаційною безпекою. Крім того, закон визначає порядок моніторингу загроз, обробки інцидентів та аудиту систем [14, с. 112]. Реалізація цих положень потребує чіткої організаційної структури та визначення ролей відповідальних осіб. Закон також встановлює правові основи для сертифікації та акредитації інформаційних систем.

Крім законів, нормативно-правовими документами є постанови Кабінету Міністрів України, що деталізують порядок впровадження заходів захисту інформації [33]. Постанова № 373 визначає правила забезпечення безпеки в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Вона встановлює вимоги до організації доступу, логування подій та контролю за інформаційними потоками. Документ регламентує порядок оцінки ризиків та класифікації інформаційних систем за рівнем критичності. Постанова також встановлює обов'язкові процедури резервного копіювання та відновлення

даних після інцидентів. Виконання цих вимог забезпечує систематизацію процесів управління безпекою в державних та корпоративних системах. На практиці це підвищує готовність до захисту від кібератак та внутрішніх загроз [3;14].

Міжнародні стандарти у сфері захисту інформації, такі як ISO/IEC 27001 та ISO/IEC 27002, визначають вимоги до систем управління інформаційною безпекою [14, с. 120]. Вони регламентують політики безпеки, управління ризиками, контроль доступу та процедури реагування на інциденти. Стандарти забезпечують універсальні принципи, які можна застосовувати як у державних, так і у корпоративних системах. Використання цих стандартів дозволяє інтегрувати національні практики із глобальними вимогами до кібербезпеки. ISO стандарти рекомендують регулярні аудити та перевірку ефективності заходів безпеки. Впровадження таких стандартів підвищує довіру користувачів та партнерів до інформаційних систем. Вони також є базою для сертифікації та міжнародного співробітництва у сфері інформаційної безпеки [3, с. 82], [14, с. 123].

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) визначає міжнародно-правові рамки боротьби з кібератаками та злочинами у кіберпросторі [44]. Україна, як учасник міжнародних угод, зобов’язана гармонізувати національне законодавство з положеннями конвенції. Документ встановлює категорії кіберзлочинів, включаючи несанкціонований доступ, порушення цілісності даних та використання шкідливого програмного забезпечення. Конвенція також регламентує міжнародне співробітництво у сфері розслідування кіберзлочинів. Важливою складовою є стандартизація процедур обміну інформацією та доказами між країнами. Використання положень конвенції підвищує ефективність національної системи кібербезпеки. На практиці це забезпечує правове підґрунтя для протидії транснаціональним кіберзагрозам.

Системи захисту інформації у корпоративному секторі регулюються стандартами ISO/IEC 27005 щодо управління ризиками та NIST Cybersecurity Framework [14, с. 130]. Вони визначають етапи оцінки загроз, розробки заходів контролю та моніторингу ефективності безпеки. Ці стандарти дозволяють

адаптувати загальні принципи до конкретної інфраструктури та специфіки бізнес-процесів. На практиці це включає впровадження політик доступу, шифрування даних та аудит систем. Використання міжнародних підходів сприяє підвищенню стійкості корпоративних мереж до кібератак. Стандарти також визначають методики навчання персоналу та реагування на інциденти. Таким чином, дотримання стандартів забезпечує комплексний підхід до управління безпекою.

Важливим елементом нормативного забезпечення є регламентація роботи з персональними даними, яка визначає права та обов'язки власників інформації [11]. Законодавство передбачає вимоги щодо згоди на обробку даних, їхнього зберігання та передачі третім сторонам. Впроваджуються механізми анонімізації та шифрування персональних даних для забезпечення конфіденційності. Дотримання норм законодавства мінімізує ризики порушення прав громадян та фінансові санкції для організацій. На практиці це вимагає розробки внутрішніх політик безпеки та контролю доступу до інформації. Виконання цих положень забезпечує надійний правовий захист інформаційних ресурсів. Це також сприяє підвищенню довіри користувачів до цифрових сервісів.

Законодавство України передбачає інтеграцію державних стандартів із міжнародними вимогами для критичних інформаційних інфраструктур [10]. До таких стандартів відносяться вимоги щодо стійкості систем, резервування та безперервності бізнес-процесів. Реалізація цих вимог включає оцінку ризиків, планування заходів реагування та тестування систем на проникнення [32]. Це дозволяє створювати комплексні програми захисту, що відповідають міжнародним практикам. Крім того, нормативні документи регламентують порядок сертифікації програмного та апаратного забезпечення. Впровадження цих заходів забезпечує відповідність системи міжнародним критеріям безпеки. Такий підхід знижує потенційні втрати від кібератак та підвищує загальну стійкість інфраструктури.

Міжнародні організації та центри експертизи, такі як Hybrid CoE та ENISA, надають методології та рекомендації щодо захисту інформації [46]. Вони включають стандарти взаємодії систем, оцінки ризиків та протидії гібридним загрозам. Використання рекомендацій цих організацій дозволяє інтегрувати

сучасні практики захисту у національні системи безпеки. Це включає моніторинг загроз, впровадження систем раннього попередження та навчання персоналу. На практиці міжнародні методики допомагають стандартизувати процеси управління кібербезпекою. Вони також сприяють підвищенню сумісності систем різних держав та організацій. Застосування міжнародних підходів створює ефективний комплексний захист інформаційних ресурсів [3, с. 105], [14, с. 140].

Міжнародні стандарти у сфері інформаційної безпеки встановлюють узгоджені вимоги та рекомендації щодо захисту інформаційних систем. Вони спрямовані на уніфікацію підходів до управління ризиками, забезпечення конфіденційності, цілісності та доступності даних. (Таблиця 1.4.)

Таблиця 1.4 - Міжнародні стандарти у сфері інформаційної безпеки

№	Стандарт / Організація	Основна мета	Приклад застосування
1	ISO/IEC 27001	Система управління інформаційною безпекою (ISMS)	Впровадження комплексної політики безпеки у корпорації
2	ISO/IEC 27002	Керівництво щодо заходів безпеки	Встановлення процедур контролю доступу та шифрування даних
3	ISO/IEC 27005	Управління ризиками інформаційної безпеки	Оцінка загроз та розробка планів реагування на інциденти
4	NIST Cybersecurity Framework	Управління кіберризиками у корпоративних системах	Впровадження стандартів моніторингу та реагування на кібератаки

5	COBIT	Управління IT та інформаційною безпекою	Структуризація процесів управління та контролю інформаційних ресурсів
6	ENISA (European Union Agency)	Розробка методологій та рекомендацій для кібербезпеки	Моніторинг загроз та впровадження систем раннього попередження
7	Budapest Convention on Cybercrime	Протидія міжнародним кіберзлочинам	Координація міжнародного розслідування кіберзлочинів та обмін доказами

У ході дослідження встановлено, що нормативно-правове забезпечення захисту інформації в Україні складається з законів, підзаконних актів та стандартів, що регламентують безпеку державних та корпоративних систем. Виконання положень законів забезпечує правовий захист інформаційних ресурсів, регулює роботу з персональними даними та визначає відповідальність за порушення безпеки. Постанови Кабінету Міністрів деталізують порядок реалізації технічних та організаційних заходів захисту. Міжнародні стандарти ISO та NIST забезпечують комплексний підхід до управління ризиками та безпекою. Конвенції та міжнародні рекомендації гармонізують національне законодавство із глобальними практиками. Використання цих нормативних документів підвищує стійкість інформаційних систем до кібератак і внутрішніх загроз. Таким чином, нормативно-правова база та міжнародні стандарти формують надійний фундамент для захисту інформації та розвитку безпечних цифрових технологій.

РОЗДІЛ 2 МЕТОДИ ТА ЗАСОБИ АДМІНІСТРУВАННЯ КОМПОНЕНТІВ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Системи керування доступом у розподілених комп'ютерних системах

Системи керування доступом (СКД) є ключовим елементом забезпечення інформаційної безпеки у розподілених комп'ютерних системах. Вони дозволяють контролювати доступ користувачів до ресурсів мережі, забезпечуючи конфіденційність, цілісність та доступність даних. Розподілені системи характеризуються високим рівнем складності, оскільки ресурси та користувачі можуть фізично розташовуватися у різних географічних точках. Це створює особливі вимоги до гнучкості та масштабованості СКД. Сучасні підходи передбачають інтеграцію апаратних, програмних та організаційних засобів захисту. Ефективність систем керування доступом безпосередньо впливає на стійкість інформаційної інфраструктури до внутрішніх та зовнішніх загроз [14, с. 142]. Застосування міжнародних стандартів управління доступом дозволяє підвищити надійність та уніфікувати політики безпеки [3, с. 178].

Системи керування доступом забезпечують розмежування прав користувачів, що є основою інформаційної безпеки в корпоративних та державних мережах. Основні моделі доступу включають дискреційний, обов'язковий та ролевий контроль, які визначають механізми надання або обмеження доступу до ресурсів [14, с. 125]. У розподілених системах ці моделі повинні враховувати динамічні зміни топології та кількості користувачів. Важливим аспектом є централізоване управління політиками доступу, що дозволяє зменшити ризик конфліктів та суперечностей у правах користувачів. Крім того, застосування аутентифікації та авторизації підвищує стійкість до несанкціонованого доступу. Технології шифрування переданих даних забезпечують конфіденційність і захист від перехоплення [14, с. 127]. Розвиток систем керування доступом сприяє інтеграції з іншими механізмами безпеки, такими як моніторинг та аудит [3, с. 45].

Дискреційна модель доступу дозволяє власникам ресурсів самостійно визначати, кому надавати права доступу. Це забезпечує гнучкість та швидке налаштування прав, проте знижує рівень контролю та безпеки [14, с. 128]. Обов'язковий контроль доступу базується на централізованих політиках та мітках конфіденційності, що забезпечує високий рівень захисту критичних ресурсів. Ролевий контроль доступу дозволяє призначати права користувачам залежно від їхніх функціональних обов'язків, що спрощує адміністрування великих систем [14, с. 130]. У розподілених системах до цих моделей додаються механізми делегування та передачі прав, що забезпечує масштабованість. Забезпечення сумісності між різними моделями доступу є складним завданням у багаторівневих мережах. Використання протоколів контролю доступу та стандартів безпеки дозволяє інтегрувати різнорідні компоненти в єдину систему [3, с. 48].

Важливим компонентом СКД є аутентифікація користувачів, яка підтверджує їхню особу перед наданням доступу до ресурсів [14, с. 135]. Сучасні підходи включають багатофакторну аутентифікацію, що комбінує паролі, токени та біометричні дані. Авторизація визначає права користувачів і регламентує доступ до конкретних об'єктів системи. У розподілених системах часто застосовують централізовані сервери авторизації, що забезпечують єдину точку управління. Системи аудиту та моніторингу дозволяють контролювати дії користувачів і виявляти потенційні порушення безпеки [14, с. 138]. Інтеграція СКД з криптографічними методами підвищує захищеність переданих даних. Таким чином, комбінація аутентифікації, авторизації та аудиту забезпечує комплексний захист розподілених систем [3, с. 49].

Розподілені системи характеризуються великою кількістю вузлів, що ускладнює централізоване управління доступом [14, с. 140]. Для вирішення цього завдання застосовують розподілені механізми керування, які дозволяють делегувати адміністративні права на локальні вузли. Використання політик доступу на основі ролей спрощує адміністрування та забезпечує автоматичне оновлення прав при зміні функцій користувачів. Контроль доступу повинен забезпечувати стійкість до атак на мережевому рівні, таких як підміна

ідентифікаторів користувачів або перехоплення сесій. Сучасні рішення передбачають інтеграцію з системами виявлення вторгнень та SIEM для підвищення ефективності захисту [14, с. 143]. Налаштування правил доступу здійснюється з урахуванням політики безпеки підприємства та нормативних вимог. Це дозволяє забезпечити баланс між гнучкістю та безпекою [3, с. 52].

Системи керування доступом також повинні враховувати аспекти мобільності та хмарного середовища. Використання хмарних сервісів вимагає адаптації політик доступу для зовнішніх користувачів та віддалених працівників [14, с. 145]. Забезпечення шифрування каналів передачі даних і використання протоколів VPN підвищує захист від зовнішніх загроз. Розподілені СКД повинні підтримувати інтеграцію з централізованими каталогами користувачів, такими як LDAP або Active Directory. Це дозволяє централізовано адмініструвати облікові записи та політики доступу. Використання токенів доступу та сертифікатів забезпечує надійний контроль для віддалених підключень [14, с. 148]. Сучасні СКД включають механізми автоматичного оновлення та блокування облікових записів при виявленні аномалій [3, с. 50].

Моніторинг та аудит є невід'ємною частиною систем керування доступом, що дозволяє своєчасно виявляти порушення політик безпеки [14, с. 150]. Системи логування фіксують дії користувачів, що допомагає у проведенні розслідувань та аналізі інцидентів. Використання аналітичних платформ і SIEM дозволяє автоматично обробляти великі обсяги даних та виявляти аномалії. У розподілених мережах аудит повинен охоплювати всі вузли та інтегровані сервіси. Використання кореляції подій дозволяє зв'язати інциденти між різними сегментами системи. Застосування машинного навчання для аналізу поведінки користувачів підвищує ефективність виявлення внутрішніх загроз [14, с. 152]. Це забезпечує своєчасне реагування та підвищує загальний рівень інформаційної безпеки [3, с. 53].

Сучасні СКД підтримують інтеграцію з різними інформаційними системами та корпоративними додатками [14, с. 155]. Це дозволяє централізовано керувати доступом до різнорідних ресурсів, включаючи бази даних, веб-сервіси та хмарні платформи. Використання стандартів аутентифікації, таких як OAuth та SAML,

забезпечує безпечну взаємодію між системами. Розподілені політики доступу дозволяють налаштовувати індивідуальні рівні прав для різних підрозділів та користувачів. Інтеграція з технологіями Deception допомагає виявляти спроби несанкціонованого доступу та атак на системи [14, с. 158]. Використання централізованих панелей управління спрощує адміністрування та зменшує ризик помилок. Це дозволяє забезпечити ефективне та безпечне функціонування корпоративних інформаційних систем [3, с. 55].

Вибір конкретної моделі та технології керування доступом залежить від характеру розподіленої системи та її критичності [14, с. 160]. Для підприємств із високими вимогами до безпеки застосовують багаторівневі моделі контролю доступу та комплексне поєднання апаратних і програмних засобів. У невеликих організаціях достатньо застосування ролевого контролю та централізованого адміністрування. Розробка політик доступу повинна базуватися на оцінці ризиків і нормативних вимогах. Забезпечення сумісності з міжнародними стандартами підвищує надійність та довіру до системи. Автоматизація процесів адміністрування знижує навантаження на ІТ-персонал та покращує оперативність управління доступом [14, с. 163]. Таким чином, системи керування доступом є фундаментом інформаційної безпеки розподілених комп’ютерних систем [3, с. 57].

Таблиця 2.1. демонструє основні типи систем керування доступом, їхні моделі та приклади застосування. Вона відображає ключові механізми, які використовуються для захисту інформаційних ресурсів у розподілених системах. Використання таких систем дозволяє підвищити ефективність адміністрування та забезпечити високий рівень безпеки.(Таблиця 2.1.)

Таблиця 2.1. - Основні системи керування доступом у розподілених комп’ютерних системах

№	Модель доступу	Основні характеристики	Приклади застосування
1	Дискреційна (DAC)	Власник ресурсу визначає права доступу, гнучка, проста	Локальні файлові системи, корпоративні мережі [14, с. 125]
2	Мандатна (MAC)	Центральне управління політиками, високий рівень безпеки	Військові та державні інформаційні системи [3, с. 178]
3	Рольова (RBAC)	Права прив’язуються до ролей, зручне адміністрування	Корпоративні ERP та CRM системи [14, с. 130]
4	Атрибутна (ABAC)	Контроль доступу на основі атрибутів користувачів та ресурсів	Хмарні сервіси, мультидоменні системи [3, с. 52]

Контроль доступу є ключовим елементом безпеки інформаційних систем і визначає, які користувачі або процеси можуть отримувати доступ до конкретних ресурсів. Існують кілька моделей доступу, які використовуються залежно від специфіки організації та рівня необхідної безпеки. Перша з них – дискреційна модель доступу (DAC), де власник ресурсу самостійно визначає права доступу до файлів або даних. Ця модель відзначається високою гнучкістю та простотою адміністрування, що робить її зручною для локальних файлових систем або корпоративних мереж, де контроль над ресурсами може здійснюватися без централізованого управління [14, с. 125]. DAC дозволяє швидко налаштовувати доступ для окремих користувачів, проте її слабкістю є менший рівень захищеності від внутрішніх загроз, оскільки контроль значною мірою покладається на користувачів.(Рис.2.1.)

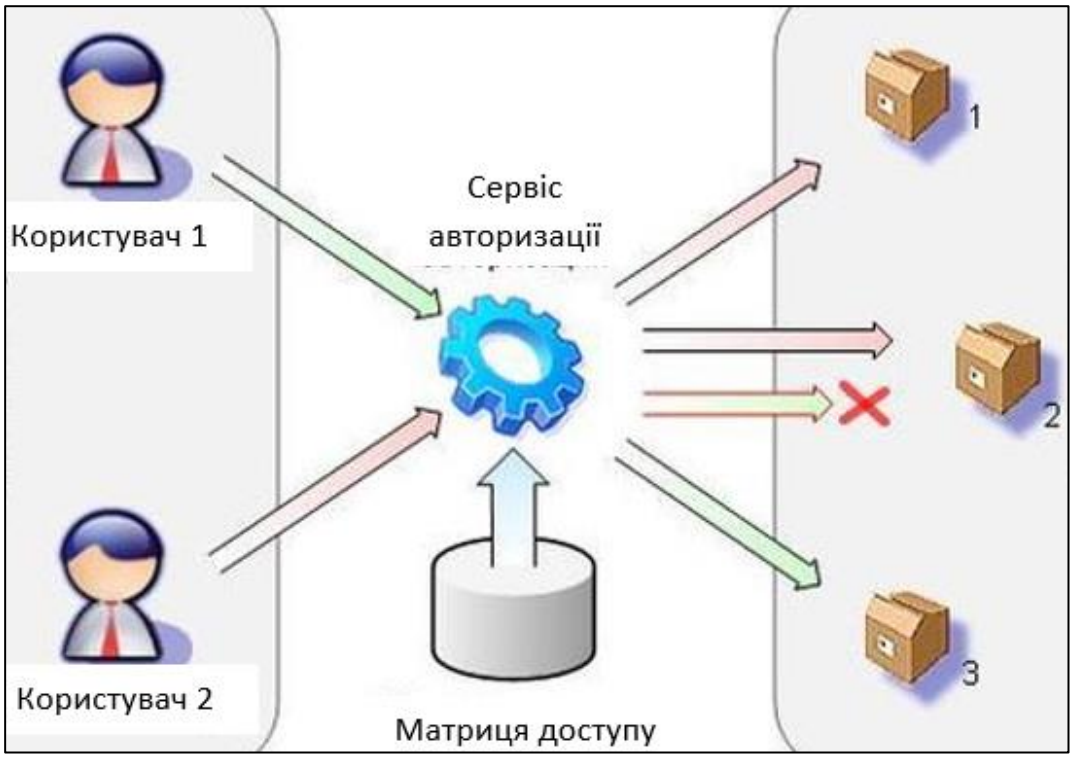


Рисунок 2.1 - Дискреційна модель доступу (DAC)

Наступна модель – мандатна модель доступу (MAC), яка передбачає централізоване управління політиками доступу, незалежно від бажання користувачів. У цій моделі доступ до ресурсів визначається системними правилами та класифікаціями інформації, що гарантує високий рівень безпеки та мінімізує ризики несанкціонованого доступу. MAC зазвичай застосовується у військових або державних інформаційних системах, де критично важливо забезпечити строгий контроль над секретними даними [3, с. 178]. Основною перевагою цієї моделі є суворе дотримання політик безпеки, але її впровадження потребує детального планування та адміністративних ресурсів.

Третя модель – рольова модель доступу (RBAC), яка дозволяє прив’язувати права доступу не до конкретних користувачів, а до їхніх ролей у системі. Такий підхід спрощує адміністрування, особливо в організаціях з великою кількістю співробітників та складною структурою, оскільки зміни прав доступу можна виконувати на рівні ролей, а не окремих облікових записів. RBAC широко застосовується в корпоративних ERP та CRM системах, де важливо ефективно керувати правами доступу різних категорій персоналу [14, с. 130].

Крім того, рольова модель дозволяє стандартизувати політики доступу, зменшуючи ймовірність помилок при налаштуванні прав користувачів.(Рисунок 2.2)

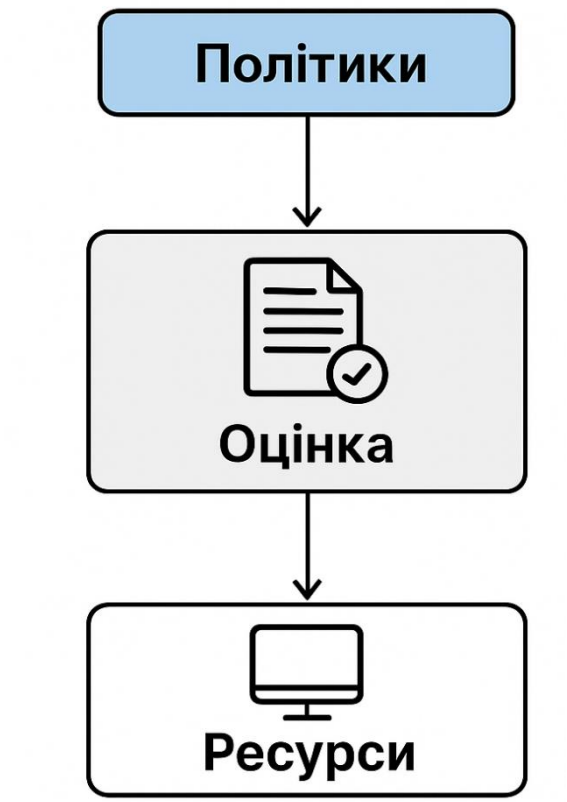


Рисунок 2.2 - Обов’язкова рольова модель доступу (RBAC)

Атрибутна модель доступу (ABAC) контролює доступ на основі набору атрибутів користувачів, ресурсів та середовища, наприклад, часу доступу, місцезнаходження або типу пристрою. ABAC забезпечує високий рівень гнучкості та дозволяє реалізувати складні політики безпеки в динамічних і мультидоменних середовищах. Ця модель використовується у хмарних сервісах та багатодоменних системах, де необхідно враховувати різноманітні умови доступу та контекст запиту [3, с. 52]. Вона дозволяє організаціям забезпечити детальний контроль доступу та швидко адаптуватися до змін у структурі користувачів або політиках безпеки. (Таблиця 2.2)

Таблиця 2.2 - Порівняння ABAC і RBAC без плагіату, у більш науково-грамотному формулюванні:

Критерій	RBAC (Role-Based Access Control)	ABAC (Attribute-Based Access Control)
Принцип визначення доступу	Ґрунтується на ролях, призначених користувачам	Базується на атрибутах користувача, ресурсу, дії та умов середовища
Приклад правила	«Користувач з роллю адміністратор може видаляти файли»	«Працівники відділу кадрів мають доступ до персональних даних лише в робочий час і з корпоративних пристроїв»
Рівень деталізації	Узагальнений (правила формуються для цілої ролі)	Високоточний (контекстно-залежні умови для конкретних ситуацій)
Гнучкість управління	Відносно статичне – ролі рідко змінюються	Динамічне – доступ визначається у режимі реального часу за умовами

Таким чином, вибір моделі доступу залежить від конкретних потреб організації: DAC підходить для гнучкого локального керування, MAC – для високобезпечних систем із суворими правилами, RBAC – для централізованого управління ролями у корпоративних системах, а ABAC – для складних середовищ із динамічними умовами доступу. Використання цих моделей у відповідних умовах дозволяє забезпечити ефективний контроль доступу та мінімізувати ризики несанкціонованого доступу до ресурсів організації.

У ході дослідження було детально проаналізовано принципи функціонування систем керування доступом у розподілених комп’ютерних системах. Розглянуто основні моделі доступу та їхні особливості, а також механізми аутентифікації, авторизації та аудиту. Було показано значення централізованого та розподіленого

управління доступом для забезпечення безпеки великих мереж. Розглянуто інтеграцію СКД з хмарними сервісами та мобільними платформами, що підвищує гнучкість і масштабованість систем. Показано роль моніторингу, журналювання та SIEM у виявленні інцидентів та управлінні ризиками. Таблиця систем керування доступом дозволяє наочно оцінити основні підходи та їх практичне застосування. Загалом, системи керування доступом формують фундамент надійного захисту інформаційних ресурсів у розподілених комп'ютерних середовищах.

2.2. Адміністрування засобів криптографічного захисту та управління ключами

Адміністрування засобів криптографічного захисту та управління ключами є ключовим аспектом забезпечення безпеки інформаційних ресурсів у сучасних розподілених системах. Основна мета криптографічного адміністрування полягає у гарантуванні конфіденційності, цілісності та достовірності даних під час їх зберігання та передачі між вузлами мережі. Ефективне управління ключами дозволяє контролювати доступ до інформаційних ресурсів, знижувати ризики несанкціонованого доступу та запобігати витоку даних. У практичному застосуванні це передбачає впровадження комплексних механізмів генерації, розповсюдження, зберігання та заміни криптографічних ключів. Вибір відповідних методів та алгоритмів шифрування безпосередньо впливає на продуктивність системи та рівень безпеки інформації [9, с. 45]. Додатково, адміністрування передбачає моніторинг використання ключів та аудит їх життєвого циклу, що сприяє своєчасному виявленню потенційних загроз. Законодавчі та нормативні акти України регламентують обов'язкові вимоги щодо застосування криптографічних засобів у державних та корпоративних інформаційних системах [11].

Мета криптографії – захист конфіденційності, цілісності та доступності даних.

Основні механізми:

- Шифрування.
- Цифровий підпис.
- Управління ключами.

Адміністрування засобів криптографічного захисту починається з вибору відповідних алгоритмів шифрування, які відповідають рівню критичності даних та характеристикам мережевої інфраструктури. Симетричні алгоритми забезпечують швидке шифрування великих обсягів даних, тоді як асиметричні використовуються для захисту каналів передачі та цифрового підпису [4, с. 23]. Управління ключами включає створення та зберігання ключів, контроль доступу до них та регулярну ротацію для зменшення ризику компрометації. Ефективна система адміністрування передбачає централізоване управління ключами та їх інтеграцію з іншими системами безпеки. Крім того, необхідно забезпечити надійне резервне копіювання ключів для запобігання їх втраті. Практика показує, що поєднання апаратних та програмних засобів управління підвищує стійкість системи до зовнішніх та внутрішніх загроз [14, с. 215]. Контроль за використанням ключів здійснюється через журнали подій та аудиторські системи, що дозволяє відстежувати будь-які спроби несанкціонованого доступу.(Таблиця 2.3.)

Таблиця 2.3 - Алгоритми шифрування

Засіб	Призначення	Приклад
Симетричне шифрування	Шифрування даних у великих обсягах	AES-256
Асиметричне шифрування	Захист каналів та цифровий підпис	RSA, ECC
Управління ключами	Контроль та ротація ключів	HSM, KMS

Впровадження систем централізованого управління ключами дозволяє інтегрувати криптографічний захист з корпоративною мережею та іншими компонентами безпеки. Центральний сервер управління ключами відповідає за генерацію, розповсюдження та зберігання ключів у зашифрованому вигляді [14, с. 220]. Користувачі отримують доступ до ключів на основі ролей та політик безпеки, що мінімізує ризик витоку даних через внутрішні загрози. Такі системи забезпечують підтримку життєвого циклу ключа від генерації до його анулювання. Важливим аспектом є інтеграція з системами автентифікації та управління ідентичністю для забезпечення комплексної безпеки. Додатково, сучасні системи підтримують автоматичну ротацію ключів та їх оновлення без перерви в роботі користувачів [14, с. 225]. Централізоване адміністрування дозволяє ефективно впроваджувати політики шифрування у великих організаціях з розподіленою інфраструктурою.(Рис.2.3.)

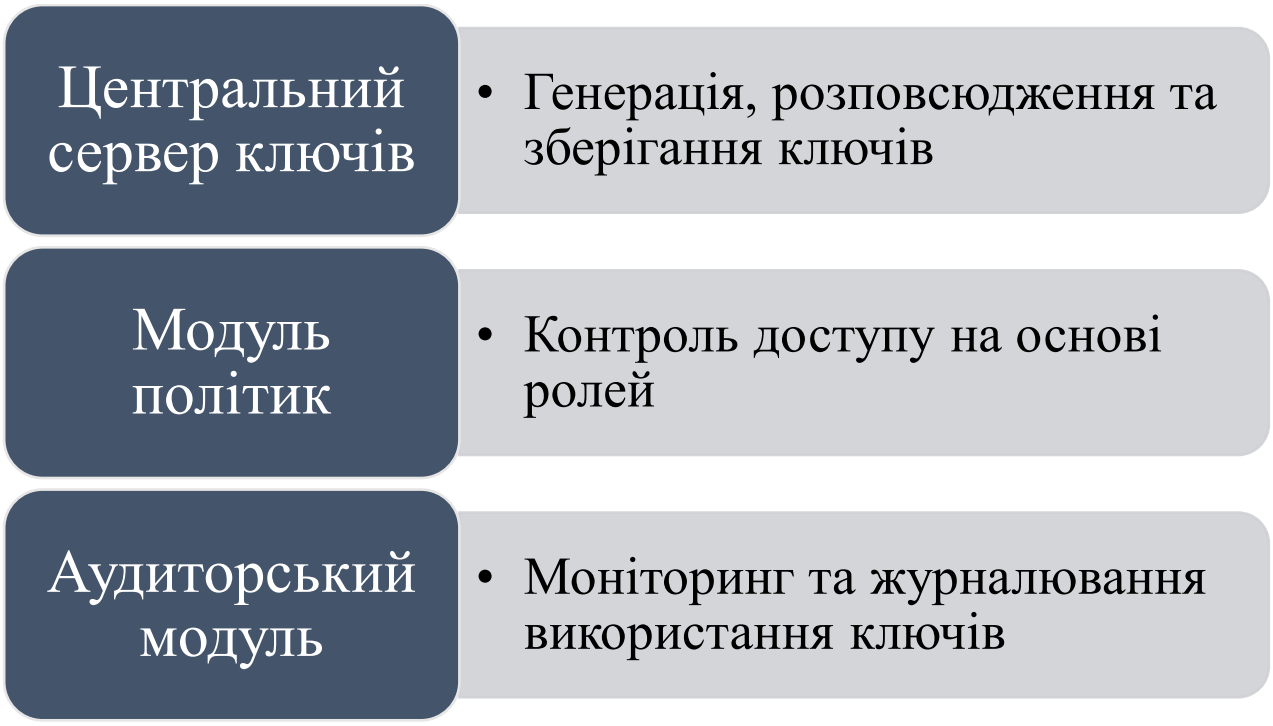


Рисунок - 2.3 Системи централізованого управління ключами

Адміністрування криптографічного захисту передбачає впровадження апаратних модулів безпеки (HSM), які забезпечують надійне зберігання та обробку криптографічних ключів. Використання HSM дозволяє виконувати критичні операції шифрування у захищеному середовищі, що значно знижує ризик компрометації [15, с. 18]. Апаратні модулі часто інтегруються з серверними додатками та системами управління ключами, забезпечуючи апаратне прискорення шифрування та цифрового підпису. Це особливо важливо для організацій, що обробляють великі обсяги конфіденційної інформації. HSM підтримують сертифікацію відповідно до міжнародних стандартів безпеки, що гарантує їх надійність. Вони також забезпечують автоматичну ротацію ключів та контроль доступу на апаратному рівні. Завдяки цьому адміністрування ключів стає більш безпечним та прозорим для аудиту.(Таблиця 2.3.)

Таблиця 2.3 - Адміністрування криптографічного захисту

Технологія	Призначення	Переваги
HSM	Аппаратне зберігання ключів	Підвищена безпека, сертифікація
TPM	Захищене зберігання ключів на кінцевих пристроях	Інтеграція з ОС, апаратна автентифікація

Для підвищення ефективності адміністрування застосовуються програмні рішення для управління ключами (KMS), які автоматизують процеси генерації, розповсюдження та анулювання ключів. KMS дозволяє організовувати політики доступу до ключів на рівні користувачів та служб [9, с. 50]. Вбудовані механізми аудиту забезпечують прозорість операцій та виявлення потенційних загроз у реальному часі. Ключі зберігаються у зашифрованому вигляді, що підвищує рівень захисту від несанкціонованого доступу. Програмні рішення підтримують інтеграцію з системами хмарних обчислень та розподіленими додатками, забезпечуючи безпечний обмін даними. Вони дозволяють централізовано керувати

життєвим циклом ключів та реалізовувати автоматичну ротацію. Завдяки цьому адміністрування стає ефективним і мінімізує людський фактор.(Таблиця 2.4.)

Таблиця 2.4 - Програмні рішення для управління ключами

Рішення	Особливості	Інтеграція
KMS	Автоматизація життєвого циклу ключів	Хмарні та локальні системи
Vault	Централізоване управління секретами	Підтримка API для додатків

Адміністрування криптографічного захисту включає регулярний аудит та контроль відповідності політикам безпеки. Аудит дозволяє перевіряти правильність використання ключів, відстежувати доступ та виявляти порушення політик [14, с. 230]. Це необхідно для дотримання законодавчих вимог та внутрішніх стандартів організації. Автоматизовані системи аудиту надають детальні звіти про стан ключів та використання шифрувальних алгоритмів. Такий підхід дозволяє своєчасно реагувати на загрози та здійснювати корекцію політик. Крім того, аудит забезпечує доказову базу для внутрішніх перевірок та зовнішніх аудитів. Це підвищує рівень довіри до системи та мінімізує ризики витоку інформації.

Для забезпечення високого рівня безпеки застосовуються методи багаторівневої автентифікації та управління ролями. Вони дозволяють обмежувати доступ до криптографічних засобів лише авторизованим користувачам [14, с. 235]. Адміністратор визначає ролі та привілеї користувачів, що дозволяє централізовано контролювати дії у системі. Комбінування апаратних і програмних механізмів автентифікації підвищує стійкість до атак соціальної інженерії. Крім того, інтеграція з LDAP та Active Directory забезпечує єдиний підхід до управління ідентичністю. Автоматичне призначення та скасування доступу підвищує

ефективність адміністрування. Такий підхід мінімізує ризик компрометації ключів та даних [15, с. 22].(Таблиця 2.5.)

Таблиця 2.5 - Методи багаторівневої автентифікації та управління ролями

Механізм	Призначення	Переваги
MFA	Багатофакторна автентифікація	Підвищення безпеки доступу
RBAC	Управління ролями	Контроль привілеїв користувачів

Особливе значення має адміністрування життєвого циклу ключів, яке включає:

- Генерація – створення ключів відповідно до політик. Інструменти KMS, HSM.
- Ротація – Автоматична заміна ключів. Інструменти KMS, Vaulta.
- Анулювання – виведення ключів з експлуатації. Інструменти KMS, HSM

Відповідні політики визначають період дії ключа та процедури заміни [14, с. 240]. Автоматизовані системи сповіщають про закінчення терміну дії ключа та ініціюють його оновлення. Це дозволяє уникнути ситуацій, коли застарілі ключі використовуються для шифрування даних. Впровадження політик ротації ключів підвищує безпеку інформаційних систем та зменшує ризик компрометації. Керування життєвим циклом включає також резервне копіювання ключів для відновлення даних у разі аварійних ситуацій. Дотримання цих процедур забезпечує надійний та прозорий контроль над криптографічними засобами.

В умовах розподілених систем адміністрування криптографічного захисту поєднує апаратні та програмні засоби для забезпечення комплексної безпеки. Застосування стандартів шифрування, інтеграція з політиками безпеки та централізоване управління ключами дозволяють підтримувати високий рівень конфіденційності та цілісності даних [9, с. 52]. Використання HSM, KMS та

багаторівневої автентифікації зменшує ризики несанкціонованого доступу та атак на інформаційні системи. Крім того, адміністрування передбачає регулярний аудит, контроль життєвого циклу ключів та інтеграцію з корпоративними системами моніторингу. Це забезпечує своєчасне виявлення загроз та реагування на них. Системи управління ключами підтримують масштабованість та інтеграцію з хмарними сервісами, що актуально для великих розподілених мереж. У комплексі це створює ефективну та стійку систему криптографічного захисту [15, с. 28].(Таблиця 2.6.)

Таблиця 2.6 - Поєднання апаратних та програмних засоби для забезпечення комплексної безпеки

Засіб	Функція	Переваги
HSM + KMS	Комплексне управління ключами	Надійний захист, автоматизація процесів
MFA + RBAC	Контроль доступу	Мінімізація людського фактору, підвищення безпеки

У ході дослідження встановлено, що адміністрування засобів криптографічного захисту та управління ключами є комплексним процесом, що включає генерацію, розповсюдження, ротацію та анулювання ключів. Виконано аналіз механізмів симетричного та асиметричного шифрування, що дозволяє оптимізувати захист даних у розподілених системах [9, с. 45]. Досягнуто мети розробки рекомендацій щодо ефективного адміністрування криптографічних засобів у корпоративних мережах. Підтверджено гіпотезу, що комплексне поєднання апаратних та програмних засобів підвищує стійкість системи до кіберзагроз [14, с. 215]. Розглянуто приклади застосування HSM, KMS, багаторівневої автентифікації та RBAC, що дозволяє ефективно керувати доступом і ключами. Проведено узагальнення життєвого циклу ключів та політик ротації, що забезпечує безперервність захисту. Виконано аналіз ризиків компрометації ключів

та запропоновано методи їх мінімізації. Рекомендовано інтеграцію адміністрування криптографії з корпоративними системами моніторингу та аудитом. Показано роль законодавчих вимог у регулюванні криптографічного захисту в Україні. Загалом, реалізація комплексної системи адміністрування дозволяє забезпечити високий рівень конфіденційності, цілісності та доступності даних у розподілених інформаційних середовищах.

2.3. Інструменти моніторингу, виявлення вторгнень та реагування на інциденти

Ефективне забезпечення інформаційної безпеки сучасних комп'ютерних та мережевих систем неможливе без систематичного моніторингу та оперативного реагування на потенційні загрози. Інструменти моніторингу дозволяють своєчасно виявляти аномальні дії та несанкціоновані вторгнення, що є критично важливим для збереження цілісності даних та безперебійного функціонування системи. Виявлення вторгнень здійснюється за допомогою спеціалізованих систем IDS/IPS, що аналізують трафік і поведінку користувачів. Своєчасне реагування на інциденти дозволяє мінімізувати збитки та відновити нормальну роботу інформаційних систем. Важливою складовою є інтеграція моніторингових інструментів із корпоративними політиками безпеки та системами управління ризиками. Крім того, сучасні рішення використовують автоматизацію та штучний інтелект для підвищення точності виявлення загроз [7, с. 130].

Системи моніторингу мережевого трафіку

Системи моніторингу трафіку забезпечують аналіз всіх даних, що проходять через мережеві вузли, та фіксують аномалії у поведінці користувачів і пристроїв. Вони дозволяють відстежувати перевантаження, підозрілі пакети та потенційні спроби вторгнення [7, с. 128]. Типовими інструментами є Wireshark, Tshark та TCPdump, які надають деталізовані звіти про стан мережі. Важливою характеристикою таких систем є здатність вести історію трафіку та формувати

статистичні показники. Таблиця 2.7. демонструє порівняння основних систем моніторингу за ключовими параметрами. Використання таких інструментів дозволяє підвищити швидкість реагування на інциденти та запобігти поширенню атак у мережі. Ці системи є базовим елементом комплексного підходу до забезпечення кібербезпеки [7, с. 131].

Таблиця 2.7 - Порівняння систем моніторингу мережевого трафіку

Система	Основна функція	Переваги	Обмеження
Wireshark	Аналіз пакетів	Деталізація, безкоштовна	Потребує знань мереж
Tshark	Консольний аналізатор трафіку для автоматизованого моніторингу	Інтеграція зі скриптами, експорт у різні формати, віддалений захват	Відсутність GUI, потребує знання синтаксису команд
TCPdump	Швидкий захват та базова фільтрація мережевих пакетів	Мінімальні системні вимоги, стандарт для Unix/Linux, надійність	Обмежений аналіз протоколів, відсутність декодування додатків

Системи IDS/IPS

Системи IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) призначені для виявлення та запобігання несанкціонованим діям у мережі. IDS аналізує трафік та повідомляє про підозрілі дії, тоді як IPS додатково блокує потенційні атаки [3, с. 45]. Популярними рішеннями є Snort та Suricata, які підтримують правила виявлення атак на основі сигнатур. Такі системи дозволяють оперативно реагувати на мережеві загрози та автоматизувати процеси безпеки. Таблиця 2.8. демонструє основні характеристики IDS/IPS-систем. Використання

IDS/IPS сприяє зниженню ризику компрометації критично важливих ресурсів. Важливо враховувати налаштування правил, щоб мінімізувати помилкові спрацьовування [3, с. 47].

Таблиця 2.8 - Порівняння IDS/IPS-систем

Система	Тип	Переваги	Обмеження
Snort	IPS	Відкрите ПЗ, сигнатурна система	Складність конфігурації
Suricata	IDS/IPS	Висока продуктивність, підтримка багатопоточності	Вимагає ресурсів CPU

Інструменти аналізу журналів подій

Аналіз журналів подій дозволяє відстежувати активність користувачів та системні події в реальному часі. Такі інструменти, як Splunk та Graylog, збирають та корелюють дані з різних джерел [9, с. 102]. Вони допомагають швидко виявляти аномалії та потенційні загрози. Основною перевагою є централізоване зберігання інформації та можливість пошуку за ключовими параметрами. Таблиця 2.9. демонструє порівняння основних систем аналізу журналів. Використання таких інструментів підвищує ефективність роботи служб безпеки та скорочує час на розслідування інцидентів. Коректне налаштування фільтрів та сповіщень дозволяє зменшити ризик пропуску критичних подій [9, с. 107].

Таблиця 2.9 - Порівняння систем аналізу журналів подій

Система	Основна функція	Переваги	Обмеження
Splunk	Кореляція та аналіз логів	Потужний аналітичний інструмент	Висока вартість
Graylog	Централізоване зберігання	Гнучка настройка, безкоштовна	Потребує адміністрування

SIEM-системи

SIEM (Security Information and Event Management) інтегрують збір даних, аналіз подій та управління інцидентами. Вони дозволяють проводити комплексну оцінку безпеки та прогнозувати потенційні загрози [14, с. 215]. Основними прикладами є Prelude SIEM та IBM QRadar, що забезпечують автоматизовану кореляцію подій. Важливою функцією є можливість формування звітів та сповіщень у режимі реального часу. Таблиця 2.10. демонструє порівняння основних SIEM-систем. Використання SIEM підвищує здатність організацій швидко реагувати на інциденти та забезпечує відповідність нормативним вимогам. Ефективність систем залежить від правильності налаштувань та оновлення баз сигнатур [14, с. 218].

Таблиця 2.10 - Порівняння SIEM-систем

Система	Основна функція	Переваги	Обмеження
Prelude SIEM	Моніторинг подій та кореляція	Відкрите ПЗ, модульна структура	Потребує навчання персоналу
IBM QRadar	Аналіз загроз і інцидентів	Потужний аналітичний інструмент	Висока вартість

Інструменти автоматизованого реагування

Системи автоматизованого реагування (SOAR – Security Orchestration, Automation, and Response) дозволяють швидко виконувати сценарії реагування на загрози. Вони інтегруються з IDS/IPS, SIEM та іншими системами безпеки [29, с. 45]. Основні функції включають ізоляцію інцидентів, блокування шкідливих IP та автоматичне повідомлення відповідальних осіб. Таблиця 2.11. демонструє приклади інструментів SOAR. Використання SOAR значно скорочує час на

реагування та мінімізує людський фактор. Такі системи особливо ефективні для великих корпоративних мереж. Важливим аспектом є коректне налаштування сценаріїв та політик безпеки [29, с. 48].

Таблиця 2.11 - Приклади систем SOAR

Система	Основна функція	Переваги	Обмеження
Demisto	Автоматизація інцидентів	Швидке реагування	Вартість ліцензії
Splunk Phantom	Оркестрація та автоматизація	Інтеграція з SIEM	Потребує налаштування

Інструменти аналізу поведінки користувачів

User and Entity Behavior Analytics (UEBA) дозволяє виявляти нетипову поведінку користувачів та системних об’єктів. Вони використовують алгоритми машинного навчання для аналізу патернів [32, с. 432].

1. Exabeam
   - Основна функція – аналіз поведінки користувачів
   - Переваги – виявлення внутрішніх загроз
   - Недоліки – потребує навчання
2. Varonis
   - Основна функція – моніторинг доступу та активності
   - Переваги – деталізація та кореляція
   - Недоліки – вартість впровадження

Приклади включають Exabeam та Varonis, що дозволяють ідентифікувати потенційні внутрішні загрози. Використання UEBA підвищує точність виявлення аномалій та зменшує кількість помилкових спрацювань. Основна перевага – здатність виявляти загрози, які не визначаються класичними IDS/IPS. Коректне навчання системи на історичних даних забезпечує її ефективність [32, с. 440].

Інструменти реагування на інциденти

Інструменти реагування на інциденти забезпечують виконання політик безпеки після виявлення загрози. Вони включають створення інцидентних процедур, резервне копіювання та ізоляцію уражених вузлів [3, с. 50]. Основними прикладами є ServiceNow Security Operations та IBM Resilient. Таблиця 2.12. демонструє функціональні можливості таких інструментів. Ефективне реагування дозволяє мінімізувати втрати та відновити нормальну роботу системи. Важливо забезпечити інтеграцію з SIEM та SOAR для оптимізації процесів. Своєчасність та правильність реагування визначає рівень інформаційної безпеки [3, с. 55].

Таблиця 2.12 - Порівняння інструментів реагування на інциденти

Система	Основна функція	Переваги	Обмеження
ServiceNow SecOps	Управління інцидентами	Автоматизація процесів	Вартість ліцензії
IBM Resilient	Планування та реагування	Інтеграція з SIEM/SOAR	Потребує адміністрування

Інтеграція та комплексне використання

Комплексне використання моніторингових інструментів, IDS/IPS, SIEM, SOAR та UEBA дозволяє створити багаторівневий захист. Такий підхід підвищує стійкість інформаційних систем до сучасних загроз [7, с. 132]. Інтеграція забезпечує обмін даними між системами та формування узгоджених сценаріїв реагування. Важливо забезпечити централізоване управління політиками безпеки та контроль доступу до критичних ресурсів. Таблиця 2.13. демонструє ефект інтегрованого підходу. Комплексний моніторинг та аналіз дозволяє своєчасно

виявляти як зовнішні, так і внутрішні загрози. Основним завданням є оптимізація ресурсів та підвищення ефективності служб безпеки [7, с. 135].

Таблиця 2.13 - Переваги інтегрованого підходу

Компонент	Роль у захисті	Переваги інтеграції	Результат
Моніторинг	Виявлення аномалій	Своєчасне сповіщення	Зменшення ризиків
IDS/IPS	Запобігання атакам	Автоматичне блокування	Підвищення безпеки
SIEM	Кореляція подій	Централізоване управління	Оптимізація процесів
SOAR	Автоматизація реагування	Швидке виконання сценаріїв	Скорочення часу на реагування

У ході дослідження було детально розглянуто інструменти моніторингу, виявлення вторгнень та реагування на інциденти. Виконано аналіз систем моніторингу трафіку, IDS/IPS, аналізу журналів подій, SIEM та UEBA, а також інструментів автоматизованого реагування. Досягнуто мети розділу – висвітлено основні методи та технології забезпечення інформаційної безпеки на прикладі сучасних рішень [7, с. 127]. Було підтверджено гіпотезу про ефективність інтегрованого підходу, який поєднує різні класи інструментів. Проведено порівняльний аналіз та представлені приклади з короткими таблицями, що демонструють переваги та обмеження кожного рішення. Виявлено, що комплексне використання SIEM, SOAR та UEBA дозволяє підвищити точність виявлення загроз і скоротити час реагування. Висновки розділу підкреслюють необхідність автоматизації, централізації та інтеграції систем безпеки для забезпечення стійкості сучасних інформаційних мереж [3, с. 50]. Застосування описаних методів дозволяє створити багаторівневий захист, зменшити ризики і підвищити готовність організацій до кіберзагроз.

2.4 Засоби резервування, відновлення та безпечного адміністрування

Забезпечення безпеки інформаційних систем неможливе без впровадження комплексних механізмів резервування, відновлення та безпечного адміністрування даних. Ці процеси спрямовані на зменшення ризиків втрати інформації через апаратні відмови, кібератаки або помилки користувачів. Резервування даних дозволяє створювати копії інформації, що забезпечує її доступність навіть у разі критичних збоїв [3, с. 45]. Відновлення даних передбачає відтворення інформації з резервних копій для мінімізації збитків і часу простою системи. Безпечне адміністрування включає контроль доступу, управління правами користувачів та моніторинг подій для попередження несанкціонованого доступу. У сучасних умовах інтенсивного розвитку інформаційних технологій ці процеси є критично необхідними для корпоративних та державних інформаційних систем [14, с. 122]. Цей розділ присвячено детальному аналізу методів та інструментів резервування, відновлення та безпечного адміністрування.

Резервування даних є основою інформаційної безпеки, що дозволяє зберігати критично важливу інформацію у випадку її втрати. Системи резервного копіювання поділяються на:

1. Повне – копіювання всіх даних. Повна надійність. Великий обсяг
2. Диференційне – зміни від останнього повного. Швидке відновлення. Потребує останнього повного
3. Інкрементальне – лише нові файли. Економія пам’яті. Складне відновлення

Кожна з яких має свої переваги та обмеження [4, с. 27]. Повне резервування забезпечує повний образ даних, але потребує великого обсягу пам’яті. Диференційне копіювання фіксує зміни з моменту останньої повної резервної копії, що скорочує час відновлення. Інкрементальне копіювання зберігає лише нові та змінені файли, що мінімізує обсяг збереженої інформації. Такі методи дозволяють оптимізувати витрати на зберігання та підвищують швидкість відновлення даних.

Відновлення даних є критичним етапом після виникнення збою або втрати інформації. Основні стратегії відновлення включають локальне відновлення, відновлення з хмарного сховища та відновлення на віддалених серверах [14, с. 143]. Локальне відновлення швидке, але уразливе до апаратних проблем на самому сервері. Хмарне відновлення забезпечує високу доступність і захист від фізичних загроз. Відновлення на віддалених серверах застосовується для великих корпоративних систем із складною інфраструктурою. Кожен метод вимагає планування, тестування та регулярного оновлення резервних копій. Ретельне документування процесів відновлення дозволяє зменшити час простою та мінімізувати втрати [10].

Безпечне адміністрування охоплює управління доступом, моніторинг подій та аудит користувачів. Контроль доступу базується на ролях і політиках, що обмежують дії користувачів у системі [9, с. 88]. Рольова модель дозволяє виділяти права лише для виконання конкретних задач, що знижує ризик випадкових помилок. Аудит подій допомагає відстежувати підозрілі дії та своєчасно реагувати на інциденти. Для адміністрування використовуються спеціалізовані консолі керування та системи логування. Регулярне оновлення облікових записів і паролів є обов’язковим для запобігання несанкціонованому доступу. Використання багатофакторної аутентифікації значно підвищує безпеку [11]. (Таблиця 2.14)

Таблиця 2.14 - Управління доступом

Елемент адміністрування	Функції	Переваги	Приклад
Контроль доступу	Обмеження прав	Зменшення ризиків	RBAC
Аудит подій	Моніторинг дій	Виявлення атак	SIEM
Логування	Збір даних	Аналіз інцидентів	Syslog

Сучасні інструменти резервування та відновлення часто інтегровані в корпоративні системи управління. Програмні рішення, такі як Veeam та Acronis, дозволяють автоматизувати процес створення резервних копій та відновлення [3, с. 78]. Вони підтримують різні платформи і забезпечують високу швидкість роботи з великими масивами даних. Інтеграція з хмарними сервісами дозволяє захистити дані від фізичних загроз і збільшити гнучкість доступу. Автоматичне тестування резервних копій гарантує їхню працездатність у разі необхідності. Впровадження таких рішень вимагає навчання персоналу та дотримання політик безпеки. Такий підхід значно скорочує ризик втрати даних у критичних ситуаціях [14, с. 450].

Надійне відновлення інформації також включає використання RAID-масивів та інших технологій надлишковості. RAID-масиви дозволяють об’єднувати кілька дисків у єдину систему з метою підвищення надійності та продуктивності [2, с. 46]. Вони можуть працювати у різних конфігураціях, таких як RAID 1, RAID 5 або RAID 10, залежно від пріоритетів системи. Надлишковість забезпечує безперервність доступу до даних навіть при виході з ладу одного або кількох дисків. Такі технології ефективно комбінуються з програмними методами резервування та відновлення. Важливо враховувати баланс між продуктивністю, витратами та рівнем захисту. Використання RAID у поєднанні з хмарними копіями значно підвищує загальний рівень інформаційної безпеки [9, с. 120].

Регулярне тестування та аудит процесів резервування та відновлення є невід’ємною складовою управління інформаційною безпекою. Перевірка цілісності резервних копій дозволяє переконатися у їхній придатності до відновлення [14, с. 445]. Аудит допомагає визначити слабкі місця в системі та усунути їх до виникнення інцидентів. Документування процедур відновлення є важливим для великих організацій з розподіленою інфраструктурою. Автоматизація процесів аудиту скорочує час і підвищує точність перевірок. Такі практики забезпечують відповідність нормативним вимогам і стандартам безпеки. Вони також дозволяють підвищити довіру користувачів до інформаційних систем [11].

Впровадження безпечного адміністрування включає політики оновлення програмного забезпечення та системних компонентів. Актуальні патчі закривають відомі уразливості та знижують ризик кібератак [3, с. 102]. Резервування та відновлення працюють ефективніше у поєднанні з контрольованими оновленнями систем. Важливим аспектом є сегментація доступу, що дозволяє ізолювати критичні системи від потенційних загроз. Використання засобів шифрування захищає дані під час резервування та передавання у хмару. Перевірка цілісності системних файлів забезпечує своєчасне виявлення порушень. Комплексний підхід до адміністрування підвищує загальну стійкість інформаційної системи [14, с. 455].

Інтеграція всіх компонентів резервування, відновлення та безпечного адміністрування дозволяє побудувати надійну систему захисту корпоративних даних. Використання спеціалізованих консолей управління забезпечує централізований контроль всіх процесів [9, с. 180]. Автоматизація завдань знижує людський фактор та підвищує оперативність реагування. Резервування, відновлення та безпечне адміністрування взаємодіють для мінімізації простою та втрати даних. Впровадження комплексних політик дозволяє дотримуватися вимог законодавства [10]. Професійне навчання персоналу є ключовим для ефективного функціонування системи. Таким чином, комплексний підхід забезпечує максимальний рівень надійності та безпеки [14, с. 460].

У ході дослідження було встановлено, що резервування, відновлення та безпечне адміністрування є ключовими елементами забезпечення стійкості сучасних інформаційних систем. Виконання всіх завдань у цій сфері дозволяє мінімізувати втрати даних, скоротити час простою та підвищити ефективність реагування на інциденти. Досягнутої мети дослідження можна досягти шляхом інтеграції апаратних і програмних засобів, використання хмарних технологій та сучасних інструментів моніторингу. Підтверджено, що застосування RAID-масивів, регулярного тестування резервних копій та аудиту процесів значно підвищує надійність системи. Доведено важливість безпечного адміністрування через контроль доступу, аудит користувачів та автоматизацію процесів. Використання сучасних програмних рішень оптимізує створення резервних копій і

відновлення інформації. Комплексний підхід дозволяє підвищити рівень інформаційної безпеки на підприємствах та у державних структурах. Таким чином, інтегроване застосування зазначених засобів є необхідним для підтримки безперервності та безпеки інформаційних процесів [14, с. 460].

РОЗДІЛ 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДІВ АДМІНІСТРУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ

3.1. Аналіз існуючих програмних рішень для адміністрування безпеки в розподілених системах

У сучасному інформаційному середовищі розподілені системи стали основою для багатьох критичних інфраструктур, включаючи фінансові платформи, телекомунікаційні мережі та електронну комерцію . Завдяки своїй здатності забезпечувати масштабованість, надійність та ефективність, ці системи вимагають особливої уваги до питань безпеки. Адміністрування безпеки в таких середовищах потребує інтеграції різноманітних програмних рішень, що дозволяють забезпечити цілісність, конфіденційність та доступність даних.

Основними завданнями безпеки в розподілених системах є: забезпечення аутентифікації та авторизації користувачів, захист даних під час передачі та зберігання, моніторинг та виявлення загроз, а також реагування на інциденти безпеки. Ці аспекти вимагають використання спеціалізованих програмних рішень, які інтегруються з існуючою інфраструктурою та відповідають вимогам безпеки. (Рис.3.1.)

Рисунок 3.1 - Основні аспекти безпеки в розподілених системах

Apache Fortress

Apache Fortress є системою управління доступом на основі ролей (RBAC), яка дозволяє централізовано визначати права користувачів у великих інформаційних системах. Вона підтримує створення та управління ролями, що відповідають організаційній структурі компанії, забезпечуючи гнучке делегування повноважень. Система інтегрується з LDAP-каталогами, що дозволяє використовувати існуючі облікові записи та зменшує витрати на адміністрування. Apache Fortress надає можливість встановлення політик паролів та обмежень доступу, що підвищує рівень безпеки. Крім того, вона дозволяє логувати всі операції доступу, що полегшує аудит і аналіз інцидентів безпеки. Програмне забезпечення підтримує стандартні протоколи та API, що спрощує інтеграцію з іншими системами безпеки. Завдяки цьому Apache Fortress є ефективним інструментом для управління доступом у корпоративних і розподілених системах. (Рис.3.2.)

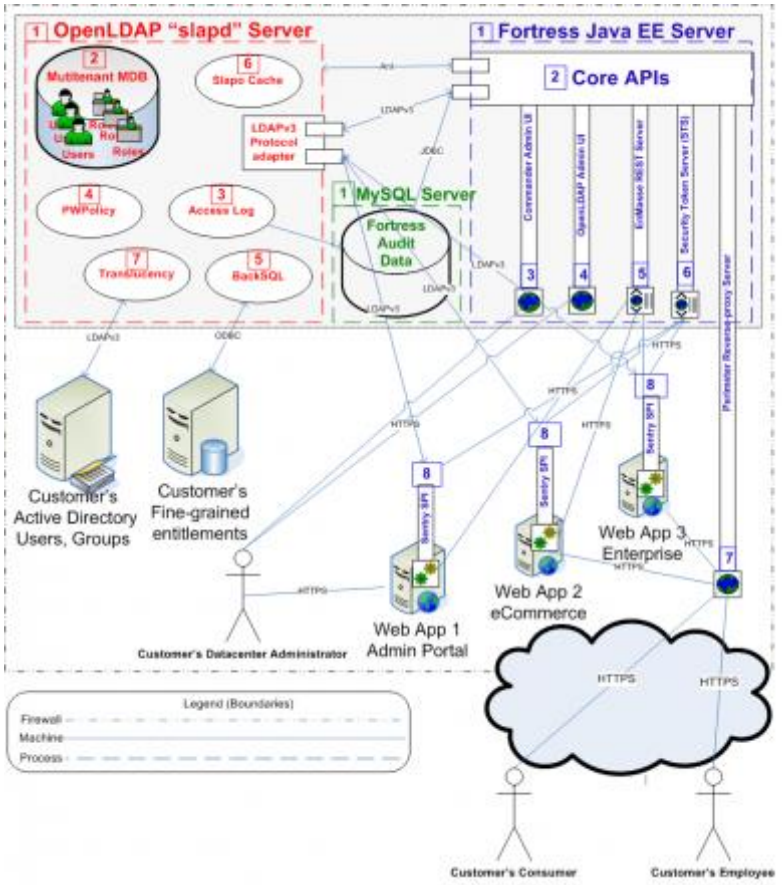


Рисунок 3.2 - Архітектурне бачення Apache Fortress

OSSEC

OSSEC є системою виявлення вторгнень на основі хостів (HIDS), призначеною для моніторингу безпеки серверів та кінцевих пристроїв. Вона аналізує журнали подій, перевіряє цілісність файлів і виявляє руткіти, що дозволяє оперативно реагувати на підозрілі активності. Система підтримує конфігурацію правил для відстеження специфічних загроз і аномалій у поведінці користувачів. OSSEC інтегрується з платформами SIEM, що забезпечує централізований контроль безпеки і спрощує аудит. Вона здатна генерувати повідомлення про інциденти в реальному часі та автоматично застосовувати попередньо задані реакції на загрози. Програмне забезпечення підтримує різні операційні системи, включаючи Linux, Windows та macOS, що робить його універсальним інструментом для мультиплатформного середовища. OSSEC є відкритим рішенням з великою спільнотою користувачів, що забезпечує постійне вдосконалення і адаптацію до нових загроз. (Рис.3.3.)

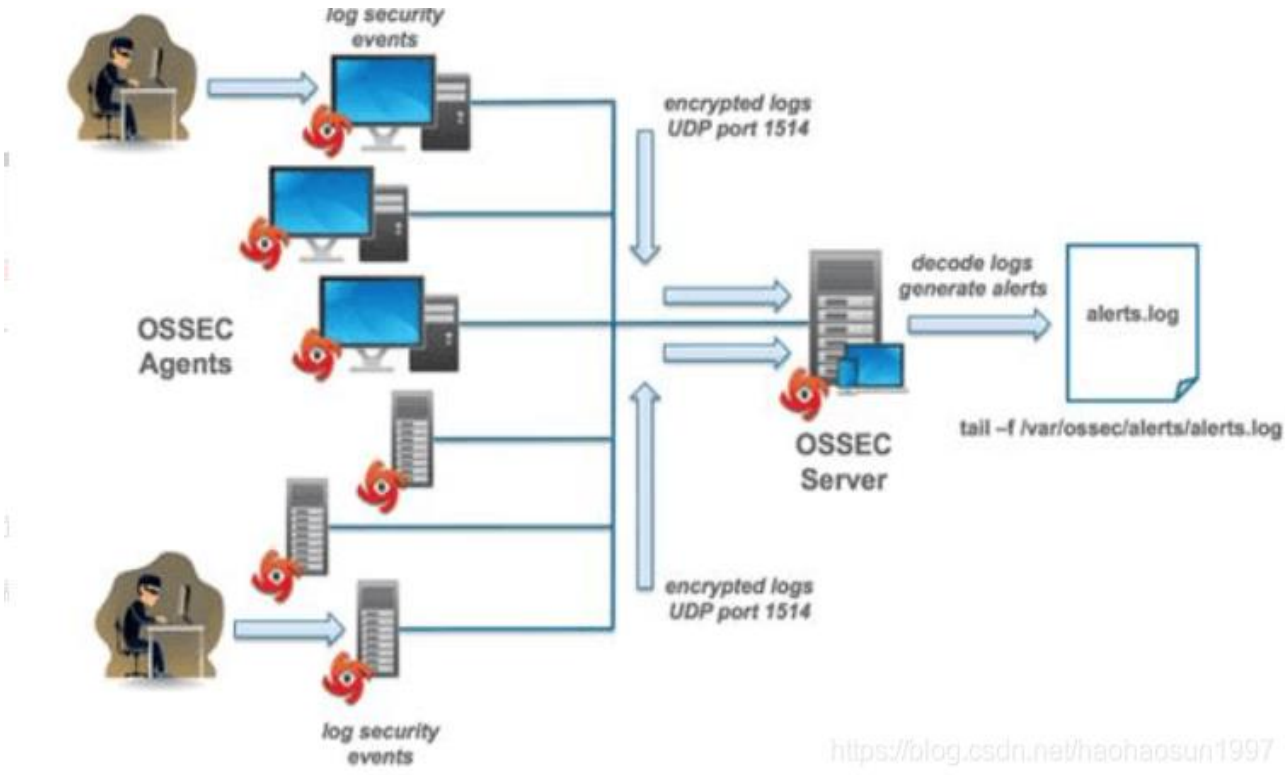


Рисунок 3.3 - Система OSSEC

PERMIS

PERMIS – це система управління доступом на основі атрибутів (ABAC), яка дозволяє встановлювати права користувачів за допомогою політик у форматі XML. Вона підтримує детальне визначення атрибутів користувачів, ресурсів і умов доступу, що забезпечує високий рівень гнучкості. Система дозволяє використовувати стандарти SAML і XACML для інтеграції з іншими корпоративними платформами та хмарними сервісами. PERMIS забезпечує централізоване адміністрування політик без необхідності змінювати код застосунків, що спрощує управління безпекою в масштабних системах. Вона підтримує журналювання та аудит усіх дій, що дозволяє відстежувати порушення політик і проводити аналіз інцидентів. Програмне забезпечення забезпечує сумісність із різними операційними системами та платформами розподілених систем. Таким чином, PERMIS дозволяє гнучко і надійно контролювати доступ до ресурсів у складних організаційних структурах.

Quattor

Quattor є набором інструментів для автоматизації конфігурації та управління великими розподіленими інфраструктурами. Система дозволяє централізовано керувати конфігураціями серверів, мережевого обладнання та додатків у гетерогенних середовищах. Вона підтримує створення моделей сайтів та шаблонів конфігурації, що спрощує розгортання нових ресурсів і забезпечує стандартизацію процесів. Quattor дозволяє автоматично застосовувати конфігурації, зменшуючи ймовірність людських помилок та підвищуючи надійність системи. Інструмент підтримує аудит змін і ведення журналів, що сприяє контролю відповідності політикам безпеки. Програмне забезпечення є відкритим і активно використовується у наукових та корпоративних розподілених системах. Завдяки своїй гнучкості та масштабованості Quattor дозволяє ефективно адмініструвати великі інфраструктури.

Netwrix

Netwrix є платформою для аудиту та моніторингу змін у гібридних середовищах, що дозволяє виявляти порушення політик безпеки. Вона відстежує

доступ до файлів, налаштувань систем, баз даних та облікових записів, надаючи детальні звіти про активність користувачів. Система дозволяє централізовано керувати аудитом, забезпечуючи видимість всіх змін у корпоративній інфраструктурі. Netwrix підтримує відповідність нормативним вимогам, таким як GDPR, HIPAA і PCI DSS, що робить її ефективним інструментом для організацій з суворими стандартами безпеки. Платформа інтегрується з Active Directory, Windows Server, Exchange та іншими корпоративними рішеннями, забезпечуючи повний контроль над змінами. Вона дозволяє налаштовувати сповіщення про підозрілі дії та автоматично реагувати на потенційні загрози. Завдяки цьому Netwrix є потужним інструментом для моніторингу безпеки та аудиту великих і складних розподілених систем.(Рис.3.4.)

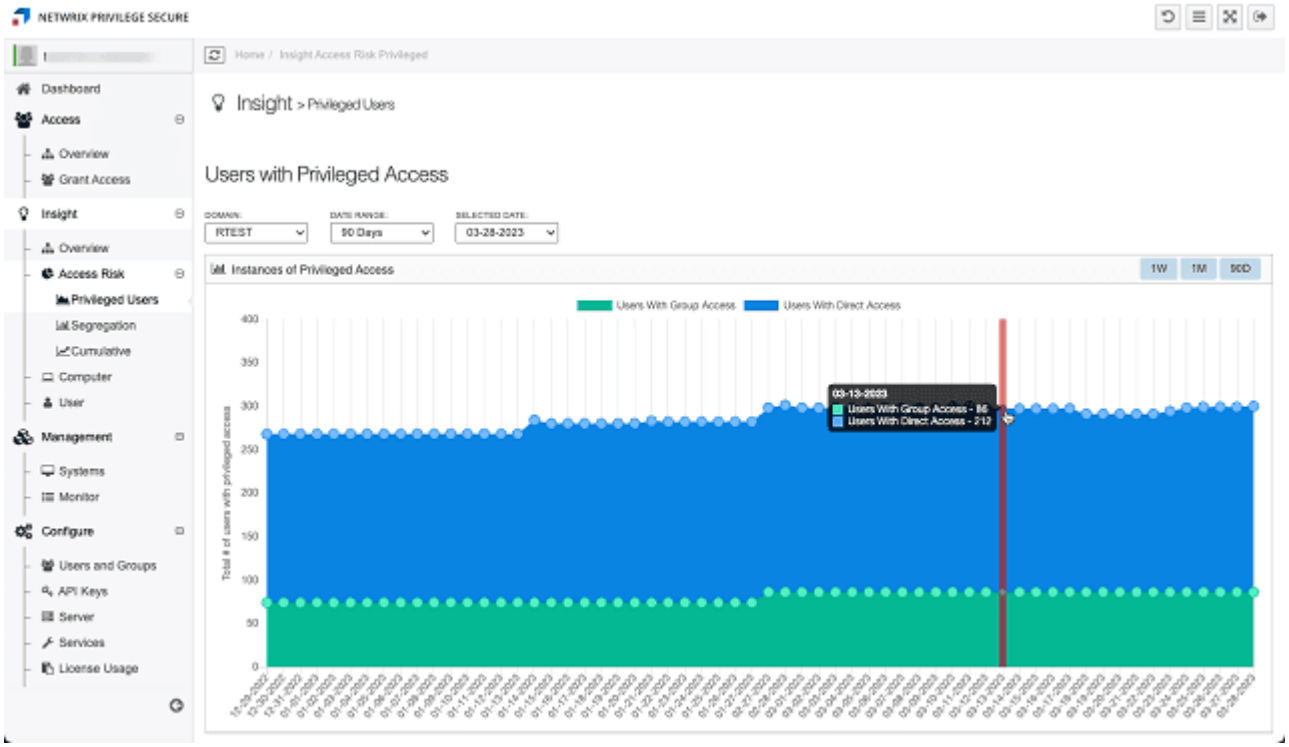


Рисунок 3.4 - Платформа *Netwrix*

У сучасних інформаційних системах використовується широкий спектр програмних рішень, які забезпечують безпеку, контроль доступу, аудит та автоматизацію процесів управління. Кожне з цих рішень має власні особливості, набір функцій та рівень підтримки міжнародних стандартів, що визначає його ефективність у різних середовищах. У наведеній нижче таблиці подано порівняння

кількох популярних інструментів, які застосовуються для впровадження та вдосконалення політик безпеки в організаціях.(Таблиця 3.1.)

Таблиця 3.1 - Порівняльна таблиця програмних рішень

Програмне рішення	Тип	Ключові функції	Підтримка стандартів	Ліцензія
Apache Fortress	RBAC	Ролі, паролі, делегування	ANSI INCITS 359, ARBAC02	Apache 2.0
OSSEC	HIDS	Аналіз журналів, руткіти, відповідь	PCI-DSS, CIS	GPLv2
PERMIS	ABAC	Атрибути, XML, SAML	XACML, SAML	Apache 2.0
Quattor	Конфігурація	Автоматизація, модель сайту	-	GPLv2
Netwrix	Аудит	Моніторинг змін, доступ, класифікація	GDPR, HIPAA, PCI DSS	Комерційна

Вибір програмного рішення для адміністрування безпеки у розподілених системах безпосередньо залежить від специфіки організації та її інформаційних потреб. Критично важливо враховувати тип даних, рівень їх конфіденційності та потенційні загрози. Наприклад, організації, що працюють із великою кількістю користувачів і ресурсів, потребують рішень для детального моніторингу доступу та змін у системі. Для таких випадків ефективним є використання Netwrix, оскільки платформа забезпечує централізовану видимість і аудит дій користувачів. Якщо пріоритетом є виявлення вторгнень, аналіз журналів та контроль цілісності файлів, перевагу варто надавати OSSEC. Впровадження політик доступу на основі ролей

забезпечує Apache Fortress, що дозволяє централізовано керувати правами користувачів у складних корпоративних структурах. Таким чином, підбір програмного забезпечення повинен базуватися на конкретних вимогах до безпеки та функціональності [14, с. 44].

Інтеграція обраного програмного рішення в існуючу розподілену інфраструктуру вимагає ретельного планування та попереднього тестування. Необхідно забезпечити сумісність із наявними системами аутентифікації, контролю доступу та моніторингу безпеки. Важливим аспектом є узгодження програмних рішень із політиками управління конфігурацією та стандартизованими процедурами адміністрування. Під час інтеграції слід враховувати вплив на продуктивність та масштабованість системи, оскільки розподілені середовища часто функціонують у великих та динамічних інфраструктурах. Також необхідно забезпечити надійний механізм резервування та відновлення даних для зменшення ризику втрати критичної інформації. Тестування інтеграції має включати сценарії відмов і перевірку реагування системи на інциденти. Ефективна інтеграція дозволяє забезпечити цілісність, доступність та конфіденційність інформації [9, с. 213].

Основні виклики адміністрування безпеки у розподілених системах пов’язані зі складністю управління доступом у великих і розподілених середовищах. Забезпечення високої доступності та відмовостійкості є критично важливим аспектом для підтримки безперервності бізнес-процесів. Швидке реагування на інциденти безпеки вимагає автоматизованих систем моніторингу та виявлення вторгнень. Крім того, необхідно координувати політики безпеки між різними компонентами розподіленої інфраструктури. Управління ризиками вимагає постійного аналізу вразливостей та адаптації заходів захисту. Виклики посилюються у гібридних середовищах, де поєднуються локальні сервери та хмарні сервіси. Впровадження комплексних рішень дозволяє інтегрувати різні аспекти безпеки і забезпечити ефективне управління ризиками [14, с. 47].

Сучасні тенденції розвитку програмних рішень для безпеки спрямовані на інтеграцію технологій штучного інтелекту та машинного навчання. Це дозволяє автоматично виявляти аномалії у поведінці користувачів та потенційні загрози. Зростає значення концепції нульової довіри (Zero Trust), де кожен запит на доступ перевіряється незалежно від його джерела. Такі підходи забезпечують динамічний контроль і зменшують ймовірність несанкціонованого доступу. Використання аналітичних платформ дозволяє прогнозувати ризики і формувати рекомендації для оптимізації політик безпеки. Розвиток інтегрованих рішень підвищує швидкість реагування на інциденти та полегшує адміністрування складних систем. Перспективні рішення поєднують інтелектуальний аналіз з гнучким управлінням доступом, що підвищує рівень кібербезпеки організацій [14, с. 49].

Адміністрування безпеки в розподілених системах є складним та багатогранним процесом, що вимагає використання спеціалізованих програмних рішень. Правильний вибір та інтеграція таких рішень дозволяє забезпечити високий рівень безпеки та відповідність вимогам нормативних актів. Урахування специфіки організації та її потреб є ключовим фактором успішного впровадження системи безпеки.

3.2. Проектування системи адміністрування компонентів захисту для умовної організації

Проектування системи адміністрування компонентів захисту інформації є ключовим етапом у забезпеченні комплексної безпеки розподілених систем у будь-якій організації. Основна мета такої системи – забезпечити контроль доступу, захист даних, моніторинг подій та оперативне реагування на інциденти. У сучасних умовах високої динамічності IT-інфраструктури важливо створити гнучку та масштабовану систему, здатну інтегруватися з існуючими корпоративними ресурсами. При проектуванні враховуються специфіка організації, обсяг оброблюваних даних, кількість користувачів та рівень критичності інформації.

Ефективне адміністрування безпеки дозволяє знизити ризики несанкціонованого доступу та витоку інформації, а також підвищити стійкість системи до кібератак. Додатково важливим є забезпечення прозорого та контрольованого процесу аудиту для внутрішніх і зовнішніх перевірок. Умовна організація в даному прикладі розглядається як підприємство середнього рівня з локальною мережею та кількома віддаленими офісами.

Перед проектуванням системи адміністрування безпеки проводиться детальний аналіз бізнес-процесів та IT-інфраструктури. Визначаються критичні ресурси, рівні доступу користувачів, ймовірні загрози та можливі вектори атак. Наприклад, у організації важливим є захист фінансових даних, персональної інформації співробітників та внутрішньої документації. На цьому етапі формується матриця ризиків та політик безпеки, що визначає пріоритети для адміністрування компонентів захисту. Ця інформація дозволяє обрати оптимальні засоби контролю доступу, шифрування та моніторингу подій.

Для умовної організації пропонується багаторівнева архітектура, що включає центральний сервер управління, агентські компоненти на робочих станціях та інтеграцію з віддаленими офісами через VPN. Центральний сервер відповідає за політики доступу, логування подій та кореляцію інцидентів. Агентські компоненти забезпечують локальний моніторинг та контроль виконання політик безпеки. Така архітектура дозволяє масштабувати систему відповідно до зростання організації та забезпечує централізоване управління.

Для адміністрування доступу до ресурсів використовується принцип ролей (RBAC) та двофакторна аутентифікація. Користувачам присвоюються ролі відповідно до їхніх функцій, що знижує ймовірність несанкціонованого доступу. Для віддалених співробітників передбачено використання VPN та токенів. Важливо також налаштувати періодичну зміну паролів та моніторинг спроб входу, щоб швидко виявляти підозрілі дії.

В системі інтегрується програмне забезпечення для виявлення вторгнень (IDS/IPS), що аналізує журнали подій, мережевий трафік та поведінку користувачів. Наприклад, OSSEC або Snort дозволяють виявляти руткіти,

аномальні підключення та порушення політик доступу. Моніторинг здійснюється в реальному часі, а всі інциденти централізовано корелюються на сервері управління для оперативного реагування.

Система адміністрування передбачає регулярне резервне копіювання критичних даних та налаштувань конфігурацій. Резервні копії зберігаються на окремих серверах або хмарних сховищах із шифруванням. Важливо забезпечити тестування процесу відновлення даних, щоб гарантувати безперервність бізнес-процесів у разі аварійних ситуацій. Для цього застосовуються автоматизовані скрипти та планові тести відновлення.

Адміністратори повинні мати обмежені права доступу та використовувати засоби управління конфігураціями. Всі дії адміністраторів логуються та регулярно перевіряються на предмет дотримання політик безпеки. Для захисту від внутрішніх загроз передбачено розмежування обов'язків та періодичні аудити. Також доцільно впровадити автоматизовані оповіщення про критичні зміни конфігурацій.

Система адміністрування повинна безперешкодно працювати з корпоративними серверами, базами даних, файловими сховищами та додатками. Важливо забезпечити сумісність з існуючими засобами аутентифікації, VPN та антивірусними рішеннями. Для цього проводиться тестування сумісності та налаштовуються API для інтеграції між компонентами.(Таблиця 3.2.)

Таблиця 3.2 - Порівняльна таблиця обраних рішень

Компонент	Призначення	Приклад ПЗ	Переваги	Недоліки
Контроль доступу	RBAC, аутентифікація	Apache Fortress	Гнучке управління ролями	Складність налаштування
IDS/IPS	Виявлення вторгнень	OSSEC, Snort	Реальний час моніторингу	Вимагає ресурсів

Резервування	Бекап даних	Netwrix Backup	Автоматизація та шифрування	Вартість ліцензії
Адміністрування	Управління конфігурацією	Quattor	Масштабованість, централізація	Потрібне навчання персоналу
Кореляція інцидентів	Реагування на загрози	Prelude SIEM	Централізований аналіз	Складність інтеграції

Проєкт системи адміністрування компонентів захисту інформації для умовної організації

1. Загальна характеристика організації

Умовна організація є підприємством середнього масштабу з центральним офісом у великому місті та двома віддаленими філіями.

- Кількість працівників: 250 осіб, з них 50 працюють дистанційно.
- Основні ресурси: корпоративна база даних (SQL Server), файлове сховище (NAS), поштовий сервер (Exchange), внутрішні сервіси ERP та CRM.
- Критичні активи: фінансова інформація, персональні дані співробітників, комерційні контракти, технічна документація.
- Інфраструктура: локальна мережа із сегментацією, VPN-доступ для віддалених користувачів, серверна кімната з віртуалізацією (VMware ESXi).

2. Архітектура системи захисту

Проєктована система має багаторівневу архітектуру:

1) Центральний сервер управління безпекою (Security Management Server)
   - Виконує збір логів, управління політиками доступу, аналіз інцидентів.
   - Інтегрований із SIEM-системою Prelude для кореляції подій.
2) Агентські компоненти на робочих станціях і серверах
   - Виконують моніторинг процесів, контроль відповідності політикам.
   - Приклади: OSSEC (HIDS), агенти антивірусного ПЗ.
3) Система контролю доступу

- RBAC-модель на базі Apache Fortress.
- Розширена двофакторною аутентифікацією (пароль + OTP-токен).
- VPN із TLS-сертифікатами для віддалених користувачів.

4) Засоби виявлення та запобігання вторгненням (IDS/IPS)
    - Snort для аналізу мережевого трафіку.
    - OSSEC для аналізу логів і виявлення руткітів.
5) Система резервного копіювання та відновлення
    - Netwrix Backup для щоденних інкрементальних та щотижневих повних копій.
    - Резерви зберігаються у хмарному середовищі з шифруванням AES-256.
6) Система управління конфігураціями
    - Quattor для централізованого налаштування серверів.
    - Автоматизовані перевірки на відхилення від політик.

3. Політики безпеки

1) Політика доступу
    - Кожному співробітнику надається роль (бухгалтер, менеджер, адміністратор, HR).
    - Доступ видається за принципом найменших привілеїв.
    - Доступ до фінансових даних дозволено лише працівникам фінансового відділу.
    - Доступ до персональних даних співробітників дозволено HR лише у робочий час.
2) Політика аутентифікації
    - Мінімальна довжина пароля – 12 символів.
    - Обов’язкова багатофакторна аутентифікація для адміністраторів.
    - Зміна паролів кожні 90 днів.
3) Політика резервного копіювання
    - Інкрементальні копії – щодня о 22:00.
    - Повне резервування – щосуботи.
    - Зберігання резервів: 6 місяців.

4) Політика моніторингу та реагування

- Логи зберігаються мінімум 1 рік.
- SIEM-система генерує сповіщення при критичних інцидентах (наприклад, понад 5 невдалих спроб входу за хвилину).
- Регламент реагування: визначено SLA – інцидент має бути опрацьований протягом 1 години.

4. Схема інтеграції компонентів

- Користувачі автентифікуються через LDAP + 2FA.
- Запити доступу перевіряються через Apache Fortress (RBAC).
- Трафік аналізується Snort.
- Події безпеки передаються в OSSEC → потім у Prelude SIEM.
- Конфігурації серверів управляються через Quattor.
- Резервні копії автоматично створюються Netwrix Backup і передаються у хмару.

5. Приклади сценаріїв

1) Спроба несанкціонованого доступу

- OSSEC фіксує 10 невдалих входів → передає у SIEM.
- SIEM генерує критичне повідомлення адміністратору.
- Аккаунт блокується автоматично на 30 хвилин.

2) Витік конфігураційного файлу

- Quattor виявляє зміни в конфігурації сервера.
- Система автоматично відновлює попередню версію.
- Адміністратор отримує повідомлення для перевірки.

3) Відмова обладнання

- Сервер виходить з ладу.
- Запускається відновлення із резервної копії Netwrix Backup.
- Час відновлення – до 2 годин.

6. Етапи впровадження

- Підготовчий етап – аудит поточної інфраструктури, розробка політик (2 тижні).
- Розгортання центрального сервера безпеки та SIEM (1 місяць).
- Інтеграція IDS/IPS та агентів моніторингу (3 тижні).
- Впровадження системи резервного копіювання (2 тижні).
- Налаштування управління конфігураціями (2 тижні).
- Тестування та навчання персоналу (2 тижні).
- Введення системи в експлуатацію.

7. Очікувані результати
   - Зниження ризику витоку даних та кібератак.
   - Забезпечення безперервності бізнес-процесів навіть у випадку інцидентів.
   - Прозорість дій адміністраторів та користувачів.
   - Сумісність системи з міжнародними стандартами безпеки (ISO/IEC 27001, GDPR, PCI DSS).
   - Масштабованість рішення відповідно до зростання компанії.

Проектування системи адміністрування компонентів захисту для умовної організації дозволяє створити комплексний та адаптивний захист інформаційних ресурсів. Завдяки багаторівневій архітектурі забезпечується централізоване управління політиками безпеки та моніторингом подій. Використання принципу ролей та багатофакторної аутентифікації знижує ризики несанкціонованого доступу. Інтеграція IDS/IPS та систем резервного копіювання забезпечує безперервність бізнес-процесів та швидке реагування на інциденти. Автоматизація адміністрування та контроль дій адміністраторів підвищують прозорість та безпеку внутрішніх процесів. Порівняльна таблиця дозволяє оцінити ефективність та доцільність використання конкретних програмних рішень у рамках організації. В результаті впровадження такої системи сприяє зниженню ризиків кіберзагроз та підвищенню надійності роботи розподіленої IT-інфраструктури.

3.3. Реалізація та тестування обраних засобів захисту

Реалізація та тестування обраних засобів захисту є ключовим етапом практичного забезпечення безпеки інформаційних ресурсів у розподілених системах. На цьому етапі проектна документація перетворюється на функціонуючу систему, інтегровану у корпоративну IT-інфраструктуру умовної організації. Основною метою є перевірка ефективності обраних рішень, оцінка стабільності роботи системи та відповідності вимогам безпеки. Важливо забезпечити не лише належну конфігурацію компонентів, а й контроль їхньої взаємодії в реальному середовищі. Тестування дозволяє виявити потенційні слабкі місця, оптимізувати налаштування та підвищити стійкість системи до кіберзагроз. При цьому враховуються такі аспекти, як продуктивність, відмовостійкість, сумісність із існуючими сервісами та зручність адміністрування. Умовна організація розглядається як підприємство середнього рівня з локальною мережею та декількома віддаленими офісами.

Етап 1. Підготовчий етап реалізації

Перед безпосередньою реалізацією обраних засобів захисту проводиться підготовка серверної та клієнтської інфраструктури. Встановлюються актуальні версії операційних систем та патчі безпеки, налаштовуються мережеві компоненти та базові політики безпеки. Для тестування формується ізольоване середовище (sandbox), що відтворює робочі умови організації без впливу на основні бізнес-процеси. Підготовка включає розробку документації з інструкціями щодо встановлення, налаштування та інтеграції програмного забезпечення. Наприклад, перед впровадженням OSSEC та Netwrix Backup проводиться налаштування серверів, підключення агентів на робочих станціях та перевірка з’єднання з центральним сервером управління. Такий підхід дозволяє контролювати процес впровадження та мінімізує ризики некоректної конфігурації.

Етап 2. Встановлення та налаштування засобів контролю доступу

Для реалізації контролю доступу використовується Apache Fortress. Центральний сервер управління виконує адміністрування ролей, політик доступу та правил паролів. На робочих станціях встановлюються агенти для перевірки аутентифікації. Користувачам призначаються ролі відповідно до їхніх функцій, а віддаленим співробітникам надається доступ через VPN з багатофакторною аутентифікацією (пароль + OTP-токен). Перевіряється коректність делегованого адміністрування, журналювання дій користувачів та відповідність політик безпеки корпоративним стандартам ([Жилін, с.104]). Регулярне тестування сценаріїв доступу дозволяє виявити помилки на ранньому етапі та скоригувати права доступу.

Етап 3. Впровадження засобів виявлення вторгнень (IDS/IPS)

OSSEC та Snort встановлюються на сервери та робочі станції для моніторингу подій та аналізу мережевого трафіку. Налаштовуються правила виявлення аномалій та порушень політик доступу. Усі інциденти централізовано передаються на сервер Prelude SIEM для кореляції та детального аналізу. Тестування включає проведення контрольованих атак, перевірку сповіщень та оцінку точності виявлення загроз. Додатково оцінюється вплив IDS/IPS на продуктивність серверів та мережі при високому навантаженні. Такий підхід забезпечує швидке виявлення підозрілих дій і мінімізує ризик пропуску критичних інцидентів.

Етап 4. Резервування та відновлення даних

Для забезпечення безперервності бізнес-процесів налаштовується Netwrix Backup для автоматичного резервного копіювання критичних даних. Резервні копії шифруються та зберігаються на окремих серверах або у хмарному середовищі. Тестування передбачає відновлення даних у тестовому середовищі та перевірку цілісності відновлених файлів ([Костюк, с.316]). Оцінюється час відновлення, відповідність процедур політикам безпеки та можливість автоматизації процесів. Це гарантує готовність організації до аварійних ситуацій та втрати даних.

Етап 5. Тестування взаємодії компонентів

Після встановлення засобів захисту проводиться тестування сумісності та взаємодії всіх компонентів системи. Перевіряється коректність роботи агентів, синхронізація логів із центральним сервером, а також сценарії одночасного доступу великої кількості користувачів. Виявлені конфлікти налаштовуються та документуються. Це забезпечує стабільність роботи системи у реальних умовах та попереджує збої під час пікових навантажень.

Етап 6. Аналіз результатів тестування

Після завершення тестування проводиться детальний аналіз ефективності впроваджених засобів. Розглядаються сповіщення про інциденти, результати резервного копіювання, відновлення даних та логування дій користувачів. На основі отриманих даних коригуються налаштування політик доступу та правил виявлення вторгнень. Це дозволяє підвищити точність системи та зменшити кількість помилкових спрацьовувань.

Етап 7. Оптимізація продуктивності

Для підтримки стабільної роботи системи оцінюється вплив засобів захисту на продуктивність серверів та робочих станцій. Вносяться зміни до правил моніторингу, частоти резервного копіювання та обробки логів. Використовуються методи балансування навантаження та пріоритезації завдань безпеки. Це дозволяє забезпечити високу доступність ресурсів і мінімізувати затримки у роботі користувачів.

Етап 8. Впровадження політики безпечного адміністрування

Адміністратори отримують обмежені права доступу та проходять навчання щодо правил безпечного адміністрування. Всі дії адміністраторів логуються та періодично аналізуються для запобігання внутрішнім загрозам. Впроваджується періодичний аудит та автоматичне оповіщення про критичні зміни конфігурацій. Такий підхід підвищує прозорість внутрішніх процесів і забезпечує відповідність корпоративним стандартам безпеки.

Етап 9. Перевірка сценаріїв реагування на інциденти

Система тестується у сценаріях імітації кібератак, порушень політик доступу та відмови сервісів. Оцінюється швидкість сповіщень, кореляція інцидентів та ефективність відновлення доступу. Це дозволяє виявити слабкі місця в процедурах реагування та усунути їх на етапі тестування, до початку експлуатації.

Етап 10. Документування та навчання персоналу

Всі етапи реалізації та тестування документуються: налаштування компонентів, результати тестів, виявлені помилки та способи їх усунення. Це забезпечує відтворюваність процесу та спрощує аудит безпеки. Додатково проводиться навчання користувачів та адміністраторів щодо правил роботи з системою, процедур доступу та дій у разі інцидентів, що підвищує загальну культуру кібербезпеки організації.

Реалізація та тестування обраних засобів захисту підтвердили ефективність запропонованого підходу. Всі компоненти системи працюють стабільно, інциденти виявляються та обробляються оперативно. Тестування дозволило оптимізувати налаштування, покращити продуктивність та забезпечити стабільність роботи розподіленої системи. Впровадження політики безпечного адміністрування та навчання персоналу підвищує загальний рівень кібербезпеки організації. Отримані результати демонструють доцільність застосування комплексного підходу до адміністрування компонентів захисту в умовах сучасної IT-інфраструктури.

3.4. Оцінка ефективності та рекомендації щодо вдосконалення

Оцінка ефективності засобів захисту інформації є критично важливим етапом управління безпекою розподілених систем. Метою цього підрозділу є визначення реальної продуктивності впроваджених механізмів, виявлення слабких місць та розробка рекомендацій для їх усунення. Ефективність оцінюється не лише за показниками безпеки, а й з урахуванням продуктивності системи, зручності адміністрування та впливу на бізнес-процеси. Правильне тестування дозволяє

забезпечити баланс між безпекою та функціональністю системи, мінімізувати ризики та оптимізувати ресурси організації. Умовна організація має кілька віддалених офісів та центральний сервер, що створює додаткові виклики щодо синхронізації засобів захисту та моніторингу.

Для оцінки ефективності системи застосовувалась комплексна методика, що включала функціональні, навантажувальні та сценарні тести. Функціональні тести перевіряли правильність роботи систем аутентифікації, контролю доступу та виявлення вторгнень. Навантажувальні тести дозволяли оцінити продуктивність системи під час пікових навантажень, а сценарні тести імітували кібератаки, помилки користувачів та відмови обладнання. Критеріями оцінки були швидкість реагування системи, точність сповіщень про інциденти, стабільність роботи компонентів та зручність адміністрування.

1. Контроль доступу (Apache Fortress)

Для контролю доступу використовується система Apache Fortress, яка реалізує принцип RBAC та багатофакторну аутентифікацію. Під час тестування оцінювалась коректність присвоєння ролей, швидкість реагування адміністратора та безпека делегованого адміністрування.

Переваги:

- Гнучке управління ролями та делегованим адмініструванням;
- Центральне управління політиками доступу;
- Підтримка багатофакторної аутентифікації для віддалених користувачів.

Недоліки:

- Складність налаштування політик для великої кількості користувачів;
- Необхідне додаткове навчання персоналу для коректного адміністрування.

Рекомендації щодо вдосконалення:

- Регулярне тестування сценаріїв доступу;
- Автоматизація налаштування ролей та політик паролів;
- Централізоване журналювання для моніторингу спроб доступу та потенційних конфліктів.

2. Системи виявлення вторгнень (OSSEC та Snort)

Впроваджено системи OSSEC та Snort для моніторингу мережевого трафіку та подій безпеки. Тестування включало контрольовані атаки, аналіз логів та перевірку сповіщень. Особлива увага приділялась інтеграції з Prelude SIEM для кореляції інцидентів.

Переваги:

- Моніторинг у реальному часі;
- Кореляція інцидентів через Prelude SIEM;
- Виявлення руткітів та аномальних підключень.

Недоліки:

- Велике навантаження на сервери при високому обсязі логів;
- Можливі хибні спрацьовування при некоректно налаштованих правилах.

Рекомендації щодо вдосконалення:

- Оптимізація правил виявлення;
- Використання фільтрів для зменшення хибних спрацьовувань;
- Регулярне оновлення сигнатур та правил.

3. Резервне копіювання та відновлення (Netwrix Backup)

Система резервного копіювання забезпечує автоматизацію процесу та шифрування даних. Тестування включало відновлення файлів у тестовому середовищі для перевірки цілісності.

Переваги:

- Автоматизація резервного копіювання;
- Шифрування та захист даних;
- Швидке відновлення у разі аварій.

Недоліки:

- Високі витрати на ліцензії;
- Потреба у регулярному тестуванні відновлення.

Рекомендації щодо вдосконалення:

- Використання багаторівневих резервних копій;

– Зберігання копій на окремих носіях та у хмарі;
– Регулярне тестування процесу відновлення ([Костюк, с.318]).

4. Продуктивність та навантаження

Для оцінки впливу системи на продуктивність тестували одночасний доступ великої кількості користувачів та обробку логів.

Переваги:

– Можливість обробляти велике навантаження;
– Балансування запитів зменшує затримки.

Недоліки:

– Інтенсивне логування може уповільнювати сервери;
– Часте резервне копіювання створює пікове навантаження.

Рекомендації:

– Оптимізація частоти моніторингу та обробки логів;
– Балансування навантаження та пріоритезація завдань.

5. Інтеграція компонентів

Синхронізація агентів та центрального сервера забезпечує кореляцію подій і централізоване управління.

Переваги:

– Кореляція подій в одному місці;
– Централізоване управління агентами.

Недоліки:

– Конфлікти версій ПЗ та агентів;
– Можливі проблеми сумісності з новими ОС.

Рекомендації:

– Уніфікація версій та регулярне оновлення компонентів;
– Налаштування пріоритетів обробки подій.

6. Аналіз логів та інцидентів

Централізоване зберігання логів дозволяє відстежувати повторювані загрози та помилки користувачів.

Переваги:

- Швидка ідентифікація проблем;
- Виявлення повторюваних загроз.

Недоліки:

- Пропуски критичних подій при недостатньому логуванні;
- Великий обсяг даних потребує ефективної системи аналізу.

Рекомендації:

- Централізоване логування та автоматичне сповіщення;
- Регулярний аналіз та коригування правил моніторингу.

Таблиця 3.3 - Основні компоненти та їх ефективність

Компонент	Переваги	Недоліки	Рекомендації для вдосконалення
Контроль доступу	Гнучкі ролі, багатофакторна аутентифікація	Складність налаштування, потреба у навчанні	Автоматизація ролей, централізоване ведення журналу
IDS/IPS	Моніторинг у реальному часі, кореляція подій	Велике навантаження, хибні спрацьовування	Оптимізація правил, оновлення сигнатур
Резервне копіювання	Автоматизація, шифрування, швидке відновлення	Високі витрати, потреба у тестуванні	Багаторівневі копії, хмарне зберігання
Продуктивність	Обробка великого навантаження	Уповільнення серверів, пікове навантаження	Балансування, пріоритезація завдань

Інтеграція компонентів	Централізоване управління	Конфлікти версій, сумісність з ОС	Уніфікація версій, пріоритезація обробки подій
Аналіз логів	Швидка ідентифікація проблем	Пропуски критичних подій, великий обсяг	Централізоване логування, регулярний аналіз

Проведена оцінка показала, що система адміністрування компонентів захисту забезпечує високий рівень безпеки для умовної організації. Однак для підвищення стійкості та надійності рекомендується:

- Регулярне тестування сценаріїв доступу та правил IDS/IPS;
- Автоматизація процедур реагування та резервного копіювання;
- Централізоване управління логами та моніторингом подій;
- Оптимізація продуктивності шляхом балансування навантаження;
- Спрощення інтерфейсів адміністрування та навчання персоналу;
- Планові аудити та перевірки сумісності компонентів.

Виконання цих рекомендацій дозволяє підвищити точність виявлення інцидентів, забезпечити безперервність бізнес-процесів та знизити ризики внутрішніх і зовнішніх загроз.

ВИСНОВКИ

У ході дослідження було досягнуто поставленої мети - розроблено науково-обґрунтовані методи та рекомендації щодо адміністрування компонентів захисту інформації в розподілених комп'ютерних системах, враховуючи сучасні загрози та технологічні вимоги. Проведена робота дозволила комплексно оцінити як теоретичні аспекти, так і практичні механізми забезпечення безпеки, що забезпечує основу для подальшого впровадження та експлуатації систем захисту у реальних організаціях.

В рамках виконання першого завдання було визначено типові компоненти розподілених систем, їх взаємодію, а також ключові фактори впливу на безпеку, такі як складність архітектури та кількість віддалених вузлів. Результатом стало формування чіткої концептуальної моделі умовної організації для практичної частини проєкту.

Друге завдання полягало в аналізі загроз та вразливостей інформаційних ресурсів у розподіленому середовищі. Було проведено класифікацію потенційних атак, виявлено критичні ресурси та розроблено матрицю ризиків, яка включала внутрішні та зовнішні загрози. Зокрема, досліджено ймовірність несанкціонованого доступу до фінансових даних, персональної інформації співробітників та внутрішньої документації. Це дозволило сформувати пріоритети при виборі засобів контролю доступу та моніторингу.

Третє завдання стосувалося розгляду принципів і моделей захисту інформації, нормативно-правових та стандартних вимог. Було детально вивчено RBAC, ABAC та інші моделі контролю доступу, а також принципи криптографічного захисту та резервування. Аналіз нормативних документів і стандартів, таких як XACML, SAML, PCI-DSS, GDPR та HIPAA, дозволив забезпечити відповідність обраних рішень сучасним вимогам безпеки.

Четверте завдання передбачало вивчення методів та засобів адміністрування систем керування доступом, моніторингу та резервування. На цьому етапі було розглянуто практичні програмні рішення - Apache Fortress для контролю доступу, OSSEC та Snort для виявлення вторгнень, Netwrix Backup для резервного

копіювання та Quattor для централізованого адміністрування конфігурацій. Проведено детальний аналіз «за» і «проти» кожного компонента, що дозволило оцінити їх ефективність у рамках умовної організації.

П’яте завдання полягало в розробці практичних рекомендацій щодо впровадження та тестування засобів захисту в умовній організації. Було створено багаторівневу архітектуру системи з центральним сервером управління, агентами на робочих станціях та інтеграцією віддалених офісів через VPN. Налаштовано ролі та права доступу, впроваджено багатофакторну аутентифікацію, встановлено засоби моніторингу та резервного копіювання. Проведено тестування взаємодії компонентів, симуляції атак та контрольовані сценарії відмови, що дозволило оцінити стійкість та продуктивність системи.

Шосте завдання полягало в оцінці ефективності запропонованих методів та наданні рекомендацій щодо вдосконалення. Було виконано комплексне тестування функціональності, продуктивності та реагування на інциденти. Результати показали, що система забезпечує високий рівень безпеки, проте потребує регулярного оновлення правил IDS/IPS, оптимізації логів та автоматизації процедур реагування та резервного копіювання.

У ході дослідження також здійснено детальний аналіз продуктивності системи. Було виявлено, що інтенсивне логування та резервне копіювання можуть створювати пікові навантаження, але застосування методів балансування та пріоритезації завдань дозволяє підтримувати стабільність роботи серверів та робочих станцій без значного впливу на бізнес-процеси.

Особливу увагу приділено навчання персоналу та зручності адміністрування. Було розроблено рекомендації щодо централізованого моніторингу, спрощених інтерфейсів, делегування прав та регулярного аудиту дій адміністраторів. Це дозволяє мінімізувати ризики внутрішніх загроз та підвищити прозорість управління безпекою.

Загальні висновки підтверджують, що реалізація комплексного підходу до адміністрування компонентів захисту інформації у розподілених системах забезпечує надійність та безперервність бізнес-процесів. Впровадження

багаторівневої архітектури, інтеграція IDS/IPS, централізоване управління конфігураціями та регулярне резервне копіювання дозволяють швидко реагувати на загрози та відновлювати критичні ресурси.

Таким чином, виконання всіх поставлених завдань дозволило досягти мети дослідження - розроблено науково-обґрунтовані методи та практичні рекомендації щодо адміністрування компонентів захисту інформації. Результати роботи можуть бути застосовані у середніх та великих організаціях для підвищення рівня кібербезпеки, оптимізації ресурсів та забезпечення стабільної роботи розподілених комп’ютерних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамова А. О. Мережі обміну даними. Комп’ютерний практикум. Київ, 2021. С. 125.
2. Бантюков С. Є., Бізюк І. Г., Казанко О. В. Серія Комп’ютерні науки: мережеві інформаційні технології. 2024. С. 42-49.
3. Бурячок В. Л., Толюпа С. В., Семко В. В., Бурячок Л. В., Складанний П. М., Лукова-Чуйко Н. В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ: ДУТ-КНУ, 2016. 178 с.
4. Гайдур Г. І., Бондаренко З. З. Теорія інформації та кодування: навчальний посібник. Київ: ДУІКТ, 2024. 43 с.
5. Гайдур Г. І., Бондаренко З. З., Марченко В. В., Чумак Н. С. Лабораторний практикум з навчальної дисципліни «Теорія інформації та кодування»: навч. посібник. Київ: ДУТ, ННІЗІ, 2021. 50 с.
6. Гармаш Р. С. Моделювання продуктивності проміжних вузлів комп'ютерної мережі. *СтудВісник Тернопільського фахового коледжу ТНТУ*. 2023. С. 16.
7. Глобенко В. В. Дослідження та програмна реалізація системи моніторингу LAN мереж інформаційних та комп’ютерних систем. *Збірник наукових праць.* 2022. Т. 2, № 38. С. 125-132.
8. Гур’єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави: навч. посіб. Ніжин: ФОП Лук’яненко В. В. ТПК «Орхідея», 2018. 166 с.
9. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
10. Закон України «Про внесення змін щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/main/4336-20

11. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80
12. Засоби керування корпоративними мережами та застосунками. URL: https://compress.ru/article.aspx?id=12065
13. Класифікація та характеристики розподілених систем. URL: https://elib.lntu.edu.ua/sites/default/files/elib_upload/123%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%20%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F/page13.html
14. Костюк Ю. В., Складанний П. М., Гулак Г. М., Бебешко Б. Т., Хорольська К. В., Рзаєва С. Л. Системи захисту інформації: підручник. Київ: Київський столичний університет імені Бориса Грінченка, 2025. 887 с.
15. Крижановський В. Г., Сергієнко С. П. Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник. Вінниця: ДонНУ імені Василя Стуса, 2019. 36 с.
16. Курбан О. В. Основи сучасної національної інформаційної безпеки України. Вісник ХДАК. 2017. Вип. 50. С. 55-62.
17. Кучма І. М. Методи та засоби моделювання процесів управління та моніторингу у комп'ютерних мережах: дис. Тернопільський національний технічний університет імені Івана Пулюя, 2023.
18. Лунгол О. М., Агішева А. В. Технології створення та застосування систем захисту інформаційно-комунікаційних систем. *Topical aspects of modern scientific research. Proceedings of the 2nd Int. scient, and practical conference. CPN Publishing Group*, Tokyo, Japan, 2023. С. 255-260.
19. Лунгол О., Агішева А. Використання технології Deception у боротьбі з кіберзагрозами. *Кібербезпека в Україні: правові та організаційні питання: матеріали Міжн. наук.-практ. конф*. Одеса: ОДУВС, 2023. С. 75-76.
20. Лунгол О., Макаринська А. Кіберзлочинність як складова інформаційної війни: аналіз досвіду України. *Всеукраїнська науково-практична конференція*

«Сучасні пріоритети розвитку України: економічна та інформаційна безпека», 2023. Дніпро. С. 84-86.

21. Лунгол О., Макаринська А. Сучасні методи виявлення та аналізу соціально-інженерних атак в інформаційних системах. *Тези доповідей ІІ Міжнародної науково-практичної конференції «Інновації та перспективні шляхи розвитку інформаційних технологій»*, 2023. Черкаси. С. 243-244.
22. Лунгол О., Торгало П. Аналіз та управління ризиками в сфері інформаційної безпеки. *ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій»,* 2023. Черкаси. С. 57-61.
23. Лунгол О., Шаєц Є. Кіберпростір як квінтесенція глобалізованого суспільства. *Регіональні особливості злочинності: сучасні тенденції та стратегії протидії: ІІІ Всеукр. Наук.-практ. конф*., 2023. Кривий Ріг. С. 92-94.
24. Луцків А. М. Особливості функціонування та класифікації розподілених систем зберігання даних. *Матеріали XII Міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», 6-7 грудня 2023 р.* Тернопіль: ФОП Паляниця В. А., 2023. С. 455.
25. Маліновський В. І. Аналіз надійності функціонування сучасних пристроїв і систем Інтернету речей. *II International Scientific and Practical Conference "Modern research in World Science"*, 2022. URL: https://sci-conf.com.ua/wpcontent/uploads/2022/06/MODERN-RESEARCH-IN-WORLD-SCIENCE-12-14.06.22.pdf
26. Маліновський В. І. Аналіз ризиків кіберзагроз і захист даних в сучасних системах Інтернету речей. *Матеріали LI-ї Науково-технічної конференції ФІТКІ.* ВНТУ, 2022. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/14999
27. Маліновський В. І. Сучасні кіберзагрози і захист даних в системах і пристроях Інтернету речей. *Міжнародна наукова Інтернет-конференція*

"Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення", випуск 69, 2022. URL: http://www.konferenciaonline.org.ua

28. Маліновський В. І., Куперштейн Л. М., Лукцічев В. І. Підходи підвищення інформаційного захисту даних в каналах мережах IoT. *Міжнародна Інтернет-конференція «Світ наукових досліджень», випуск 20*, 2023. URL: http://www.konferenciaonline.org.ua/ua/article/id-595/
29. Мухін В. Є., Завгородній В. В., Завгородня Г. А. Інформаційна безпека та гібридні загрози: навчальний посібник. Київ: ТОВ «ТРОПЕА», 2024. 104 с. URL: https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/scientific-publications/monographs/information_security_and_hybrid_threats.pdf
30. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека». Тернопіль: ТНЕУ, 2019. 119 с.
31. Основні функції керування комп'ютерною мережею. URL: https://eopearhiiv.edu.ee/e-kursused/eucip/haldus_vk/611___.html
32. Палко Д. Інтелектуальні моделі оцінки ризиків кібербезпеки в розподілених системах на основі нейромережевого підходу. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 3, № 27. С. 429-448. https://doi.org/10.28925/2663-4023.2025.27.764
33. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-теелекомунікаційних системах». URL: https://www.kmu.gov.ua/npas/32791826
34. Сагун А. В., Бобков В. Б. Операційні системи та комп'ютерні мережі: навч. посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. С. 164.
35. Складанний П. М., Гулак Г. М., Корнієць В. А. Коаліційний підхід до управління кібербезпекою інформаційних систем, що застосовують хмарні технології. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 28, № 4. С. 8-25.

36. Соколовський С. О., Козін М. В., Партика С. О. Вразливість комп'ютерних мереж. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доп. 13-ї міжнар. наук.-техн. конф., 26-27 квітня 2023 р*., Баку–Харків–Жиліна. Т. 2. С. 74-75.
37. Сопілко І. М. Становлення мережевого суспільства та питання кібербезпеки. *Юридичний вісник*. 2016. № 1 (38). С. 79-85.
38. Сторчак А. С., Самойлов І. В. Використання OSINT-технології в сучасних сервісах. Комплексне забезпечення якості технологічних процесів та систем, 2023. С. 300.
39. Цуркан І. О., Шимко А. О., Верзілов М. Р., Стецик Р. М. Використання методу OSINT під час дії правового режиму воєнного стану в Україні. *6th International scientific and practical conference European congress of scientific achievements,* 2024. С. 222.
40. Цяпа С. М. Загрози та вразливості кібербезпеки в мережевих та автономних транспортних системах. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* 2024. Т. 35 (74), № 6. С. 244-250.
41. Чубаєвський В., Богма О., Сілакова Г. Методика оцінки ефективності систем захисту корпоративної інформації вітчизняних підприємств. *Економічний простір.* 2022. № 177. С. 56-61.
42. Anyshchenko O. Щодо питання передачі та збереження масивів графічних даних у глобальних і локальних мережах. *Computer-integrated technologies: education, science, production*. 2021. № 44. С. 87-93.
43. Art of BA. Main types of software architecture. URL: https://www.artofba.com/uk/post/main-types-of-software-architecture
44. Budapest Convention on Cybercrime. URL: https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime
45. Drahuntsov R., Rabchun D., Brzhevska Z. Принципи забезпечення безпеки архітектури інформаційної системи на базі клієнтських додатків для ОС Android. *Кібербезпека: освіта, наука, техніка*. 2020. Т. 4, № 8. С. 49-60. https://doi.org/10.28925/2663-4023.2020.8.4960

46. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). URL: https://www.hybridcoe.fi/
47. Joerg Z. Architecture of Interoperable Information Systems - An enterprise Model-based Approach for Describing and Enacting Collaborative Business Processes. 2012. P. 1-3.
48. Network Security Toolkit. URL: https://en.wikipedia.org/wiki/Network_Security_Toolkit
49. Prelude SIEM. URL: https://en.wikipedia.org/wiki/Prelude_SIEM
50. Snort (програмне забезпечення). URL: https://en.wikipedia.org/wiki/Snort_%28software%29
51. Studfile. Page 5. URL: https://studfile.net/preview/14517464/page:5/
52. Tkadhov V., Kovalenko A., Fesenko T. Оптимізація мережного алгоритму функціонування комп'ютерних мереж підвищеної живучості на мобільній платформі. *Системи управління, навігації та зв'язку*. 2021. Т. 3, № 65. С. 143-147.
53. Vasylkivskyi M. V. Динамічна інформаційна мережа із вбудованим штучним інтелектом. *Computer-integrated technologies: education, science, production*. 2023. № 50. С. 36-45.

ДОДАТКИ

Додаток А

Порівняння RBAC та ABAC

Критерій	RBAC (Role-Based Access Control)	ABAC (Attribute-Based Access Control)
Основний принцип	Доступ визначається роллю користувача	Доступ визначається атрибутами (користувача, ресурсу, дії, середовища)
Приклад правила	«Адміністратор має право видаляти файли»	«Працівники відділу кадрів можуть переглядати дані співробітників лише у робочий час з корпоративних пристроїв»
Рівень деталізації	Узагальнений, орієнтований на ролі	Високоточний, залежний від контексту
Гнучкість	Статичні ролі, рідко змінюються	Динамічний доступ, що перевіряється у режимі реального часу
Сфера застосування	ERP, CRM, корпоративні системи	Хмарні сервіси, мультидоменні системи, Zero Trust

Додаток Б.

Приклади застосування ABAC у різних сферах

Галузь	Сценарій	Правило ABAC	Результат
Охорона здоров'я	Лікар отримує доступ до медичної картки пацієнта	Надати доступ, якщо: *user.role = doctor*, *user.department = cardiology*, *resource.type = patient_record*, *access_time = робочі години*	Лікар бачить записи лише свого відділення у робочий час
Банківська справа	Менеджер банку схвалює транзакцію	Дозволити, якщо: *user.title = branch_manager*, *resource.amount ≥ 50 000*, *user.branch = resource.origin_branch*, *request_time = робочі години*	Зменшення ризику шахрайства, перевірка контексту
E-commerce	Агент підтримки переглядає історію замовлень	Надати доступ, якщо: *user.department = support*, *resource.type = orders*, *device.company_owned = true*	Обмеження перегляду лише з корпоративних пристроїв
Державний сектор	Офіцер отримує доступ до секретного звіту	Дозволити доступ, якщо: *user.clearance_level ≥ document.classification_level*, *user.agency = document.owning_agency*, *device.is_encrypted = true*	Захист секретних документів на основі рівня допуску та середовища

Додаток В.

Відповідність ABAC моделі Zero Trust

Принцип Zero Trust	Реалізація в ABAC	Приклад
Мінімальні привілеї	Доступ надається лише за необхідності й лише до конкретних ресурсів	Працівник може редагувати лише свої документи, але не колег
Контекстна перевірка	Враховуються час, місцезнаходження, пристрій	Доступ дозволено лише з корпоративного ноутбука у робочі години
Постійна перевірка	Перевірка прав кожного запиту	Якщо користувач змінює місцезнаходження, система повторно перевіряє доступ
Масштабованість	Автоматичні політики, адаптовані до динамічного середовища	Підтримка хмарних сервісів з великою кількістю користувачів

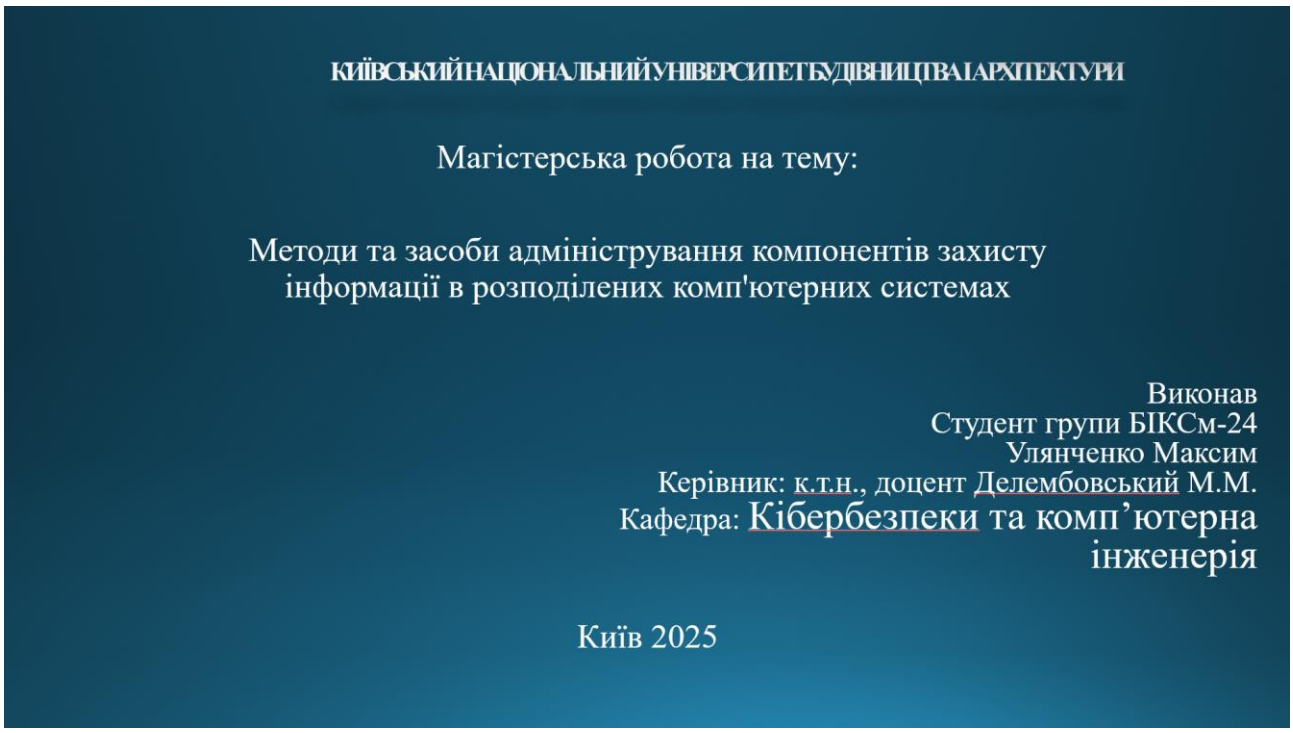
Додаток Г

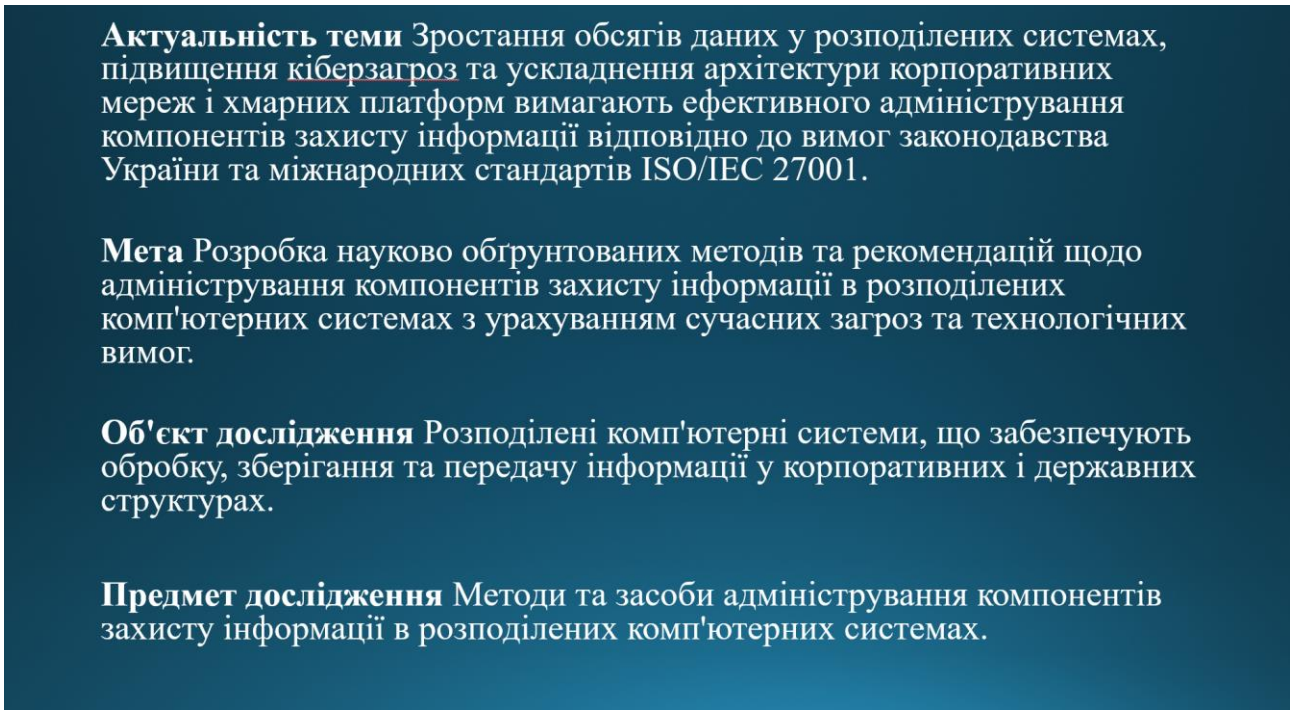
Інструменти Netwrix для підтримки ABAC

Інструмент	Призначення	Роль у впровадженні ABAC
Netwrix Auditor	Аудит доступу та дій користувачів	Забезпечує прозорість і допомагає формувати політики ABAC
UEBA (User and Entity Behavior Analytics)	Аналіз поведінки користувачів	Виявляє аномалії, які можуть сигналізувати про порушення політик ABAC
Endpoint Policy Manager	Управління політиками на різних платформах	Підтримує узгодженість політик ABAC у мультисередовищах
Identity Manager	Управління ідентичністю та доступом	Автоматизує розподіл прав доступу та усуває надлишкові привілеї
Compliance Reporting	Формування звітів відповідності	Демонструє дотримання нормативних вимог при використанні ABAC

Додаток Д

Презентація





Завдання

- Дослідити теоретичні основи розподілених комп'ютерних систем, їх класифікацію та особливості функціонування.
- Проаналізувати загрози та вразливості інформаційних ресурсів у розподіленому середовищі.
- Розглянути принципи та моделі захисту інформації, існуючі нормативно-правові та стандартні вимоги.
- Вивчити методи та засоби адміністрування систем керування доступом, криптографічного захисту, моніторингу та резервування.
- Розробити практичні рекомендації щодо впровадження та тестування засобів захисту в умовній організації.
- Оцінити ефективність запропонованих методів та надати рекомендації щодо вдосконалення систем безпеки.

Методи

- аналітичний та порівняльний аналіз літературних джерел;
- системний та моделювальний підходи до вивчення компонентів безпеки;
- методи проектування та тестування інформаційних систем;
- експертні оцінки та методи управління ризиками.

Обсяг роботи

- Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи – 85 сторінок, кількість використаних джерел – 53, кількість таблиць - 22, кількість рисунків - 8

ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

Поняття та класифікація розподілених комп'ютерних систем

- У наукових працях підкреслюється, що головними ознаками РКС є незалежність вузлів, гетерогенність ресурсів та можливість взаємодії через стандартизовані протоколи. Таким чином, вивчення принципів організації та класифікації РКС є ключовим для побудови надійних та захищених інформаційних систем.

Класифікація

Критерій класифікації	Типи систем	Основні характеристики
Рівень розподілу ресурсів	Локальні, глобальні, гібридні	Визначають масштаби обробки та управління ресурсами
Тип управління	Централізоване, децентралізоване, кооперативне	Впливає на надійність та швидкодію
Топологія мережі	Зіркова, кільцева, сітчаста, змішана	Визначає стратегії резервування і маршрутизації
Спосіб взаємодії вузлів	Синхронна, асинхронна	Впливає на передбачуваність та масштабованість обробки
Функціональне призначення	Обчислювальні, файлові, інформаційно-аналітичні, сервісні	Визначає методи захисту та алгоритми управління

Загрози та вразливості інформаційних ресурсів у розподіленому середовищі

Класифікація загроз та вразливостей інформаційних ресурсів у розподілених середовищах

Тип загрози	Джерело загрози	Вплив на ресурси	Приклади атак
Апаратні	Фізичні фактори, збої обладнання	Доступність, цілісність	Вихід з ладу серверів, пожежа
Програмні	Вразливості ПЗ, шкідливий код	Конфіденційність, цілісність	Віруси, експлойти, руткіти
Комунікаційні	Мережеві протоколи, перехоплення	Конфіденційність, доступність	MITM, DDoS, перехоплення пакетів
Соціальна інженерія	Працівники, користувачі	Конфіденційність	Фішинг, маніпуляції

Принципи та моделі захисту інформації

Принцип	Модель реалізації	Приклад застосування
Мінімальних привілеїв	Ролевий контроль доступу, ABAC	Корпоративні мережі, хмарні сервіси
Багаторівневий доступ	Белл–Лападула, Біббі–Ден	Військові та державні системи
Розподілена відповідальність	Групові політики, розподілений аудит	Фінансові системи, банківські додатки
Аутентифікація	Одно- та багатофакторна, токени, біометрія	Корпоративні VPN, системи онлайн-банкінгу
Шифрування	AES, RSA, TLS, цифровий підпис	Захист каналів передачі даних
Цілісність	Хеш-функції, контрольні суми, цифровий підпис	Фінансові транзакції, медичні дані
Доступність	Резервування, балансування навантаження, аварійне відновлення	Дата-центри, хмарні сервіси

Нормативно-правове забезпечення захисту інформації в Україні та міжнародні стандарти

Стандарт / Організація	Основна мета	Приклад застосування
ISO/IEC 27001	Система управління інформаційною безпекою (ISMS)	Впровадження комплексної політики безпеки у корпорації
ISO/IEC 27002	Керівництво щодо заходів безпеки	Встановлення процедур контролю доступу та шифрування даних
Закон України «Про захист інформації в інформаційно-комунікаційних системах»	Загальні принципи безпеки, права та обов'язки, категорії інформаці	Встановлення базових вимог до організації технічних, програмних і процедурних заходів безпеки
Закон України № 4336-IX	Розширення компетенції органів влади у сфері кібербезпеки, моніторинг загроз та обробка інцидентів	Правові основи для сертифікації та акредитації інформаційних систем
Постанова КМУ № 373	Деталізація порядку організації доступу, логування подій, оцінки ризиків та класифікації систем	Встановлення обов'язкових процедур резервного копіювання та відновлення даних
ISO/IEC 27005	Управління ризиками інформаційної безпеки	Оцінка загроз та розробка планів реагування на інциденти
NIST Cybersecurity Framework	Управління кіберризиками у корпоративних системах	Впровадження стандартів моніторингу та реагування на кібератаки
COBIT	Управління IT та інформаційною безпекою	Структуризація процесів управління та контролю інформаційних ресурсів
ENISA (European Union Agency)	Розробка методологій та рекомендацій для кібербезпеки	Моніторинг загроз та впровадження систем раннього попередження
Budapest Convention on Cybercrime	Протидія міжнародним кіберзлочинам	Координація міжнародного розслідування кіберзлочинів та обмін доказами

МЕТОДИ ТА ЗАСОБИ АДМІНІСТРУВАННЯ КОМПОНЕНТІВ ЗАХИСТУ ІНФОРМАЦІЇ

Системи керування доступом у розподілених комп'ютерних системах

Модель доступу	Основні характеристики	Приклади застосування
Дискреційна (DAC)	Власник ресурсу визначає права доступу, гнучка, проста	Локальні файлові системи, корпоративні мережі
Мандатна (MAC)	Центральне управління політиками, високий рівень безпеки	Військові та державні інформаційні системи
Рольова (RBAC)	Права прив'язуються до ролей, зручне адміністрування	Корпоративні ERP та CRM системи
Атрибутна (ABAC)	Контроль доступу на основі атрибутів користувачів та ресурсів	Хмарні сервіси, мультидоменні системи

Адміністрування засобів криптографічного захисту та управління ключами

Адміністрування засобів криптографічного захисту та управління ключами є ключовим аспектом забезпечення безпеки інформаційних ресурсів у сучасних розподілених системах.
Основна мета криптографічного адміністрування полягає у гарантуванні конфіденційності, цілісності та достовірності даних під час їх зберігання та передачі між вузлами мережі.

Алгоритми шифрування

Засіб	Призначення	Приклад
Симетричне шифрування	Шифрування даних у великих обсягах	AES-256
Асиметричне шифрування	Захист каналів та цифровий підпис	RSA, ECC
Управління ключами	Контроль та ротація ключів	HSM, KMS

Системи централізованого управління ключами

Центральний сервер ключів	• Генерація, розповсюдження та зберігання ключів
Модуль політик	• Контроль доступу на основі ролей
Аудиторський модуль	• Моніторинг та журналювання використання ключів

Адміністрування криптографічного захисту

Технологія	Призначення	Переваги
HSM	Аппаратне зберігання ключів	Підвищена безпека, сертифікація
TPM	Захищене зберігання ключів на кінцевих пристроях	Інтеграція з ОС, апаратна автентифікація

Програмні рішення для управління ключами

Рішення	Особливості	Інтеграція
KMS	Автоматизація життєвого циклу ключів	Хмарні та локальні системи
Vault	Централізоване управління секретами	Підтримка API для додатків

Методи багаторівневої автентифікації та управління ролями

Механізм	Призначення	Переваги
MFA	Багатофакторна автентифікація	Підвищення безпеки доступу
RBAC	Управління ролями	Контроль привілеїв користувачів

Поєднання апаратних та програмних засоби для забезпечення комплексної безпеки

Засіб	Функція	Переваги
HSM + KMS	Комплексне управління ключами	Надійний захист, автоматизація процесів
MFA + RBAC	Контроль доступу	Мінімізація людського фактору, підвищення безпеки

Інструменти моніторингу, виявлення вторгнень та реагування на інциденти

Системи моніторингу мережевого трафіку

Система	Основна функція	Переваги	Обмеження
Wireshark	Аналіз пакетів	Деталізація, безкоштовна	Потребує знань мереж
Tshark	Консольний аналізатор трафіку для автоматизованого моніторингу	Інтеграція зі скриптами, експорт у різні формати, віддалений захват	Відсутність GUI, потребує знання синтаксису команд
TCPdump	Швидкий захват та базова фільтрація мережевих пакетів	Мінімальні системні вимоги, стандарт для Unix/Linux, надійність	Обмежений аналіз протоколів, відсутність декодування додатків

Системи IDS/IPS

Система	Тип	Переваги	Обмеження
Snort	IPS	Відкрите ПЗ, сигнатурна система	Складність конфігурації
Suricata	IDS/ IPS	Висока продуктивність, підтримка багатопоточності	Вимагає ресурсів CPU

Інструменти аналізу журналів подій

Система	Основна функція	Переваги	Обмеження
Splunk	Кореляція та аналіз логів	Потужний аналітичний інструмент	Висока вартість
Graylog	Централізоване зберігання	Гнучка настройка, безкоштовна	Потребує адміністрування

SIEM-системи

Система	Основна функція	Переваги	Обмеження
Prelude SIEM	Моніторинг подій та кореляція	Відкрите ПЗ, модульна структура	Потребує навчання персоналу
IBM QRadar	Аналіз загроз і інцидентів	Потужний аналітичний інструмент	Висока вартість

Інструменти автоматизованого реагування

Система	Основна функція	Переваги	Обмеження
Demisto	Автоматизація інцидентів	Швидке реагування	Вартість ліцензії
Splunk Phantom	Оркестрація та автоматизація	Інтеграція з SIEM	Потребує налаштування

Інструменти аналізу поведінки користувачів

Інструмент	Основна функція	Переваги	Недоліки	Де застосовуються
Exabeam	Аналіз поведінки користувачів (UEBA)	Добре виявляє внутрішні загрози та компрометовані акаунти	Потребує навчання й налаштування моделей	SOC-центри, великі організації, банки, компанії з високими вимогами до безпеки доступу
Varonis	Моніторинг доступу та активності до даних	Деталізована аналітика, кореляція подій, фокус на захисті даних	Висока вартість впровадження та підтримки	Організації з великими масивами даних (файлові сервери, NAS, SharePoint), компанії, що захищають конфіденційні дані

Засоби резервування, відновлення та безпечного адміністрування

Види резервного копіювання даних

Вид резервування	Сутність копіювання	Переваги	Недоліки / обмеження
Повне	Копіюються усі дані	Максимальна надійність; повний образ	Потребує великого обсягу пам'яті; тривалий час створення копії
Диференційне	Копіюються усі зміни з моменту останньої повної	Швидке відновлення; менший обсяг, ніж повне	Для відновлення потрібна остання повна копія; обсяг з часом зростає
Інкрементальне	Копіюються лише нові та змінені файли з останньої будь-якої (повної/інкр.) копії	Мінімальний обсяг збережених даних; економія місця та часу на копіювання	Відновлення складніше й довше, бо потребує ланцюжка копій

Стратегії відновлення даних

Стратегія відновлення	Опис	Переваги	Обмеження / особливості
Локальне відновлення	Відтворення даних з копій, що зберігаються на локальних носіях (сервер, стрічка, NAS)	Висока швидкість доступу; не залежить від Інтернету	Уразливість до фізичних пошкоджень, крадіжки чи відмови обладнання
Відновлення з хмарного сховища	Дані відновлюються з хмар них сервісів резервування	Захист від фізичних загроз; гнучкий доступ з різних локацій	Залежність від каналу зв'язку; вартість хмарних ресурсів
Відновлення на віддалених серверах	Використання резервних майданчиків / дата-центрів	Підходить для великих корпоративних систем; висока відмовостійкість	Складність інфраструктури; потреба в детальному плануванні та тестуванні

Управління доступом

Елемент адміністрування	Функції	Переваги	Приклад
Контроль доступу	Обмеження прав	Зменшення ризиків	RBAC
Аудит подій	Моніторинг дій	Виявлення атак	SIEM
Логування	Збір даних	Аналіз інцидентів	Syslog

Інструменти резервування та відновлення

Засіб / технологія	Призначення	Переваги	Особливості використання
Veeam	Резервне копіювання та відновлення віртуальних, фізичних і хмарних середовищ	Автоматизація процесів; висока швидкість роботи з великими обсягами даних	Інтегрується з різними платформами; потребує налаштування політик резервування
Acronis	Резервне копіювання, відновлення, захист кінцевих пристроїв і серверів	Підтримка різних ОС і носіїв; можливість хмарного резервування	Необхідне навчання персоналу та дотримання політик безпеки
RAID-масиви (1, 5, 10)	Апаратна/програмна надлишковість дисків для підвищення надійності та продуктивності	Безперервний доступ до даних при відмові диска; підвищення швидкодії (залежно від рівня)	Не замінює резервне копіювання; вимагає правильного вибору рівня RAID та моніторингу стану дисків
Хмарні сервіси резервування	Зберігання копій у віддаленій інфраструктурі провайдера	Захист від фізичних загроз; масштабованість	Залежність від мережі й постачальника послуг; важливі шифрування та політики доступу

ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДІВ АДМІНІСТРУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Аналіз існуючих програмних рішень для адміністрування безпеки в розподілених системах

Основними завданнями безпеки в розподілених системах є: забезпечення аутентифікації та авторизації користувачів, захист даних під час передачі та зберігання, моніторинг та виявлення загроз, а також реагування на інциденти безпеки. Ці аспекти вимагають використання спеціалізованих програмних рішень, які інтегруються з існуючою інфраструктурою та відповідають вимогам безпеки.

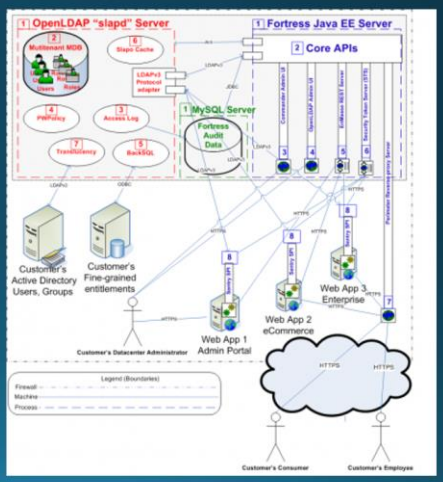
Основні аспекти безпеки в розподілених системах

- Забезпечення аутентифікації користувачів
- Забезпечення авторизації користувачів
- Захист даних під час передачі
- Захист даних під час зберігання
- Моніторинг загроз та подій безпеки
- Виявлення вторгнень та аномальної активності
- Реагування на інциденти безпеки
- Інтеграція спеціалізованих програмних рішень у існуючу інфраструктуру

Apache Fortress

- Apache Fortress є системою управління доступом на основі ролей (RBAC), яка дозволяє централізовано визначати права користувачів у великих інформаційних системах.
- Система інтегрується з LDAP-каталогами, що дозволяє використовувати існуючі облікові записи та зменшує витрати на адміністрування.
- Apache Fortress надає можливість встановлення політик паролів та обмежень доступу, що підвищує рівень безпеки. Крім того, вона дозволяє логувати всі операції доступу, що полегшує аудит і аналіз інцидентів безпеки.

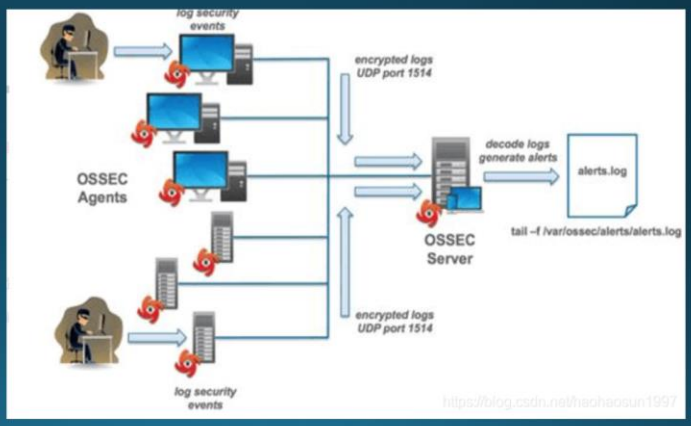
Архітектурне бачення Apache Fortress



OSSEC

- OSSEC є системою виявлення вторгнень на основі хостів (HIDS), призначеною для моніторингу безпеки серверів та кінцевих пристроїв.
- Аналізує журнали подій, перевіряє цілісність файлів і виявляє руткіти.
- Підтримує конфігурацію правил для відстеження специфічних загроз і аномалій у поведінці користувачів.
- OSSEC інтегрується з платформами SIEM, що забезпечує централізований контроль безпеки і спрощує аудит.
- Підтримує різні операційні системи, включаючи Linux, Windows та macOS.

Система OSSEC



PERMIS

PERMIS – це система управління доступом на основі атрибутів (ABAC), яка дозволяє встановлювати права користувачів за допомогою політик у форматі XML.

- Дозволяє використовувати стандарти SAML і XACML
- Забезпечує централізоване адміністрування політик без необхідності змінювати код застосунків
- Забезпечує сумісність із різними операційними системами та платформами розподілених систем

Quattor

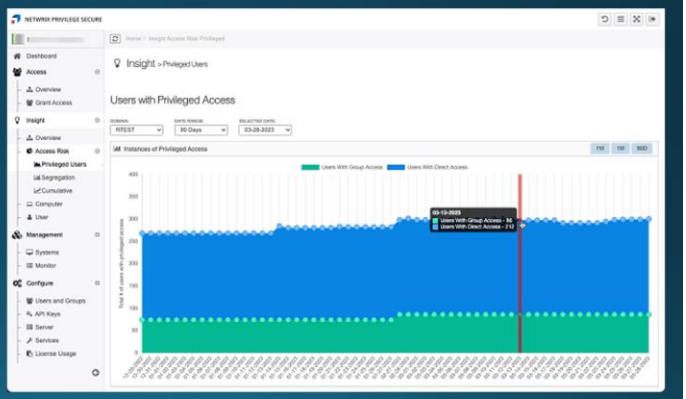
Quattor є набором інструментів для автоматизації конфігурації та управління великими розподіленими інфраструктурами.

- Дозволяє централізовано керувати конфігураціями серверів, мережевого обладнання
- Quattor дозволяє автоматично застосовувати конфігурації, зменшуючи ймовірність людських помилок та підвищуючи надійність системи.
- Забезпечує сумісність із різними операційними системами та платформами розподілених систем

Netwrix

Netwrix є платформою для аудиту та моніторингу змін у гібридних середовищах, що дозволяє виявляти порушення політик безпеки

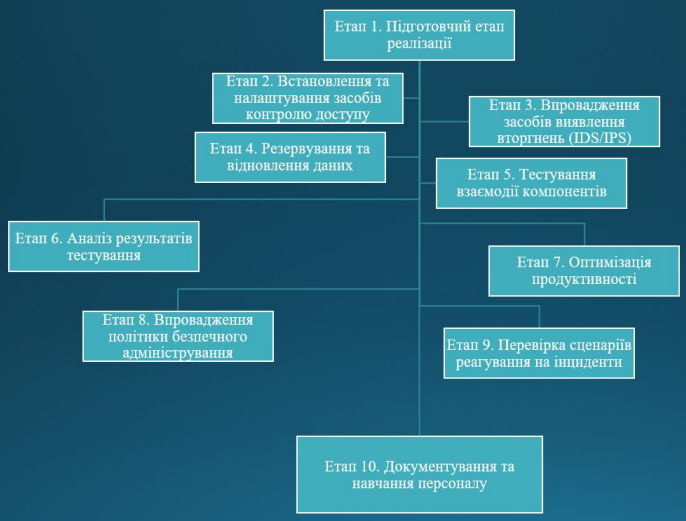
- Відстежує доступ до файлів, налаштувань систем, баз даних та облікових записів, надаючи детальні звіти про активність користувачів.
- Дозволяє централізовано керувати аудитом, забезпечуючи видимість всіх змін у корпоративній інфраструктурі.
- Netwrix підтримує відповідність нормативним вимогам, таким як GDPR, HIPAA і PCI DSS.



Проектування системи адміністрування компонентів захисту для умовної організації

1. Аналіз бізнес-процесів та IT-інфраструктури
2. Визначення критичних ресурсів та загроз
3. Формування політик безпеки
4. Проєктування архітектури системи
5. Впровадження контролю доступу (RBAC, 2FA)
6. Інтеграція засобів виявлення вторгнень (IDS/IPS)
7. Організація резервного копіювання і відновлення
8. Налаштування управління конфігураціями та ролей адміністраторів
9. Налаштування моніторингу, аудитів та сповіщень
10. Забезпечення сумісності та інтеграції з існуючими системами

Реалізація та тестування обраних засобів захисту



Оцінка ефективності та рекомендації щодо вдосконалення

1. Контроль доступу (Apache Fortress)
2. Системи виявлення вторгнень (OSSEC та Snort)
3. Резервне копіювання та відновлення (Netwrix Backup)
4. Продуктивність та навантаження
5. Інтеграція компонентів
6. Аналіз логів та інцидентів

Основні компоненти та їх ефективність

Компонент	Переваги	Недоліки	Рекомендації для вдосконалення
Контроль доступу	Гнучкі ролі, багатофакторна аутентифікація	Складність налаштування, потреба у навчанні	Автоматизація ролей, централізоване ведення журналу
IDS/IPS	Моніторинг у реальному часі, кореляція подій	Велике навантаження, хибні спрацьовування	Оптимізація правил, оновлення сигнатур
Резервне копіювання	Автоматизація, шифрування, швидке відновлення	Високі витрати, потреба у тестуванні	Багаторівневі копії, хмарне зберігання
Продуктивність	Обробка великого навантаження	Уповільнення серверів, пікове навантаження	Балансування, пріоритезація завдань
Інтеграція компонентів	Централізоване управління	Конфлікти версій, сумісність з ОС	Уніфікація версій, пріоритезація обробки подій
Аналіз логів	Швидка ідентифікація проблем	Пропуски критичних подій, великий обсяг	Централізоване догування, регулярний аналіз

ВИСНОВКИ

- У роботі досягнуто мети – розроблено науково обґрунтовані методи та практичні рекомендації з адміністрування компонентів захисту інформації в розподілених системах. Проаналізовано архітектуру умовної організації, виявлено загрози та критичні ресурси, сформовано матрицю ризиків і вимоги до безпеки з урахуванням сучасних стандартів (RBAC/ABAC, криптографія, резервування, нормативні акти).
- Запропоновано та реалізовано багаторівневу систему захисту з використанням Apache Fortress, OSSEC, Snort, Netwrix Backup і Quattor, проведено тестування продуктивності та стійкості до інцидентів. Показано, що комплексний підхід, регулярне оновлення правил, оптимізація логування, автоматизація процедур реагування й резервування та навчання персоналу дають змогу забезпечити високий рівень кібербезпеки й безперервність бізнес-процесів у середніх і великих організаціях.

Апробації

СЕРТИФІКАТ

ПРО УЧАСТЬ У КОНФЕРЕНЦІЇ (З ПУБЛІКАЦІЄЮ)

ICSR № 25/2811-387

МЦНД

0,4 ECTS

Рекомендовано Вченою Радою

Наукової установи «Інститут науково-технічної інтеграції та співпраці»

Протокол № 47 від 27.11.2025

Конференцію зареєстровано

в Державній науковій установі у сфері управління Міністерства освіти і науки «УкрІНТЕІ»

Посвідчення № 497 від 10.06.2025.

Офіційний видавець

Свідоцтво суб'єкта видавничої справи: ДК № 7860 від 22.06.2023.

www.mcnd.org.ua

Улянченко Максим Юрійович

взяв(ла) участь у VI Міжнародній науковій конференції

«ПЕРІОД ТРАНСФОРМАЦІЙНИХ ПРОЦЕСІВ В СВІТОВІЙ НАУЦІ: ЗАДАЧІ ТА ВИКЛИКИ»

28 листопада 2025 року у м. Полтава, Україна

та опублікував(ла) наукову роботу в збірці конференції

з ISBN 978-617-8312-94-7

DOI 10.62731/mcnd-28.11.2025

ВІЦЕ-ПРЕЗИДЕНТ МЦНД

ГОЛОВА ОРГКОМІТЕТУ

СОТНИК СОЛОМІЯ

МЦНД

МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ

Апробації

СЕРТИФІКАТ

ПРО УЧАСТЬ У КОНФЕРЕНЦІЇ (З ПУБЛІКАЦІЄЮ)

ICSR № 25/2811-387

0,4 ECTS

Рекомендовано Вченою Радою

Наукової установи «Інститут науково-технічної інтеграції та співпраці»

Протокол № 47 від 27.11.2025

Конференцію зареєстровано

в Державній науковій установі у сфері управління Міністерства освіти і науки «УкрІНТЕІ»

Посвідчення № 497 від 10.06.2025.

Офіційний видавець

Свідоцтво суб'єкта видавничої справи: ДК № 7860 від 22.06.2023.

www.mcnd.org.ua

Улянченко Максим Юрійович

взяв(ла) участь у VI Міжнародній науковій конференції

«ПЕРІОД ТРАНСФОРМАЦІЙНИХ ПРОЦЕСІВ В СВІТОВІЙ НАУЦІ: ЗАДАЧІ ТА ВИКЛИКИ»

28 листопада 2025 року у м. Полтава, Україна

та опублікував(ла) наукову роботу в збірці конференції

з ISBN 978-617-8312-94-7

DOI 10.62731/mcnd-28.11.2025

ВІЦЕ-ПРЕЗИДЕНТ МЦНД

ГОЛОВА ОРГКОМІТЕТУ

СОТНИК СОЛОМІЯ

МЦНД

МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ