МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Комп'ютерна інженерія»

Група: 2БКС-29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача освіти денної форми навчання

БКС.29.14.000.КРБ

КУЗНЄЦОВА
ОЛЕКСАНДРА ОЛЕГОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: **«Комп'ютерна інженерія»**

Група: **2БКС-29**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра на тему:

Аналіз методів комплексного захисту інформації в хмарних сховищах даних

Проєктний матеріал складається з пояснювальної записки на **66** сторінках та графічного (презентаційного) матеріалу на **15** аркушах (слайдах).

Виконавець _____ (Кузнєцов О.О.)

Керівник _____ (Краснієнко Н.В.)

Консультанти:

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувач кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Краснокутська К.Г.)

Захист «17» 06 2025 р. Протокол ЕК № 2

Оцінка ЕК 4 (добре) 180

Секретар ЕК _____

АНОТАЦІЯ

Метою кваліфікаційної роботи «Аналіз методів комплексного захисту інформації в хмарних сховищах даних» є розробка рекомендацій щодо забезпечення безпеки даних у хмарних сервісах та власних дата-центрах із фокусом впливу на безпеку та ефективність управління інформацією в бізнесі.

В роботі використано методи наукового пізнання, що включають мислений експеримент, абстрагування, аналіз та синтез й т.ін.

В роботі розроблено рекомендації щодо створення моделі реактивного захисту шляхом інтеграції Zabbix і Fail2Ban: модель координації моніторингу та реагування підтримує концепцію глибоко ешелонованого захисту (defense in depth), де моніторинг, аналітика та активне реагування працюють у тісній зв’язці, утворюючи єдиний цикл обробки інцидентів: виявлення → аналіз → локалізація → повідомлення → блокування.

У розділі охорони праці розглянуто негативні фактори, що впливають на користувача комп’ютерних мереж і персонального комп’ютера

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"28" 05 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачеві освіти *Кузнєцову Олександру Олеговичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз методів комплексного захисту інформації в хмарних сховищах даних*

затверджена наказом по коледжу від "14" 11 2025 р. № 246

2. Термін здачі студентом кваліфікаційної роботи *20.06.2025*

3. Вихідні дані до роботи *1. 1. Програмне забезпечення Matlab для моделювання характеристик. 2. Інструменти для забезпечення кібербезпеки у хмарних середовищах даних. 3. Проаналізувати шляхи інтеграції Zabbix і Fail2Ban. 4.Стоворити програмну модель аналізу вразливостей та трафіку мережі у системі Matlab. 5. Розробити рекомендації щодо механізмів захисту інформації в хмарних середовищах даних.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1.Аналітичний огляд методів та технологій захисту інформації. 2.Провести аналіз понять та визначень інформаційної безпеки 3.Проаналізувати стратегії захисту мережевих систем. 4.Провести 2D- моделювання вразливостей та 3D моделювання навантаження на ресурси системи. 5.Охорона праці та техніка безпеки

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) *Мета дослідження. Інструменти для забезпечення кібербезпеки. Мережевий контроль трафіку. Моделювання вразливостей системи. Моделювання надійності резервування. Двох- та тривимірна моделі навантаження на ресурси. Контроль поштової системи. Система фільтрації трафіку. Захист web-системи. сховища. Інтерфейс адміністратора. Висновки.*

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що їх стосуються

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний розділ	*Краснієнко Н.В.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання _____

Керівник роботи *Краснієнко Н.В.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	*Формування вступу*	*10.05.25*	
2	*Аналіз предметної області*	*15.05.25*	
3	*Підбір науково-технічної літератури*	*20.05.25*	
4	*Аналіз апаратних засобів*	*30.05.25*	
5	*Проєктування структурних схем*	*01.06.25*	
6	*Впровадження моделей*	*06.06.25*	
7	*Аналіз результатів дослідження.*	*07.06.25*	
8	*Оформлення пояснювальної записки*	*08.06.25*	
9	*Оформлення графічної (презентаційної) частини*	*10.06.25*	
10	*Розробка питань з охорони праці та техніки безпеки*	*14.06.25*	
11	*Оформлення пояснювальної записки*	*16.06.25*	
12	*Аналіз результатів рецензування*	*18.06.25*	
13	*Підготовка доповіді для захисту*	*20.06.25*	

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 29.14 000. 00 КРБ	Дипломний проєкт		
А4			БКС 29.14 000. 00 КРБ ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 29. 14 000. 00 КРБ		
Розроб.		Кузнєцов О.О.		20.06	Аналіз методів комплексного захисту інформації в хмарних сховищах даних	Літ.	Аркуш 4 / Аркушів 66
Перевірив		Краснієнко Н.В		20.06		Н Д П	
Н. Контр.		Петрашова В.І.		20.06	ВСП «ОТФК ОНТУ» гр. 2БКС-29		
Затверд.		Іванова Л.В.		20.06			

ЗМІСТ

ВСТУП

У сучасних умовах функціонування бізнесу важливу роль відіграє використання інформаційних технологій та систем, які стали невід'ємною частиною бізнес-процесів будь якої організації. Однією з ключових функцій є зберігання операційних даних, що застосовуються в процесі діяльності організації. Актуальність теми дослідження підкреслюється сучасними особливостями, згідно яким підприємства звертаються до сторонніх сервісів для зберігання даних. Такий підхід часто є виправданим для невеликих компаній, які не можуть дозволити собі власний дата-центр і знайти кваліфікованих спеціалістів для обслуговування системи зберігання даних.

Однак, поряд з перевагами існують деякі недоліки, які отримуються від сторонніх сервісів для зберігання даних, а саме: залежність від послуг стороннього постачальника. Підприємства, які створюються на хмарних сервісах, залишаються залежними від їхнього постачальника. Якщо провайдер має технічні проблеми, збій або припиняє свою діяльність, це може призвести до тимчасової недоступності даних або навіть їх втрати. У випадку виникнення конфліктів чи юридичних проблем з провайдером компанія може виявити серйозні труднощі у відновленні доступу до своїх даних.

Ці фактори можуть впливати на якість і швидкість роботи з даними, а також на загальну ефективність бізнес-процесів підприємства. Сторонні служби зберігання даних часто працюють через Інтернет, швидкість і стабільність з'єднання разом впливають на ефективність доступу до даних. Якщо підприємство має обмежену пропускну здатність каналу або часто стикається з проблемами з'єднання, це може привести до затримок у роботі з даними, сповільнюючи бізнес-процеси та знижуючи їх загальну продуктивність.

Метою аналізу є розробка рекомендацій щодо забезпечення безпеки даних у хмарних сервісах та власних дата-центрах із фокусом впливу на безпеку та ефективність управління інформацією в бізнесі.

В роботі використано методи наукового пізнання, що включають мислений експеримент, абстрагування, аналіз та синтез й т.ін.

У розділі охорони праці розглянуто негативні фактори, що впливають на користувача персонального комп'ютера, враховувано можливі негативні впливи використання бездротових пристроїв на здоров'я користувачів, зокрема, можливість виникнення електромагнітної сумісності, а також відповідність вимогам стандартів безпеки. Дотримання правил і норм безпеки при експлуатації бездротових мереж є важливою частиною охорони праці.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Ключові поняття та визначення інформаційної безпеки

Ключові поняття та визначення інформаційної безпеки охоплюють фундаментальні аспекти захисту даних, систем і мереж. Нижче приведено основні складові:

1) Інформаційна безпека – це сукупність заходів, спрямованих на забезпечення захищеності даних від несанкціонованого доступу, модифікації або знищення.
2) Конфіденційність – гарантування того, що інформація доступна лише авторизованим користувачам.
3) Цілісність – забезпечення точності та повноти даних, запобігання їх несанкціонованій зміні.
4) Доступність – гарантування надійного доступу до інформації уповноваженим користувачам у потрібний час.
5) Ідентифікація – процес розпізнавання суб’єкта або об’єкта за унікальними характеристиками.
6) Аутентифікація – підтвердження особи користувача або пристрою для отримання доступу.
7) Авторизація – надання визначених прав доступу до ресурсів системи.
8) Криптографія – набір методів шифрування для захисту даних від стороннього втручання.
9) Кіберзагрози – потенційні атаки, що можуть порушити безпеку інформаційних систем (віруси, DoS-атаки, фішинг).
   - Захист даних – комплекс організаційних і технічних заходів для збереження безпечного середовища обробки інформації.

Ці принципи формують основу кібербезпеки та впливають на розробку стратегії захисту даних у різних сферах

1.2 Загрози інформаційній безпеці: класифікація атак

Сучасні підприємства все частіше обирають сторонні сервіси для зберігання даних через декілька переваг:

1) Економічна вигода: Використання сторонніх сервісів зазвичай дешевше за
2) створення власної інфраструктури.
3) Висока доступність та надійність: Хмарні сервіси забезпечують постійну
4) доступність та резервне копіювання даних.
5) Безпека даних: Провайдери хмарних послуг використовують сучасні методи
6) захисту, включаючи шифрування та багаторівневу аутентифікацію.
7) Гнучкість і масштабованість: Сторонні сервіси дозволяють легко збільшувати обсяги зберігання відповідно до потреб бізнесу.
8) Делегування відповідальності за ризики: Передача управління зберіганням даних стороннім провайдерам знижує ризики, пов'язані з технічними збоями та безпекою, дозволяючи підприємствам зосередитися на основній діяльності. Рішення про використання сторонніх сервісів для зберігання даних може мати значний вплив на якість та швидкість роботи з даними, а також на ефективність бізнес-процесів. Хмарні сервіси працюють через Інтернет, тому швидкість та стабільність з'єднання є ключовими факторами. Обмежена пропускна здатність або проблеми з'єднання можуть призвести до затримок у роботі з даними, що сповільнює бізнес-процеси.

Для багатьох малих та середніх підприємств використання сторонніх сервісів є вигідним рішенням, оскільки це дозволяє уникнути значних інвестицій у власну інфраструктуру. Великі компанії мають можливості для організації власних дата-центрів, що надає їм більший контроль над інфраструктурою та захистом від зовнішніх загроз. Однак це підходить із високими витратами на обслуговування та потребує кваліфікованих фахівців.

Основні переваги власного дата-центру:

– повний контроль над інфраструктурою;

– більша ізольованість від зовнішніх загроз.

Недоліки власного дата-центру:

– висока вартість обладнання та обслуговування;

– потреба у кваліфікованих фахівцях.

На інформаційну безпеку існує кілька основних типів атак:

1) Атаки доступу: Спосіб отримання доступу до інформації, до якої у зловмисника немає дозволу. Порушує конфіденційність даних.

2) Атаки модифікацій: Зміни або фальсифікація даних.

3) Атаки на відмову в обслуговуванні (DoS): Перевантаження системи, що призводить до недоступності послуг для легітимних користувачів.

4) Атаки на відмову від обов'язків: Відмови визнати виконання чи надання послуг або транзакцій.

5) Атаки здійснюються за допомогою програмного забезпечення, соціального інжинірингу або через дірки в комп'ютерних системах.

Наприклад, атака доступу передбачає копіювання інформації зловмисником.

6) Типи атак доступу:

7) Підглядання: Перегляд файлів та документів.

8) Підслуховування: Використання електронних пристроїв для перехоплення інформації, особливо у бездротових мережах. У дротових мережах зловмиснику необхідно фізично підключитися до мережі.

Ці атаки можуть серйозно загрожувати безпеці даних, тому важливо використовувати належні заходи захисту.

Атаки на інформаційну безпеку включають:

Атаки доступу: Інформація перехоплюється під час передачі, блокується або руйнується. Ціль – отримати доступ до інформації, до якої у зловмисника немає дозволу.

Атаки модифікації: Зміна або фальсифікація інформації, порушення її цілісності. Можливі типи: заміна існуючої інформації, додавання нових даних, видалення даних.

Атаки на відмову в обслуговуванні (DoS): Приводять до недоступності

системи для легітимних користувачів. Можуть зробити інформацію неможливою для використання, змінити або видалити її, перенести в інше місце. Атаки на відмову доступу до додатків або системи виводять з ладу комп'ютерну систему або додатки, унеможливлюючи виконання завдань.

Атаки на відмову доступу до засобів зв'язку виводять з ладу комунікаційне середовище, порушуючи цілісність системи та інформації.

Ці атаки можуть серйозно загрожувати безпеці даних, тому важливо використовувати належні заходи захисту.

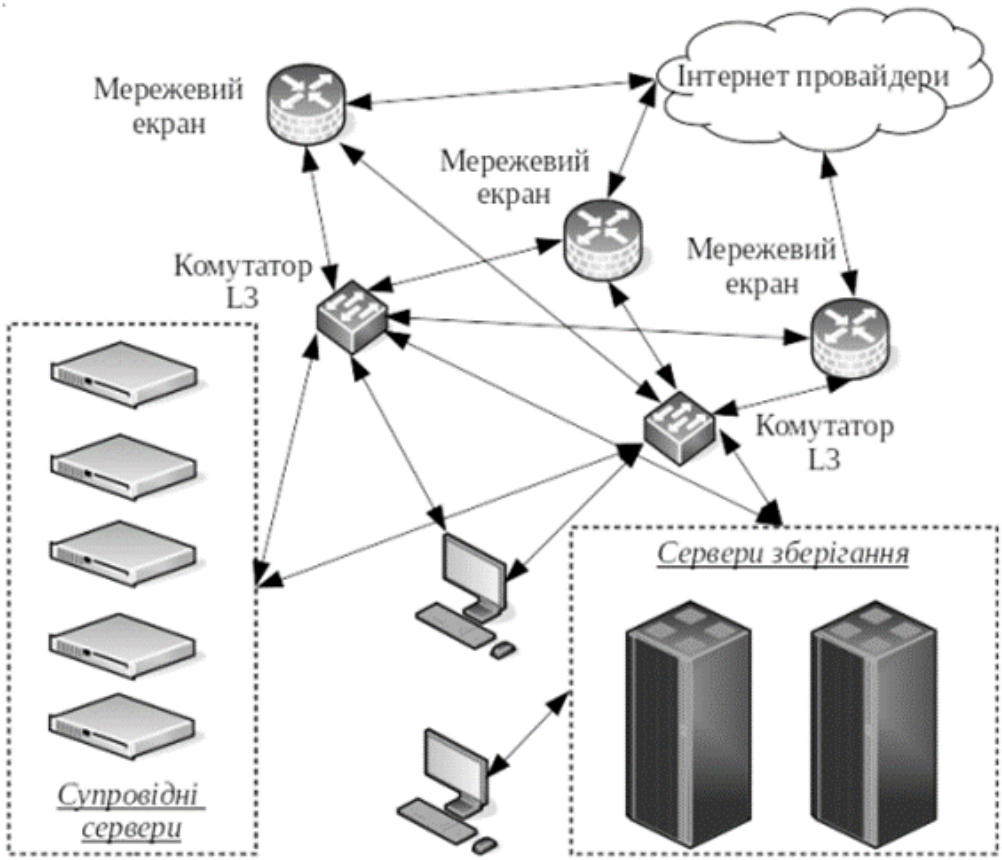


Рисунок 1.1. Функціональна схема мережі із апаратною безпекою даних

1.3 Методи захисту даних

Інформаційна безпека – організована система для знаходження вразливостей і забезпечення захисту даних. Вона включає:

захист від несанкціонованого доступу, використання або зміни даних:

1) Фізичний захист.

2) Захист комунікацій.

3) Захист від випромінювань.

4) Захист комп’ютерів та мереж.

5) Інформація – це повідомлення, факти, дані, команди, знання.

6) Безпека – стан вільності від небезпек та забезпечення збереженості.

Все це разом утворює надійну систему захисту даних і процесів у компаніях.

Конфіденційність – це сукупність служб, які гарантують збереження секретності інформації, забезпечуючи доступ до неї виключно для аутентифікованих користувачів.

Це відіграє ключову роль у захисті систем від несанкціонованого доступу.

Основні засоби захисту конфіденційності файлів:

1) Забезпечення фізичного захисту пристроїв і носіїв.
2) Контроль доступу до інформаційних ресурсів на рівні операційної системи.
3) Використання алгоритмів шифрування для збережених даних.
4) Формування чітких вимог до конфіденційності файлів.
5) Впровадження процедур ідентифікації та аутентифікації.
6) Налаштування параметрів комп’ютерних систем відповідно до політик безпеки.
7) Ефективне управління ключами при реалізації шифрування.

Передавання даних захищається шифруванням, що унеможливлює їхнє перехоплення через підслуховування, хоча не гарантує повного захисту від доступу.

Для цього необхідне підкріплення надійною системою автентифікації. Конфіденційність потоків даних не забезпечує цілісність самих повідомлень, проте ускладнює аналіз структури трафіку, що досягається шляхом його маскування серед великого обсягу даних [6].

Цілісність – служба, покликана забезпечити точність, коректність і достовірність інформації. При правильному налаштуванні системи зберігається впевненість у незмінності даних під час зберігання та передавання. Для

підвищення безпеки цілісність доцільно поєднувати з ідентифікацією — це дає змогу підтвердити справжність інформації [6].

Механізми підтримання цілісності включають:

1) Захист від змін, внесених стороннім впливом.
2) Протидію атакам перехоплення за допомогою комплексного застосування ідентифікації, автентифікації й шифрування.

Поєднання цих засобів сприяє захисту від спроб змінити дані або уникнути відповідальності за дії в системі.

Доступність — характеристика, що відображає готовність системи до функціонування та забезпечує своєчасний доступ до ресурсів: програм, даних і апаратного забезпечення.

Стандартним засобом збереження інформації є резервне копіювання, однак воно не гарантує повної доступності. Тому застосовують додаткові засоби:

1) Перемикання по відмові — автоматичне переключення на резервні компоненти у разі збоїв основного обладнання.
2) Відновлення після аварій — захист інформаційної інфраструктури під час стихійних лих або техногенних катастроф.
3) Прогнозування та нейтралізація атак це реалізація механізмів протидії DoS-атакам і швидкого відновлення після збоїв.

Хоча повне відновлення після серйозних інцидентів може бути складним, ці заходи значно знижують їхні наслідки і сприяють стабільності функціонування.

Ідентифікаційність – функція, що діє у взаємодії з іншими службами безпеки, відіграючи важливу роль у запобіганні атакам. Ідентифікація й автентифікація дають змогу адміністраторам точно визначити користувача та перевірити рівень його повноважень.

Аудит – служба, що здійснює фіксацію дій і подій у комп’ютерних системах і мережах.

Вона взаємодіє з механізмами ідентифікації, авторизації та автентифікації, ведучи журнали, в яких детально фіксуються всі дії користувачів у системі [6].

1.4 Безпечне функціонування DNS-сервісів

Служба доменних імен (DNS) виконує критично важливу роль – перетворює доменні імена на відповідні мережеві адреси і навпаки. Як ключова ланка в інфраструктурі Інтернету, DNS вимагає особливої уваги до питань безпеки, оскільки є вразливим до широкого спектру атак.

До компонентів DNS, що потребують захисту, належать:

1) Апаратна база та відповідне програмне забезпечення.
2) Програмне забезпечення серверів імен.
3) Транзакції DNS (запити, відповіді, оновлення зон).
4) Репозиторії даних (зонні файли, кеш-пам’ять).
5) Конфігураційні файли сервера та клієнта.

Основні служби безпеки DNS включають:

1) Надійна аутентифікація учасників обміну.
2) Забезпечення цілісності інформації у транзакціях.
3) Реалізація механізмів захисту платформи виконання (операційна система, оточення).
4) Захист запитів, відповідей і динамічних оновлень DNS.
5) Комплексне адміністрування: генерація алгоритмів, обробка ключів, контроль доступу до управління.

Поширені загрози для DNS-сервісу:

1) Переповнення буфера — атаки на ОС або ПЗ серверу можуть призвести до збоїв та DoS-сценаріїв.
2) Наводнення пакетів — масова генерація фальшивих запитів може перевантажити сервер.
3) Внутрішні загрози — компрометація через локальну мережу, зокрема атаки на основі ARP-спуфінгу.
4) Атаки на конфігураційні файли — порушення роботи DNS між вузлами, потенційний несанкціонований доступ або відмова в обслуговуванні.

Заходи безпеки програмного забезпечення DNS-сервера:

1) Ізоляція середовища виконання для мінімізації наслідків компрометації.
2) Постійне оновлення до останніх стабільних версій із виправленням вразливостей.
3) Виконання з обмеженням прав доступу (наприклад, запуск у контейнері або від окремого користувача без адміністративних прав).

Досліджувані перераховані заходи впливають на зниження ризику для критичних компонентів DNS: даних зон, структури ієрархії доменів та конфігурацій.

1.5 Захист web-серверів та їх інфраструктури

Web-сервера є частою ціллю атак зловмисників. Вони формують інформацію за протоколом HTTP і є важливим компонентом web-служб. Web-клієнт надає доступ до інформації на web-сервері і є менш вразливим [5].

Основні загрози:

1) Використання помилок ПЗ на web-серверах для отримання неавторизованого доступу.

2) DoS-атаки, спрямовані на web-сервера.

3) Заходи безпеки

4) Конфігурування операційної системи

5) Конфігурування ПЗ web-сервера

6) Встановлення механізмів захисту, таких як міжмережеві екрани

Ці заходи допомагають захистити web-сервера та мережеву інфраструктуру, що їх підтримує.

1.6 Інструменти для забезпечення кібербезпеки

Для ефективного виявлення вразливостей у системі необхідне постійне тестування мережевого середовища та підключених пристроїв. Інструменти аналізу вразливостей класифікують за місцем їх розміщення (наприклад, локальні або хмарні) та за типами інформації, яку вони використовують для виявлення загроз. Такі засоби аналізують:

- структуру файлів,
- параметри конфігурацій,
- поточний стан системи.

Переваги використання систем аналізу вразливостей:

1) Виявлення вразливих ділянок у системі до того, як ними скористається зловмисник.
2) Можливість планового та автоматизованого тестування безпеки.
3) Своєчасне виявлення змін у системі безпеки й оперативне інформування адміністраторів.
4) Комплексний аудит змін, який допомагає виявити та усунути ризики ще до того, як вони стануть критичними.

Недоліки використання таких систем:

1) Тісна інтеграція з ОС та прикладними програмами може створити потребу в додатковому налаштуванні та керуванні.
2) Існує ризик генерації хибних позитивних сповіщень (false positives), які можуть відволікати увагу від реальних загроз.

Деякі тести, особливо без ретельної попередньої конфігурації, можуть негативно вплинути на стабільність системи.

Захист інформації в хмарних сховищах і локальних системах зберігання вимагає комплексного підходу, що включає:

- апаратні засоби захисту (фізична безпека, ізоляція інфраструктури);
- програмні рішення (антивірусне ПЗ, міжмережеві екрани, шифрування);

організаційні заходи (розподіл прав доступу, навчання персоналу, політики резервного копіювання).

Ключовим є визначення всіх критичних вузлів інфраструктури та чітке формулювання вимог до їх захисту. Це дає змогу не лише зменшити ризики, а й побудувати керовану архітектуру кібербезпеки.

Узагальнена таблиця аналізу типів вразливостей, відповідних інструментів їх виявлення, а також переваг та обмежень цих засобів (табл.1.1).

Таблиця 1.1 Аналіз вразливостей

Тип вразливості	*Типовий метод виявлення*	*Інструменти*	*Переваги*	*Обмеження*
Конфігураційні помилки	Аналіз конфігурацій систем/мереж	Nessus, OpenVAS, Lynis	Швидке виявлення потенційних помилок	Можливість помилкових сповіщень (false positives)
Вразливості ОС та програмного забезпечення	Сканування на відомі вразливості з баз даних	Nexpose, Qualys, Microsoft Defender VA	Постійне оновлення баз CVE	Вимагає регулярного оновлення та налаштування
Вразливості вебсервісів	Тестування зовнішніх інтерфейсів і вебпортів	Nikto, Acunetix, Burp Suite	Виявлення специфічних загроз для вебзастосунків	Часто потребує ручної перевірки результатів
Внутрішні порушення доступу	Аналіз прав, активності та журналів	OSSEC, Wazuh, Tripwire	Виявлення аномалій серед внутрішніх користувачів	Потребує інтеграції з SIEM/логами для повного охоплення
Мережеві вразливості	Сканування портів, виявлення відкритих сервісів	Nmap, ZMap, Zenmap	Оцінка доступності та конфігурації пристроїв	Може бути виявлене системами захисту (IDS/IPS)
Вразливості хмарних середовищ	Аудит конфігурацій, політик доступу, шифрування	ScoutSuite, Prowler, CloudSploit	Спеціалізовані засоби для AWS, Azure тощо	Обмежена підтримка приватних хмар або гібридних моделей

Комплексний захист даних у хмарних сховищах та локальних мережах зберігання потребує інтеграції апаратних, програмних і організаційних заходів. Для ефективної побудови системи інформаційної безпеки важливо:

- провести інвентаризацію критичних вузлів,
- визначити вимоги до захисту кожного компоненту,
- реалізувати багаторівневу модель захисту.

Захист мережевих систем

Мережева інфраструктура є базовою платформою для передавання даних, тому її безпека є ключовим фактором стабільної роботи.

Контроль доступу до мережевого обладнання:

1) Реалізація списків контролю доступу (ACL) для обмеження входу.
2) Використання асиметричних криптографічних ключів з довжиною не менше 2048 біт.
3) Впровадження двофакторної аутентифікації для доступу до інтерфейсів керування.

Захист конфігурацій обладнання:

1) Резервне зберігання конфігурацій на окремих серверах.
2) Періодична перевірка цілісності конфігураційних файлів.
3) RAID-дзеркалювання дисків для забезпечення відмовостійкості даних.

Захист від перевантаження та аномалій трафіку:

- Системи моніторингу відстежують навантаження на інтерфейси й сервіси.
- Порушення у роботі виявляються за допомогою сигналів (тригерів) і графіків.

Zabbix — один із найбільш ефективних інструментів моніторингу, який забезпечує:

- Візуалізацію трафіку на мережевих інтерфейсах.
- Динамічне оновлення інформаційної панелі подій.
- Інформування адміністраторів про інциденти через поштові сервіси та месенджери.

Збір інформації про стан мережевих пристроїв: протокол Syslog.

Протокол Syslog — невід'ємна частина моніторингу та аудиту мережевого обладнання. Він дозволяє відслідковувати:

1) Стан мережевих інтерфейсів.
2) Рівень завантаження процесорів.
3) Використання оперативної та постійної пам'яті.
4) Заповненість файлових систем.
5) Роботу компонентів введення/виведення.

Захист кінцевих пристроїв (робочих станцій, ноутбуків, планшетів, мобільних пристроїв тощо) є критичним елементом у загальній системі

кібербезпеки, оскільки саме ці пристрої є точками взаємодії користувачів із мережею та даними.

Мета такого захисту – забезпечити цілісність інформації, доступність обладнання та контроль виконання сервісів і процесів. Окрему увагу приділяють захисту операційної системи, що реалізується за допомогою спеціалізованого стороннього програмного забезпечення, включно з антивірусними рішеннями [7].

Переваги використання антивірусного ПЗ:

1) Протидія шкідливому коду — запобігання проникненню вірусів, троянів, шпигунських програм та інших форм зловмисного ПЗ.
2) Моніторинг і контроль системних процесів — виявлення аномалій, що свідчать про вторгнення чи порушення політик безпеки.
3) Фільтрація мережевого трафіку — перевірка даних, які надходять через інтерфейси (Ethernet/Wi-Fi), для виявлення підозрілої активності.
4) Оцінка стану пристрою — аналіз навантаження, продуктивності та наявності потенційних загроз у реальному часі.

Рисунок 1.2. Реалізація програмної моделі безпеки даних

1.7 Стратегії захисту мережевих систем

Захист даних включає забезпечення конфіденційності, цілісності та доступності [6].

Захист доступності даних вимагає:

1) Контроль щільності трафіку в мережі.
2) Контроль мережевих інтерфейсів на всьому обладнанні.
3) Резервування даних.
4) Фільтрацію трафіку.

Захист конфіденційності даних вимагає:

1) Використання симетричного шифрування AES192 для даних, що зберігаються та передаються.
2) Аутентифікації та розмежування доступу до даних.
3) Використання хеш-функцій для сховування паролів та контрольних кодів доступу.
4) Моніторинг діяльності користувачів, процесів та програмного забезпечення.

Контроль цілісності використовується для:

1) Контролю цілісності ідентифікаційних даних.
2) Аутентифікації повідомлень всередині мережі.
3) Зберігання паролів та кодів.
4) Контролю цілісності даних на серверах.

Для забезпечення цілісності, доступності та відновлюваності даних у випадку збоїв чи інцидентів, у корпоративному середовищі застосовується резервування як на локальних серверах, так і на окремому резервному обладнанні. Ці заходи дозволяють зменшити ризики втрати критичної інформації (рис.1.3.)

Основні підходи до реалізації резервування:

1) RAID-масиви використовуються для створення надмірності в локальних системах серверів, що забезпечує відмовостійкість дискового простору.

2) Сервери резервування це виділені сервери призначені для зберігання копій даних, конфігурацій систем та обладнання.

Періодичне збереження користувацьких даних реалізується шляхом:

- щоденного резервування за останні 7 днів;
- створення щомісячної копії для довготривалого зберігання.

Автоматичне збереження конфігурацій при внесенні змін — дозволяє оперативно відновити попередні параметри у разі помилкового оновлення або атаки. Доцільно вести архівування історії конфігурацій.

За технологією архівування історії конфігурацій — зберігаються 20 останніх знімків конфігураційного стану обладнання, що забезпечує контроль змін та гнучке відновлення.

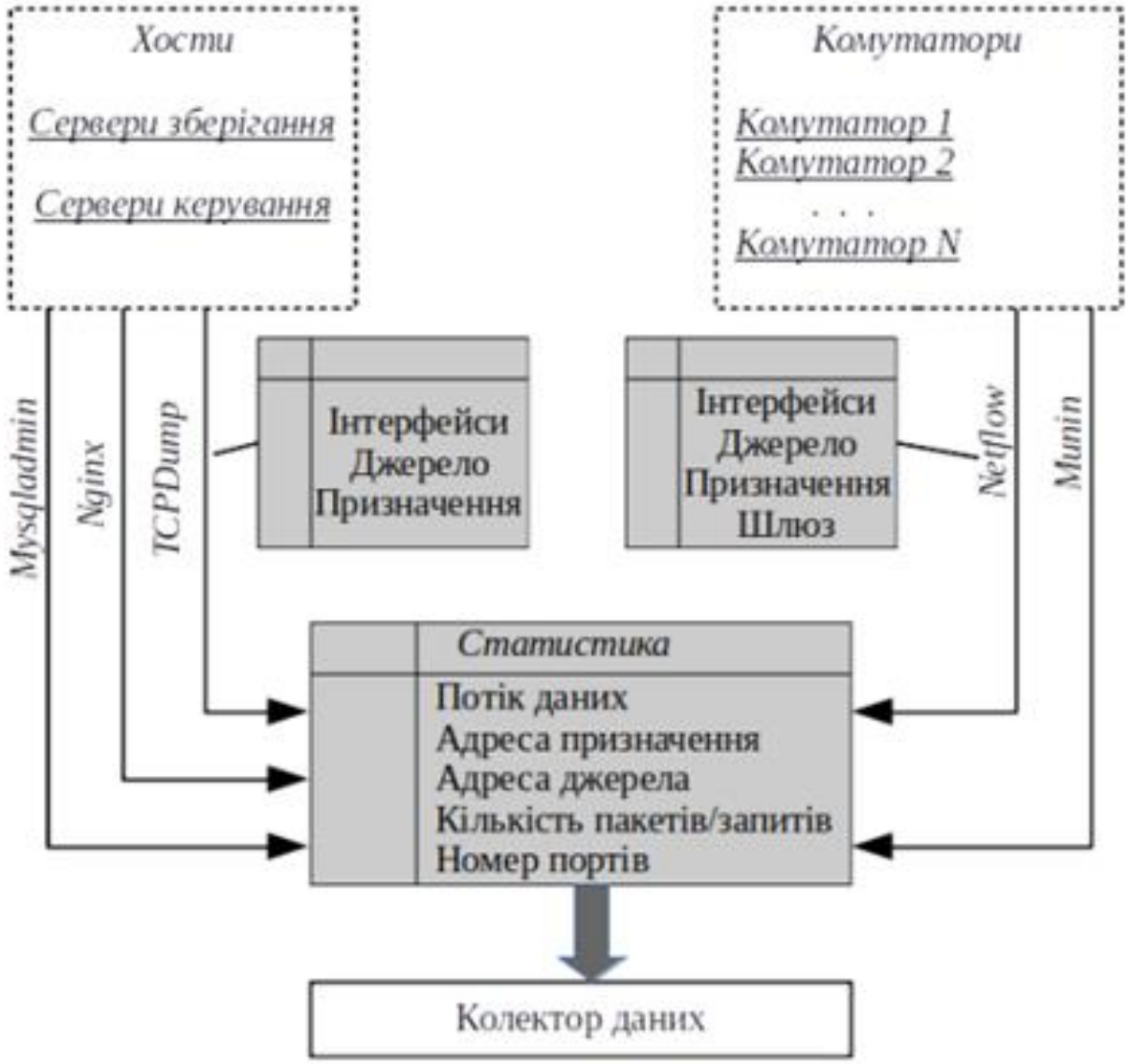


Рисунок 1.3. Організація системи внутрішнього контролю трафіку

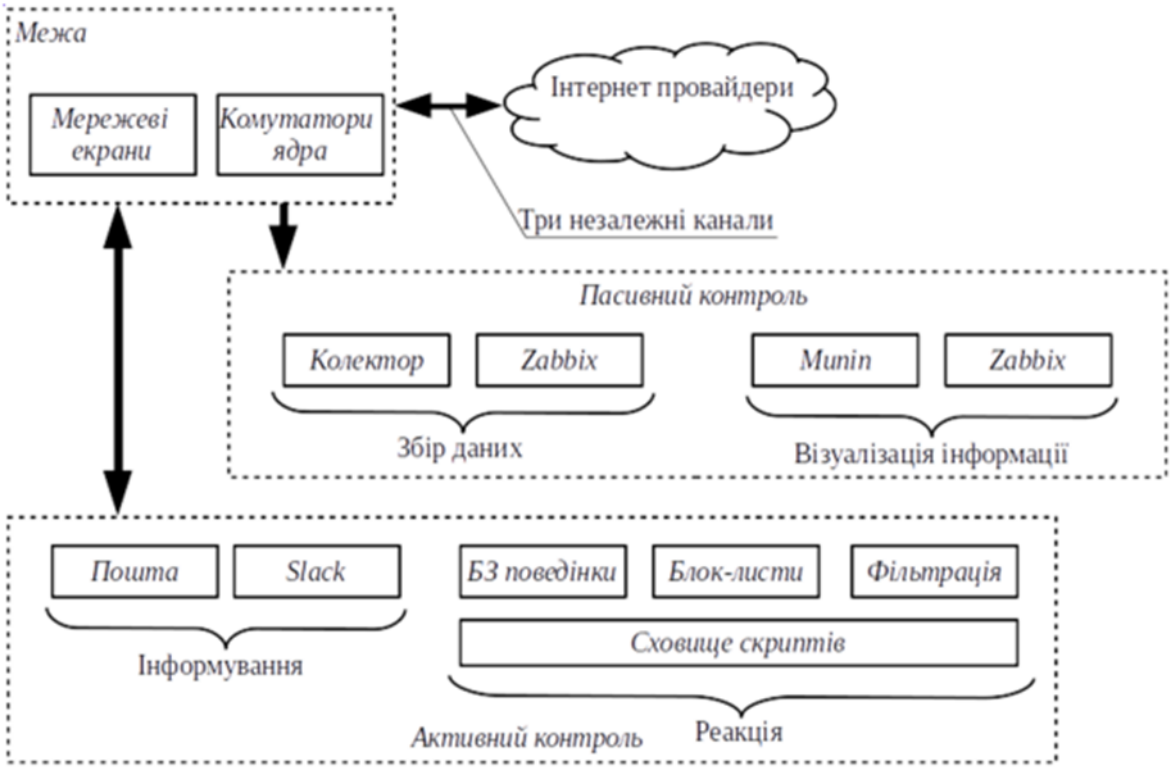


Рисунок 1.4. Функціональна схема системи міжмережного контролю трафіку

1.8 Захист кінцевих пристроїв: принципи та технології

Організаційні заходи покликані регламентувати поведінку користувачів і персоналу в системах зберігання даних. Вони охоплюють як елементи управління доступом, так і підвищення обізнаності щодо відповідальності за дотримання політик безпеки.

До таких заходів належать:

- Розробка правил доступу до системи: вимоги до створення та зберігання паролів, правила завантаження та зберігання даних, управління ідентифікаторами.
- Документування цілей і важливості функціонування систем зберігання для забезпечення розуміння їхньої критичності.
- Визначення відповідальності користувачів за порушення встановлених правил безпеки.
- Розмежування ролей та обов’язків між користувачами та обслуговуючим персоналом.

Апаратна модель базується на побудові логічної інфраструктури засобів контролю, фільтрації та реагування. Вона забезпечує базовий рівень фізичного та мережевого захисту системи зберігання даних.

До її основних компонентів належать:

- Межові системи фільтрації трафіку (файрволи, мережеві шлюзи).
- Syslog-сервер — для централізованого збору повідомлень про події з усього мережевого обладнання.
- Колектори трафіку — для детального аналізу навантажень і виявлення аномалій.
- Мережеві комутатори з підтримкою фільтрації та сенсорів IDS.
- Сервер виявлення вторгнень — фіксує спроби несанкціонованого доступу.
- Сервер моніторингу — дозволяє у реальному часі візуалізувати стан обладнання та реагувати на інциденти.

У сукупності ці пристрої формують інженерну топологію захисту, яка підтримує безпечне функціонування всієї мережі.

Програмна модель доповнює апаратну, надаючи можливості глибокого аналізу поведінки користувачів, системних процесів і мережевого трафіку. Вона спрямована на виявлення відхилень від норми й запобігання витоку інформації.

Ключові компоненти:

- Вбудовані механізми ОС серверів — IPS-системи, журнали подій, засоби захисту внутрішніх сервісів.
- Засоби ОС мережевого обладнання — контроль MAC-адрес, списки ACL.
- Система виявлення вторгнень (IDS/IPS) — виявляє та зупиняє підозрілу активність.
- Система моніторингу подій — збір логів, формування сповіщень для адміністратора.
- Системи візуалізації — дашборди, графіки навантажень, повідомлення про інциденти.

– Захист від витоку даних (DLP) — моніторинг пересилання конфіденційної інформації.
– Антивірусне програмне забезпечення — виявлення і нейтралізація шкідливого коду.

Нижче приводжу моделювання аналізу вразливостей за типами (мережеві (апаратні), програмні, організаційні) впродовж року у системі Matlab.

```
Matlab
% Приклад даних
months = 1:12;
network_vuln = [15 17 14 13 12 10 9 11 13 14 12 10];
software_vuln = [8 10 7 9 6 5 4 5 6 7 6 5];
org_vuln = [3 4 3 5 4 3 2 3 3 4 3 2];
% Побудова графіка
figure;
plot(months, network_vuln, '-o', 'LineWidth', 2);
hold on;
plot(months, software_vuln, '-s', 'LineWidth', 2);
plot(months, org_vuln, '-^', 'LineWidth', 2);
hold off;
% Налаштування графіка
title('Динаміка виявлених вразливостей за типами протягом року');
xlabel('Місяць');
ylabel('Кількість виявлених вразливостей');
legend('Мережеві', 'Програмні', 'Організаційні', 'Location', 'northeast');
grid on;
```

На рис. 1.5. представлено узагальнений графік аналізу вразливостей за типами (мережеві (апаратні), програмні, організаційні) впродовж 12 місяців у системі Matlab. Що цей графік показує: порівняння динаміки виявлень трьох типів вразливостей; зниження або зростання ризиків у часі (можна моделювати, наприклад, після впровадження нових заходів захисту). Далі приводжу моделювання надійність механізмів резервування у системі

Matlab

```
% Вхідні дані: відсоток успішних і невдалих копій щомісяця
months = 1:12;
successful_backup = [92 95 91 90 93 94 96 97 95 94 92 93];
failed_backup = 100 - successful_backup;
% Побудова стовпчастого графіка
figure;
bar(months, [successful_backup; failed_backup]', 'stacked');
title('Ефективність резервного копіювання за місяцями');
xlabel('Місяць');
ylabel('Відсоток копій');
legend('Успішні копії', 'Невдалі копії', 'Location', 'southoutside', 'Orientation', 'horizontal');
grid on;
```

Графік візуалізує надійність механізмів резервування та дає можливість проаналізувати періоди, коли система працювала нестабільно.

Далі створюємо умовний приклад тривимірного графіка в MATLAB**,** який імітує навантаження на ресурси системи (CPU, пам’ять, диск) упродовж тижня. Цей аналіз зручний для нагдяду за стабільностью роботи серверів або кінцевих пристроїв (рис.1.7.)

Рисунок 1.5. Графік порівняння динаміки виявлень трьох типів вразливостей

Рисунок 1.6. Візуалізація надійності механізмів резервування

Рисунок 1.7. Тривімірна модель навантаження на ресурси системи (CPU, пам’ять, диск) упродовж тижня

Графік показує:

Вісі X і Y — дні тижня й години;

Вісь Z — рівень навантаження;

Графік дозволяє оцінити, коли навантаження пікове (наприклад, вранці в будні).

Код скрипта:

Matlab

```
% Вхідні дані
days = 1:7; % Дні тижня
time = 1:24; % Години доби
[Day, Hour] = meshgrid(days, time);

% Симуляція навантаження
CPU_load = 30 + 20*sin((Day+Hour)/2) + randn(size(Day))*5;
Memory_load = 40 + 15*cos((Day+Hour)/3) + randn(size(Day))*4;
Disk_io = 20 + 25*sin(Day/2) .* cos(Hour/4) + randn(size(Day))*3;

% Побудова тривимірного графіка
figure;
surf(Day, Hour, CPU_load);
hold on;
surf(Day, Hour, Memory_load, 'EdgeColor', 'none');
surf(Day, Hour, Disk_io, 'EdgeColor', 'none');
hold off;

% Налаштування вигляду
xlabel('День тижня');
ylabel('Година');
zlabel('Навантаження (%)');
title('Тривимірне навантаження на ресурси системи');
legend('CPU', 'Пам’ять', 'Диск');
colormap parula;
shading interp;
view(45, 30);
```

1.9 Аналіз та пропозиції механізмів безпеки даних

По-перше, розглянемо захист від небажаної розсилки (спаму). Небажані розсилки — це суттєва загроза для стабільної роботи мережевих інфраструктур і серверів зберігання даних. Вони викликають перевантаження:

- інтерфейсів серверів;
- пам’яті кінцевих пристроїв;
- каналів зв’язку мережевого обладнання.

Це призводить до затримок у наданні послуг, втрати продуктивності та потенційної компрометації мережі.

По-друге, розглянемо типові загрози, пов’язані зі спамом:

- Поштовий спам: масова розсилка електронних листів у напрямку до серверів або від них до сторонніх поштових служб.
- Спам-атаки на вебсервіси: реєстрація фальшивих акаунтів, DDoS через форми зворотного зв’язку тощо.
- Автоматична генерація службових повідомлень від серверів або мережевих пристроїв — якщо не контролюється, може викликати лавиноподібне навантаження.

Для запобігання цим загрозам впроваджуються:

- системи фільтрації поштового трафіку (на основі вмісту, IP або поведінки),
- аналізатори перехопленого трафіку,
- внутрішні правила обмеження розсилок.

Проаналізуємо захист поштового сервісу в хмарних середовищах. У сучасних хмарних рішеннях поштовий сервіс є не лише каналом зв’язку, а й критичним елементом системи ідентифікації користувачів. Через нього проходить:

- розсилання службових повідомлень;
- надсилання кодів підтвердження для двофакторної автентифікації;
- створення сповіщень про події безпеки.

Однак існує ряд ризиків:

1) Зловмисне використання системи для спам-розсилок може призвести до блокування доменного імені поштового сервісу.
2) Поштове навантаження може викликати блокування IP-адрес мережі.
3) Надмірне використання сервісу сприяє порушенню роботи підсистем зберігання.
4) Порушення роботи поштового сервісу — загроза доступності системи загалом.

Заходи, які запобігать включають:

- контроль черг поштових повідомлень (обмеження на обсяг/швидкість);
- аналіз вмісту повідомлень (виявлення спаму, фішингу тощо);
- автентифікація джерела поштового трафіку (використання SPF, DKIM, DMARC);
- відстеження шаблонів поведінки розсилок.

Для мінімізації цих загроз важливо впроваджувати заходи контролю тазахисту. Для запобігання цих загроз використовується ряд заходів, які дозволяють контролювати черги поштових повідомлень, аналіз змісту поштових повідомлень та інше (рисунок 1.8).

Проаналізував вище викладене в комплексній роботі пропонується нижче приведені заходи.

1) Перший рівень захисту: програмний інтерфейс поштового сервісу

Базовий рівень контролю реалізується вбудованими інструментами самого поштового сервісу, який надає функціонал для аналізу поштового трафіку та оперативного реагування. Його призначення — виявлення аномалій і зниження ризиків спаму.

Ключові функції інтерфейсу:

- Підрахунок кількості повідомлень у черзі.
- Отримання списку активних повідомлень у черзі.
- Зчитування заголовків повідомлень (для виявлення підозрілих адрес, тем тощо).

– Зчитування тіла повідомлень (аналіз вмісту на наявність шкідливих компонентів).

Ці функції дозволяють адміністраторам:

- оцінити стан черг;
- запобігти лавиноподібній генерації спаму;
- виявити заражені вузли в мережі.

Приводжу рекомендації щодо механізму активного контролю. Активний контроль — це визначені дії, що автоматично запускаються при:

- виявленні відхилень від стандартної поведінки мережевих об’єктів,
- спрацьовуванні тригерів системи моніторингу (наприклад, порогових значень навантаження або частоти повідомлень).

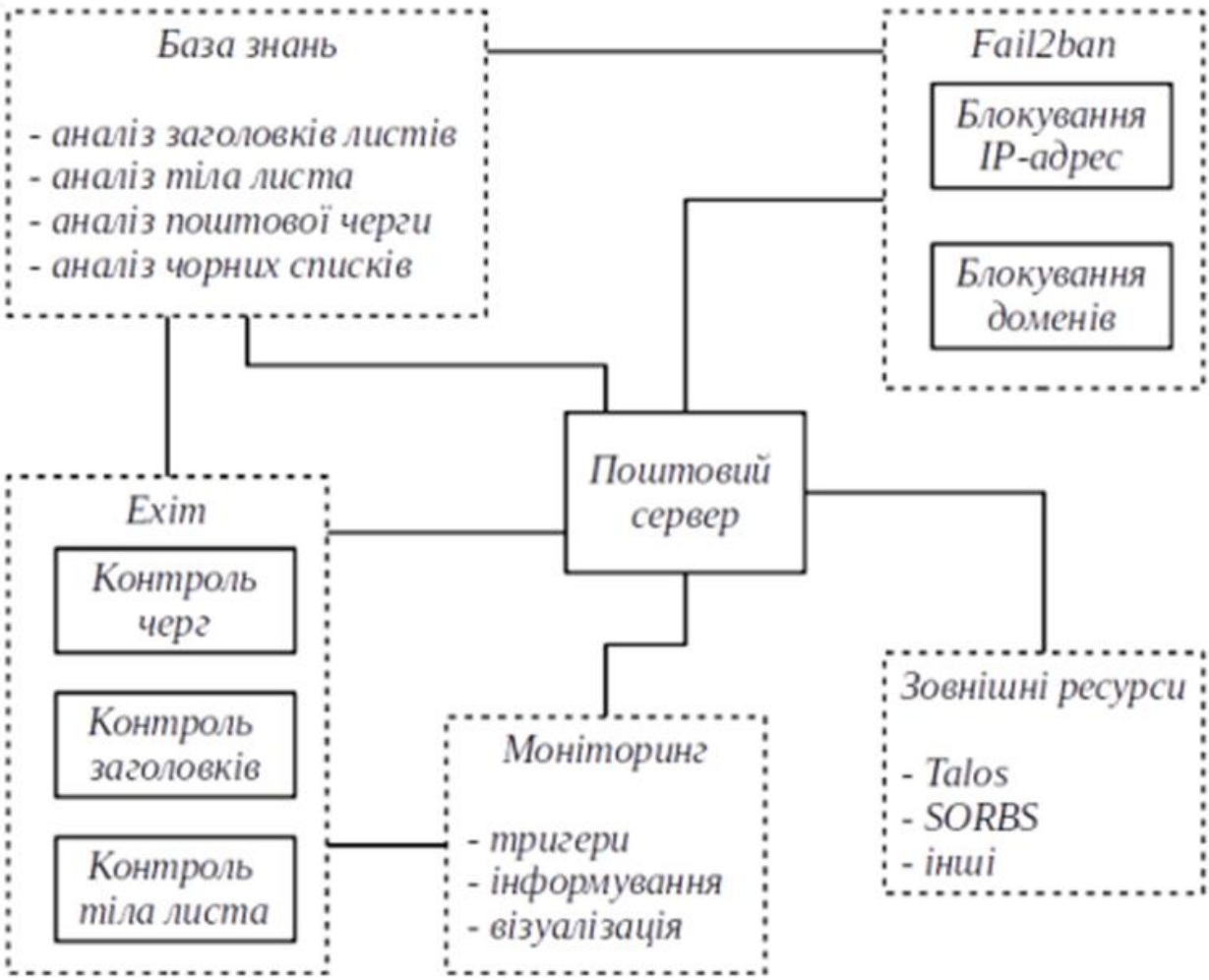


Рисунок 1.8. Контроль поштової системи

Рекомендації щодо механізму інформування відповідальних осіб. Успішна система моніторингу обов'язково включає канали сповіщення. У межах комплексної роботи визначено два типи інформування, які використовуються залежно від рівня критичності події:

1) Електронна пошта
   - Застосовується для всіх рівнів подій: від інформаційних до критичних.
   - Повідомлення включають: текст події/помилки, часову мітку, технічну інформацію для розслідування.
2) Месенджери
   - Використовуються для оперативного сповіщення про події 5 рівня та вище згідно класифікації syslog.
   - Повідомлення – стислий опис інциденту + посилання на систему моніторингу для швидкого реагування.

Веб-системи у мережах зберігання даних: роль, ризики та механізми захисту має велике значення

Веб-системи у складі мережі зберігання даних (СЗД) виконують важливу роль у взаємодії між інтерфейсами користувачів, адміністраторами системи та внутрішньою інфраструктурою. Вони можуть бути реалізовані як окремі веб-сервери або як вбудовані компоненти хмарних сервісів.

Основне призначення:

- Підтримка корпоративних веб-сайтів, що використовують дані із СЗД у режимі реального часу;
- Надання користувачам графічного доступу до функціональності сервісів: перегляду файлів, візуалізації об'єктів, керування обліковими записами тощо;
- Забезпечення інтеграції з іншими зовнішніми або внутрішніми інформаційними системами через API, REST, SOAP або веб-інтерфейси.

Переваги використання веб-систем у СЗД:

1) Інтерфейсно-орієнтований доступ: користувачі взаємодіють із сервісами через зрозумілі візуальні середовища, що зменшує потребу у технічній підготовці.
2) Уніфіковані протоколи доступу (HTTP/HTTPS): забезпечують легку інтеграцію та доступ із будь-яких пристроїв.
3) Можливість централізованого керування та спостереження за активністю користувачів.
4) Платформна незалежність: веб-системи функціонують незалежно від ОС або пристроїв кінцевих користувачів.

Потенційні ризики для інформаційної безпеки такі. Попри зручність використання, веб-системи створюють нові вектори атак, які можуть бути критичними для цілісності та доступності даних у СЗД.

Найпоширеніші загрози:

1) DDoS-атаки на веб-сервер — штучне перевантаження каналу доступу, що може призвести до недоступності сервісу.
2) Несанкціонований доступ до адміністративного інтерфейсу — через підбір паролів, експлуатацію вразливостей або відсутність двофакторної автентифікації.
3) Компрометація даних — несанкціонована зміна файлів або конфігурацій системи через веб-інтерфейс.
4) Порушення правил доступу користувачів — підвищення привілеїв, викрадення сесій або підміна ролей.

Механізми захисту веб-систем на рівні операційної системи:

- Функції контролю доступу до портів і служб (iptables, firewalld, Windows Defender Firewall);
- Обмеження прав сервісних облікових записів;
- Логи доступу, інтегровані із SIEM-системами.

На рівні веб-сервера:

- Верифікація запитів (рейт-лімітинг, CAPTCHA);

– Захист від SQL-ін’єкцій, XSS, CSRF через конфігурацію фреймворків;
– Резервне копіювання HTML, CSS, скриптів, конфігурацій.

Зовнішні засоби:

– Веб-екрани додатків (WAF) — аналізують веб-трафік у реальному часі;
– Приватні мережеві екрани (NGFW) — комбінують фільтрацію, IDS/IPS і глибоку інспекцію пакетів;
– CDN з антимітинговим захистом — дозволяє відсікати надлишковий трафік ще до точки входу.

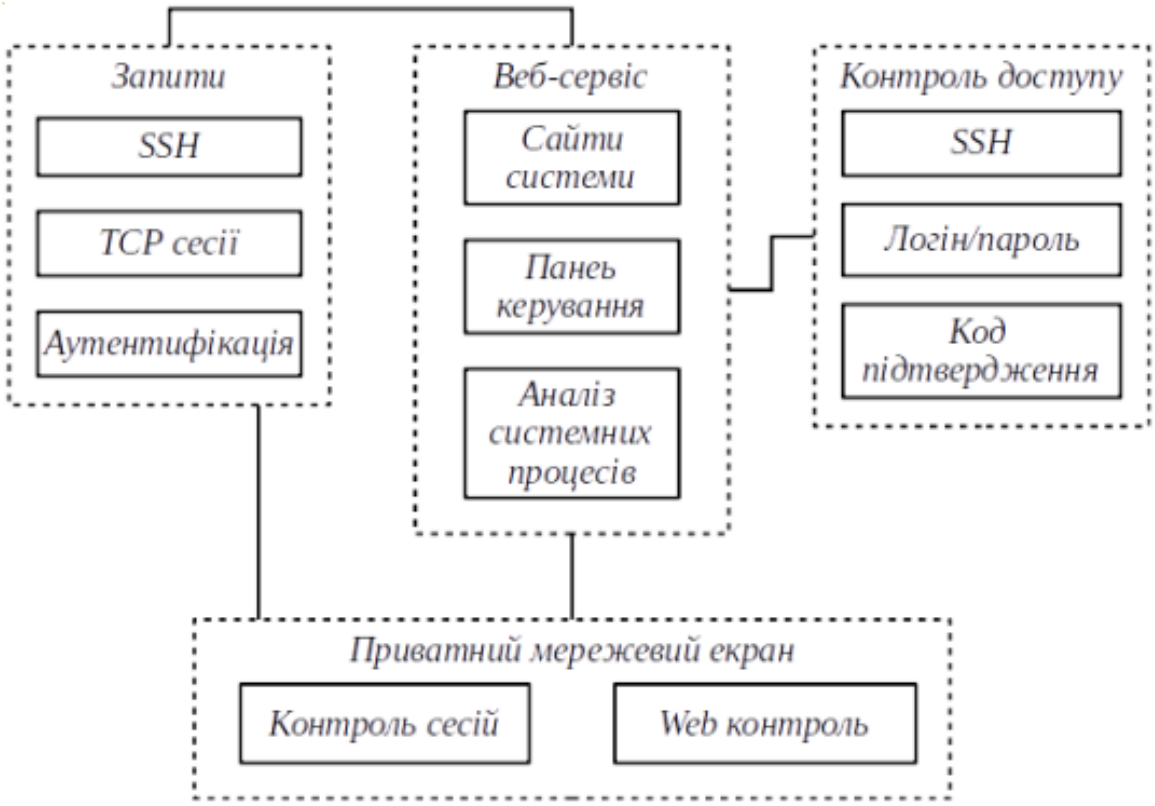


Рисунок 1.9. Захист веб-системи сховища

Нижче приводжу модель реалізації концепції інтеграції Zabbix і Fail2Ban у межах системи інформаційної безпеки:

Інтеграція Zabbix і Fail2Ban: модель координації моніторингу та реагування

Zabbix — це система моніторингу, яка призначена для спостереження за станом IT-інфраструктури в режимі реального часу: сервісів, ресурсів, логів, мережевого навантаження тощо. Вона аналізує поведінку системи, визначає відхилення від нормальних параметрів, генерує тригери й відправляє сповіщення адміністратору.

Fail2Ban — це система захисту, яка автоматично блокує підозрілу активність, насамперед спроби зламу, шляхом сканування лог-файлів і внесення правил фільтрації до фаєрволу (iptables, nftables або інші). Об'єднання цих двох інструментів створює ефективну модель реактивного захисту, в якій:

Zabbix відповідає за виявлення потенційних інцидентів безпеки;

Fail2Ban — за негайне застосування захисних дій у відповідь.

Основні переваги моделі:

Централізований моніторинг подій: Zabbix відстежує події безпеки, наприклад, невдалі логіни, аномальну активність або повторювані помилки.

Автоматичне реагування: Fail2Ban блокує IP-адреси зловмисників ще до того, як вони можуть завдати шкоди.

Багаторівнева взаємодія: Zabbix може аналізувати логи Fail2Ban, а також запускати власні скрипти реагування на події, підсилюючи логіку самозахисту.

Гнучкість і масштабованість: модель легко адаптується до хостинг-платформ, веб-серверів, баз даних, систем SSH тощо.

Зменшення навантаження на адміністраторів: автоматизація рутинних дій дозволяє фокусуватись на критично важливих загрозах.

Об'єднання цих двох інструментів створює ефективну *модель реактивного захисту*, в якій:

- Zabbix відповідає за виявлення потенційних інцидентів безпеки;
- Fail2Ban — за негайне застосування захисних дій у відповідь.

Основні переваги моделі:

1) Централізований моніторинг подій: Zabbix відстежує події безпеки, наприклад, невдалі логіни, аномальну активність або повторювані помилки.

2) Автоматичне реагування: Fail2Ban блокує IP-адреси зловмисників ще до того, як вони можуть завдати шкоди.
3) Багаторівнева взаємодія: Zabbix може аналізувати логи Fail2Ban, а також запускати власні скрипти реагування на події, підсилюючи логіку самозахисту.
4) Інтеграція Zabbix і Fail2Ban: модель координації моніторингу та реагування.
5) Zabbix — це система моніторингу, яка призначена для спостереження за станом IT-інфраструктури в режимі реального часу: сервісів, ресурсів, логів, мережевого навантаження тощо. Вона аналізує поведінку системи, визначає відхилення від нормальних параметрів, генерує тригери й відправляє сповіщення адміністратору.
6) Fail2Ban — це система захисту, яка автоматично блокує підозрілу активність, насамперед спроби зламу, шляхом сканування лог-файлів і внесення правил фільтрації до фаєрволу (iptables, nftables або інші).

Об'єднання цих двох інструментів створює ефективну модель реактивного захисту, в якій:

– Zabbix відповідає за виявлення потенційних інцидентів безпеки;
– Fail2Ban — за негайне застосування захисних дій у відповідь.
– Основні переваги моделі:
– Централізований моніторинг подій: Zabbix відстежує події безпеки, наприклад, невдалі логіни, аномальну активність або повторювані помилки.
– Автоматичне реагування: Fail2Ban блокує IP-адреси зловмисників ще до того, як вони можуть завдати шкоди.
– Багаторівнева взаємодія: Zabbix може аналізувати логи Fail2Ban, а також запускати власні скрипти реагування на події, підсилюючи логіку самозахисту.

Приводжу рекомендації щодо захисту сховищ даних (рис. 1.10.).

Рисунок 1.10. Захист схвищ

1) Захист систем зберігання даних

Системи зберігання даних (СЗД) є критичними компонентами інформаційної інфраструктури, особливо в умовах хмарних технологій, багатокористувацьких середовищ та високонавантажених серверів.

Висока інтенсивність обміну даними між користувачами та серверами створює ряд потенційних загроз.

Основні загрози для СЗД:

2) Завантаження зловмисного коду. Зловмисники можуть обійти традиційні фільтри, розбиваючи шкідливий код на фрагменти, які потім автоматично збираються в цільовій системі.

3) Перевищення квоти користувача Кожному користувачу зазвичай виділяється ліміт на використання дискового простору. Його вичерпання може заблокувати функціонування легітимних процесів або використовуватись для DoS-атак.

4) Циклічний перезапис файлів між серверами У результаті невірної конфігурації або зловмисного сценарію може виникати нескінченний цикл передачі файлів, що створює перевантаження каналів і серверів.

5) Засоби зниження ризиків і захисні механізми

Для мінімізації зазначених загроз необхідно впровадити багаторівневу систему контролю:

1) Контроль квоти користувача

- Виявлення та сповіщення при перевищенні ліміту;
- Автоматичне призупинення завантажень;
- Аудит використання простору за категоріями файлів.

2) Контроль фрагментації файлів

- Виявлення ознак завантаження коду, розділеного на частини (наприклад, послідовні блоки скриптів);
- Перевірка структури файлу перед обробкою;
- Кореляція між частинами на часовій шкалі.

3) Контроль доступу до файлової системи

- Аутентифікація користувачів на основі ролей;
- Встановлення дозволів (ACLs, RBAC);
- Логування дій: завантажень, відкриттів, змін.

4) Ізольоване середовище ("пісочниця")

- Автоматичне перенаправлення нових файлів у sandbox для поведінкового аналізу;
- Виявлення шкідливих дій до активації файлу;
- Інтеграція з антивірусами й аналізаторами вмісту.

Пріоритетами інтерфейсів мережевих екранів є такий принцип, згідно якого кожному інтерфейсу, призначеному до певної зони, надається значення

пріоритету, яке визначає ступінь довіри. Зона з низьким рівнем довіри не може мати доступ до мережі з вищим ступенем довіри. Схема реалізації представлена на рис.1.11.

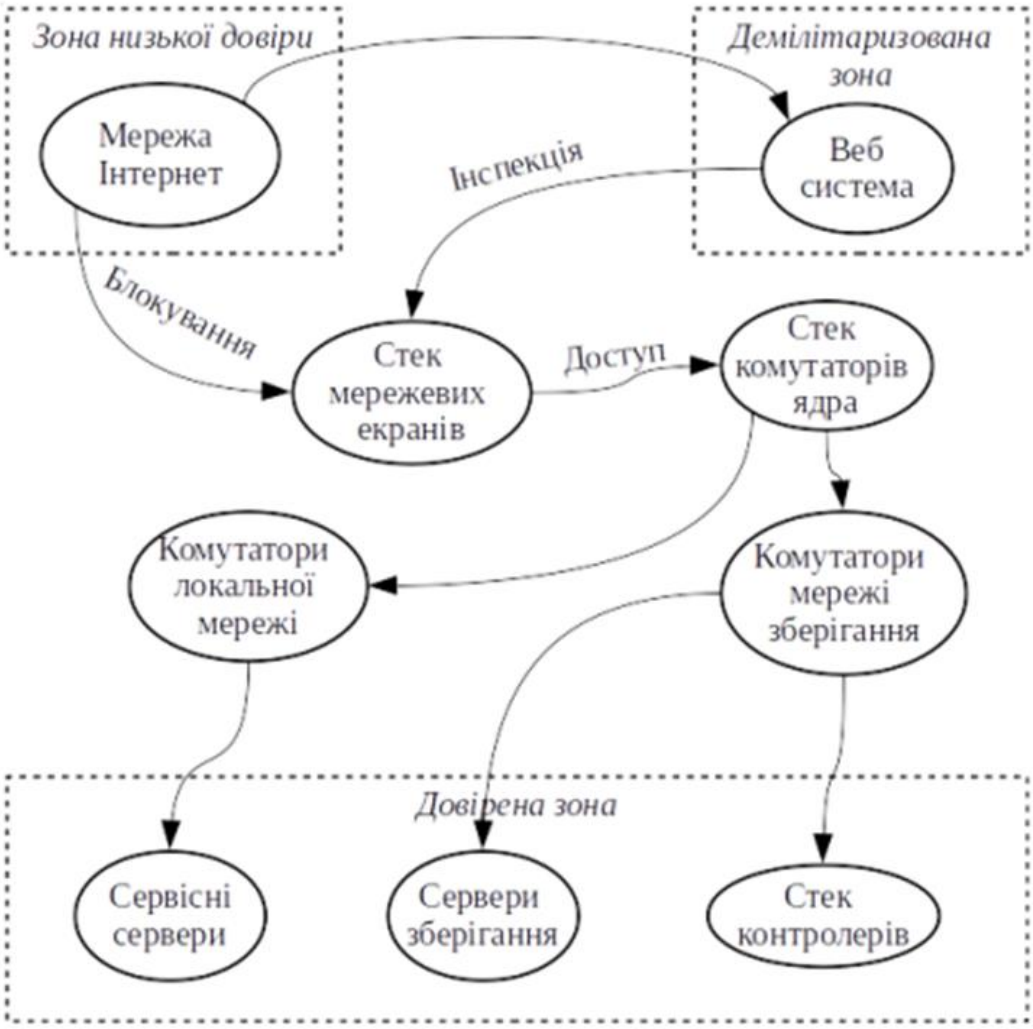


Рисунок 1.11. Система фільтрації трафіку

Фільтрація трафіку в системах зберігання даних це ключовий механізм забезпечення конфіденційності, цілісності й доступності даних у системах зберігання.

Вона дозволяє обмежити доступ до ресурсів, контролювати напрямок передавання даних і запобігати несанкціонованій активності.

Основні механізми фільтрації приведено нижче.

Списки контролю доступу (Access Control Lists, ACL):

- Застосовуються на маршрутизаторах і комутаторах 3-го рівня.
- Працюють на рівні IP-адрес і портів.
- Обмежують доступ до критичних компонентів — серверів зберігання або мережевих контролерів.
- Можуть бути іменованими (для гнучкості), з чітким порядком виконання.

  Типові задачі:
  - фільтрація внутрішніх і зовнішніх маршрутів;
  - створення безпечних VPN-каналів;
  - обмеження доступу до певних підмереж.

Міжмережеві екрани (Firewall):

- Працюють на мережевому та транспортному рівні (OSI-рівні 3–4).
- Розташовуються на межі мережі зберігання, забезпечуючи зонування доступу.
- Здійснюють перевірку стану з’єднання (stateful inspection) та контроль за політиками.
- У мережі з кількома точками виходу до Інтернету використовуються багатоекранні шлюзи, що забезпечують маршрутизацію й фільтрацію незалежно для кожного каналу.

Особливості впровадження фільтрації:

- Фільтрація ґрунтується на зонуванні мережі — призначенні IP-адрес, ролей та інтерфейсів.
- ACL-фільтрація завершується загальним правилом deny any — тобто, забороною всього трафіку, який не відповідає жодному з дозволених критеріїв.
- Політики фільтрації в системі описуються адміністратором інформаційної безпеки один раз, і потім застосовуються постійно — без потреби ручного оновлення.

Сегментація мережі за рівнем довіри дозволяє визначити, який трафік дозволений між зонами приведено у табл. 1.2.

Таблиця 1.2. Модель зон довіри (Trust Zones)

Зона	*Призначення*
Зона низької довіри	Інтерфейси з прямим доступом до Інтернету.
Демілітаризована зона	Проміжна зона для сервісів, які потребують доступу зсередини й ззовні.
Довірена зона	Сервери системи зберігання, бази даних, внутрішні програми.
Транзитна зона	Комутатори, маршрутизатори та інші вузли передачі даних.

Політика фільтрації між зонами:

Трафік з недовіреної до довіреної — заборонений за замовчуванням.

Трафік з довіреної до будь-якої іншої — дозволений за замовчуванням.

Трафік з демілітаризованої зони до недовіреної — дозволений.

Трафік з демілітаризованої до довіреної зони — інспектується (аналіз пакету, протокол, порт).

1.10 Функції інтерфейсу аналізу захищеності мережі

Програмний інтерфейс керування та аналізу безпеки хмарних сховищ даних виконує наступні функції адміністраторів (рисунок 1.12)

- Збір комплексних даних про трафік в мережі та стан мережевого та кінцевого обладнання.
- Візуалізація отриманих даних.
- Візуалізація виявлених помилок (dashboard)
- Сигналізація про події.
- Інтерфейс доступу для налаштування обладнання.

Візуальна частина інтерфейсу дозволяє отримувати графіки, що показують стан мережевого обладнання, серверів, мережевого трафіку та сервісів.

Вона також формує список повідомлень про відхилення параметрів функціонування системи від заданих тригерами, правилами та системними змінними.

Основні системи та функції:

Система моніторингу Zabbix:

Візуалізація широкого діапазону параметрів, включаючи характеристики трафіку, доступність пристроїв та сервісів мережі зберігання.

Інформування адміністраторів про наявність відхилень за допомогою поштової системи та системи Slack.

Система Grafana:

Візуалізація характеристик серверів.

Термінальні сервери мережі:

Підключення до пристроїв в мережі для отримання додаткової інформації про помилки або для їх конфігурації.

Для цього застосовуються способи керування та аналізу безпеки хмарних сховищ даних:

- Ansible: Дозволяє здійснювати одночасні глобальні операції на серверах та інших пристроях, такі як масове оновлення програмного забезпечення та завантаження типових пакетів.
- SSH: Індивідуальне підключення до конкретного пристрою для виконання специфічних завдань.

Глобальні операції включають масове оновлення програмного забезпечення, завантаження типових пакетів та інші операції, які однакові і мають бути здійснені на великій кількості пристроїв.

Індивідуальне підключення здійснюється з використанням асиметричного шифрування, що дозволяє уникнути введення логінів та паролів для кожного підключення.

Це дозволяє адміністраторам автоматично здійснювати консольне підключення до пристрою через інтерфейс адміністратора.

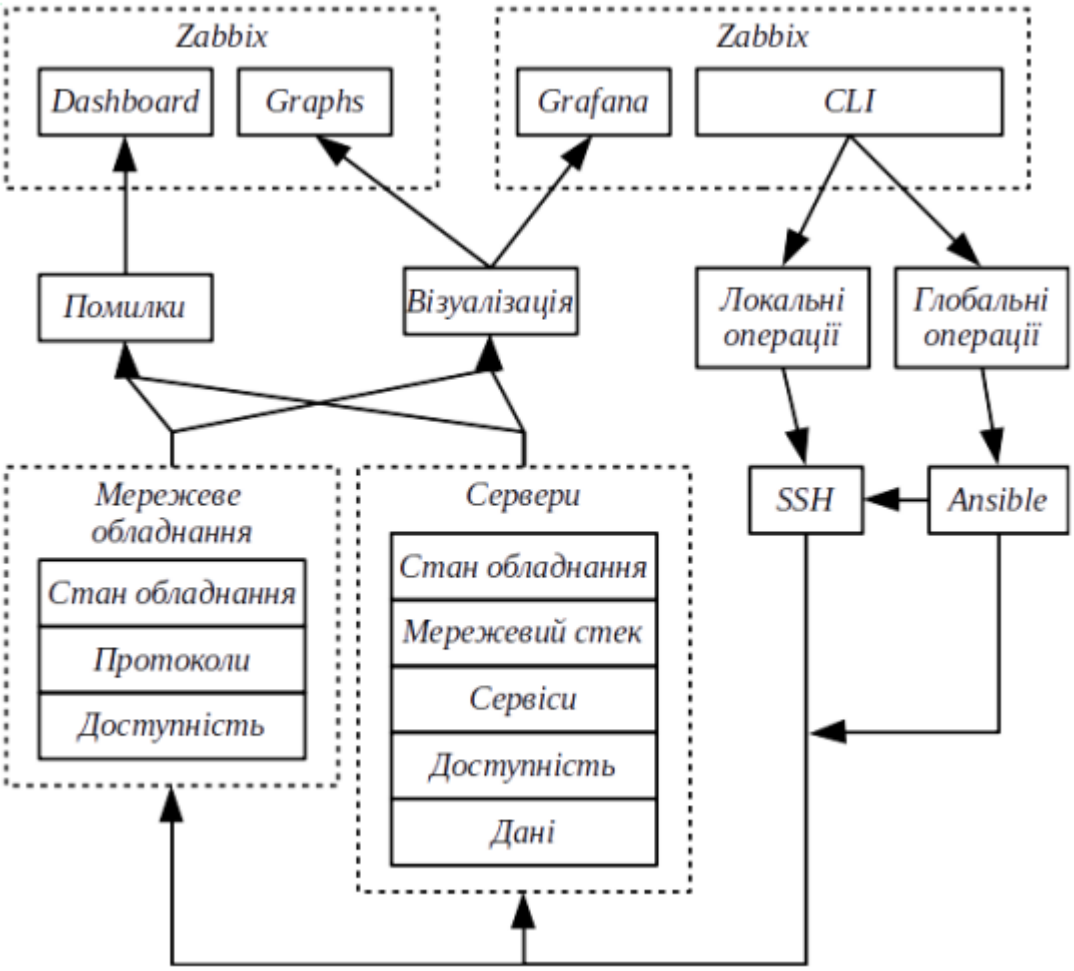


Рисунок 1.12. Інтерфейс адміністратора

1.11 Виявлення та попередження зловживань

Для захисту від зловживань в мережі, де зберігаються і обробляються дані клієнтів, визначено наступні дії:

1) Завантаження виконавчих файлів (віруси, скрипти та ін.)
2) Завантаження файлів до інших користувачів
3) Завантаження конфігурацій до мережевого обладнання
4) Сканування мережі та її пристроїв
5) Несанкціонований доступ
6) Несанкціоноване вивантаження даних
7) Інші дії, не асоційовані з обліковим записом користувача
8) Для контролю ризиків здійснюється аудит дій користувачів, обладнання та процесів на кінцевих хостах.

1.12 Три основні механізми захисту, які передбачено в досліджені

1) Система виявлення вторгнень: Забезпечує моніторинг поведінки трафіку від кожного користувача для визначення аномалій в мережевому трафіку.
2) Антивірусний захист: Забезпечує контроль кінцевих станцій мережі, включаючи контроль процесів на хості та виконання задач на хості.
3) Система запобігання витоків інформації: Контролює ризики копіювання та передачі інформації за межі сховищ даних.

Кожна з систем є окремим модулем, що дозволяє їх модифікувати або замінювати в майбутньому.

Антивірусний захист використовується програмне забезпечення ClaimAV, яке є вільним для використання та найчастіше використовується в Linux-системах на серверах. Захист здійснюється за допомогою наступних модулів:

База даних (БД): Містить всі завантажені шаблони шкідливого ПЗ. Порівнює поведінку об'єктів системи з шаблонами, містить профілі для системи виявлення вторгнень.

Клієнт завантаження: Контролює актуальність баз даних, формує запити на їх оновлення, контролює цілісність шаблонів.

Контроль процесів: Перевіряє діяльність системних процесів хоста для виявлення вірусів та іншого ПЗ.

Контроль програм: Перевіряє програми за переліком, створеним адміністраторами.

Шаблонні поведінки: Визначають ресурси, з якими взаємодіє програма.

Контроль трафіку: Перевіряє мережевий трафік хоста.

Модуль DLP: Виконує функції по запобіганню витоків інформації з серверів системи.

Пісочниця: Виконує підозрілі файли та процеси в ізольованому середовищі для визначення приналежності до шкідливого ПЗ.

1.13 Напрямки безпеки застосування хмарних технологій

Сьогодні сучасні обчислювальні технології оптимізують процедури, пов'язані з віддаленою роботою, обміном ідеями та аналізом даних. Приклади:

Microsoft Azure та Amazon Web Services (AWS): Використовуються для швидкого й ефективного обчислення, аналізу і створення різноманітних послуг.

Tableau і Apache Hadoop: Використовуються для зберігання та аналізу великих обсягів даних.

Palo Alto Networks і CrowdStrike: Використовуються для боротьби з кібератаками та покращення мережевої безпеки та виявлення загроз.

Slack і Trello: Керують проектами та завданнями команд, сприяючи співпраці та комунікації.

Зростання використання штучного інтелекту супроводжується додатковими ризиками. Наприклад, Hugging Face містить понад 1 мільйон моделей, наборів даних і додатків, щомісяця привертаючи понад 19 мільйонів користувачів. Технології з відкритим кодом і нова хвиля загроз вимагають підготовки розробників до захисту екосистеми ШІ.

Наразі компанія Palo Alto Networks у своїх розробках дозволяє командам із безпеки інфраструктури розгортати мережевий рівень для захисту екосистем штучного інтелекту. Пропонує безпеку штучного інтелекту як код для свого портфоліо продуктів.

Компанія запустила AI Runtime Security, доступний для функціонування як з мережею, так і з точками контролю на основі API. Тобто, завдяки цій новій функції API Palo Alto Networks виводить на ринок безпеку штучного інтелекту як код, щоб забезпечити безпеку штучного інтелекту швидким і простим способом.

Розробники отримують доступ до RESTful API і можуть вставляти спеціально створений шаблон коду в існуючий код програми.

Це дає змогу аналізувати корисне навантаження в підказках і відповідях, які користувачі створюють між будь-якими розробленими програмами ШІ та будь-

якими моделями, які їх використовують. Клієнти надсилають свої підказки та моделі відповідей до API у своєму коді програми, а потім отримують вердикт. Це вказує, чи було виявлено загрозу, а також рекомендовані дії, які слід виконати.

Основні напрямки безпеки в хмарних технологіях.

1) Контроль доступу та автентифікація
   - Ідентифікація користувачів через багатофакторну автентифікацію (2FA, MFA).
   - Використання протоколів безпечного доступу (OAuth2, SAML, OpenID).
   - Ієрархічне делегування прав відповідно до ролей (RBAC, ABAC).

2) Захист даних на всіх етапах життєвого циклу
   - Шифрування даних у стані спокою (ат-рес) — AES-256, сервісні ключі.
   - Шифрування при передаванні (ат-транзиті) — TLS 1.2/1.3.
   - Контроль над зберіганням та знищенням резервних копій.

3) Моніторинг і аудит подій
   - Централізоване логування (CloudTrail, Azure Monitor, Stackdriver).
   - Виявлення аномальної поведінки користувачів (UEBA).
   - Автоматизоване реагування на події через системи SIEM/SOAR.

4) Сегментація і розмежування зон довіри
   - Віртуальні приватні хмари (VPC/VNet) з ізольованими підмережами.
   - Демілітаризовані зони (DMZ) для вебсервісів.
   - Поділ ресурсів між орендарями (multi-tenant isolation).

5) Контроль конфігурацій і стану безпеки
   - Політики безпеки для сервісів (cloud security posture management — CSPM).
   - Попередження неправильного налаштування (наприклад, відкритих S3-бакетів).
   - Застосування шаблонів безпечної інфраструктури (Infrastructure as Code з політиками).

6) Захист від атак і шкідливої активності

- WAF, IDS/IPS, анти-DDoS у хмарі (наприклад, AWS Shield, Azure DDoS Protection).
- Засоби фільтрації вмісту та URL-контроль.
- Поведінкова аналітика для виявлення ботів, сканерів, експлойтів.

7) Тестування безпеки та відповідність стандартам

- Періодичні оцінки вразливостей (Vulnerability scanning, PenTesting).
- Аудити відповідності: ISO/IEC 27001, SOC 2, GDPR, PCI DSS.
- Оцінка надійності постачальника (service-level agreements, trust center).

2 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Дотримання трудового законодавства, професійних стандартів та правил охорони праці є ключовими чинниками формування безпечних умов на робочих місцях. Важливе значення має не лише виконання формальних нормативів, але й відповідальне ставлення працівників до власної безпеки, що сприяє захисту їхнього здоров'я та підвищенню загального рівня безпеки на підприємствах.

Охорона праці фахівців із захисту інформації в хмарних сховищах є критично важливою, адже вони працюють із складними системами, які повинні забезпечити безпеку даних та відповідати строгим стандартам кібербезпеки. Важливо звернути увагу на безпеку такого робочого процесу, включаючи ергономіку робочого місця та фактори, що впливають на продуктивність користувача.

Саме ці аспекти варто враховувати для забезпечення належного рівня охорони праці.

2.1 Аналіз умов праці й забезпечення безпеки при виконання основних видів робіт на об'єкті дослідження

Захист інформації у хмарних технологіях – це не лише питання кібербезпеки, а й забезпечення комфортних та безпечних умов праці для працівників, хто стоїть на сторожі цифрового захисту.

Основні аспекти охорони праці таких працівників:

1) Психологічна та емоційна безпека. Постійний моніторинг загроз і атаки може спричиняти виснаження та стрес. Важливо впроваджувати програми підтримки ментального здоров'я.

2) Фізичні умови праці. Тривала робота за комп'ютером потребує ергономічного робочого місця. Важливо мінімізувати ризики, пов'язані з зоровим напруженням та синдромом зап'ястного каналу.

3) Доступ та захист від кіберзагроз. Співробітники повинні мати обмежені доступи відповідно до принципу мінімальних привілеїв. Робота із секретними

даними потребує спеціалізованих безпечних середовищ (віртуальні приватні мережі, двофакторна аутентифікація).

4) Правові аспекти та відповідальність. Працівники повинні бути ознайомлені з міжнародними стандартами безпеки (ISO/IEC 27001, NIST). Важливою є чітко прописана відповідальність у випадку витоку даних.

ISO/IEC 27001 та NIST Cybersecurity Framework—це два ключові стандарти, які визначають підходи до управління інформаційною безпекою.

ISO/IEC 27001 – міжнародний стандарт для управління інформаційною безпекою (ISMS).

Цей стандарт розроблений Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Він визначає вимоги до створення, впровадження та підтримки системи управління інформаційною безпекою (ISMS).

Таблиця 2.1. Основні відмінності між ISO/IEC 27001 та NIST

Характеристика	*ISO/IEC 27001*	*NIST Framework*
Тип стандарту	Формальний, сертифікований	Гнучкий, рекомендаційний
Охоплення	Управління інформаційною безпекою	Кібербезпека та ризики
Сфера застосування	Глобальний стандарт	Переважно США, але використовується міжнародно
Сертифікація	Обов’язкова для відповідності	Необов’язкова, але рекомендована

Обидва стандарти важливі для працівників, які займаються захистом інформації у хмарних сховищах, адже вони допомагають мінімізувати ризики та забезпечити надійний захист даних.

5) Навчання та підготовка. Постійне підвищення кваліфікації з новітніх загроз та методів захисту. Проведення регулярних тренінгів з інформаційної безпеки та кризових ситуацій.

Застосування персонального комп’ютера для інтеграції заходів охорони праці в офісі охоплює низку важливих аспектів. Це передбачає створення безпечного

робочого середовища для персоналу шляхом удосконалення робочих процесів, моніторингу стану обладнання та використання цифрових технологій для аналізу потенційних ризиків. Зокрема, комп'ютерна система сприяє ефективному управлінню вентиляційними установками, регулюванню температурного режиму, оцінці ергономіки робочого місця та автоматизації заходів безпеки.

2.1.1 Мікроклімат робочої зони працівників, вентиляція

Мікроклімат робочої зони значно впливає на комфорт, продуктивність та здоров'я працівників. Він охоплює показники температури, вологості, циркуляції повітря та рівня забруднення атмосфери.

Основні аспекти мікроклімату:

Температура: Оптимальний діапазон залежить від характеру роботи. Для магазинів та офісних приміщень комфортна температура – 18–24°C.

Вологість: Занадто сухе чи вологе повітря може негативно впливати на самопочуття працівників. Оптимальний рівень – 40–60%.

Швидкість повітря: Важливо забезпечити рівномірний розподіл повітряних потоків без протягів.

Якість повітря: Фільтрація та контроль рівня CO_2 допомагають уникнути втоми та зниження концентрації.

Вентиляція як ключовий фактор:

Природна вентиляція (вікна, двері) може бути ефективною, але її достатність залежить від погодних умов.

Механічна вентиляція (вентилятори, кондиціонери) допомагає стабільно підтримувати комфортний мікроклімат.

Системи примусової вентиляції (повітряні фільтри, рекуператори) забезпечують очищення повітря від пилу, алергенів та токсичних речовин.

Важливо правильно організувати повітрообмін, щоб забезпечити свіже повітря без зайвих перепадів температури чи вологості. У спортивному магазині, де можуть бути зони з підвищеним навантаженням (наприклад, склади чи

демонстраційні простори з тренажерами), особлива увага має приділятися якісним вентиляційним системам.

В приміщеннях з ВДТ рекомендовано застосування припливної вентиляції та застосування кондиціонерів. Об'ємно-планувальні рішення будівель та приміщень для роботи з ВДТ ЕОГМ і ПЕОМ мають відповідати нижче приведеним вимогам. Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено.

Площа на одне робоче місце має становити не менше ніж 6,0 м2, а об'єм не менше ніж 20,0 м3. Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і зебезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Розраховується КПО за методикою, викладеною в СНиП II-4-79.

Виробничі приміщення для роботи з ВДТ (операторські, диспечерські) не повинні межувати з приміщеннями, в яких рівні шуму і вібрації перевищують допустимі значення (виробничі цехи, майстерні тощо) за СН 3223-85, СН 3044-84, ГР 2411-81, ГОСТ 12.1.003-83.

Звукоізоляція огороджувальних конструкцій приміщень з ВДТ має забезпечувати параметри шуму, що відповідають вимогам СН 3223-85, ГОСТ 12.1.003-83, ГОСТ 12.1.012-90 (дод.1).

2.1.2 Виробничі випромінювання

На робочому місці користувача ПК впливає неіонізуюче електромагнітне випромінювання, яке може позначатися на його робочому середовищі. Щодо іонізуючих електромагнітних випромінювань, їх рівень на відстані 0,05 м від екрана до корпусу відеотерміналу при будь-яких положеннях регулювальних пристроїв не повинен перевищувати $7{,}74 \times 10^{-12}$ А/кг, що еквівалентно дозі 0,1 мбер/год (100 мкР/год). Контроль, нормування та вимірювання рівнів електромагнітних полів промислової частоти здійснюється відповідно до чинних

нормативних документів, зокрема: ДСНіП №476-2002 (ДСН 3.3.6.096-2002), ДСНіП №239-96, ГОСТ 12.1.002-84.

2.1.3 Електробезпека

Персональні комп'ютери, периферійні пристрої та інше обладнання, включаючи апаратуру управління, контрольно-вимірювальні прилади, освітлювальні пристрої, електропроводи та кабелі, повинні відповідати класу зони та забезпечувати належний рівень захисту. Важливим аспектом є наявність систем захисту від струму короткого замикання та інших аварійних ситуацій. Під час монтажу та експлуатації електромереж необхідно виключити ризик виникнення загоряння через коротке замикання або перевантаження проводів. Для цього слід мінімізувати використання проводів із легкозаймистою ізоляцією та, за можливості, застосовувати негорючі матеріали. Живлення електромережі організовується як окрема групова трипровідна система, що включає фазовий, нульовий робочий і нульовий захисний провідники, що забезпечує стабільність та безпеку електропостачання.

2.2 Пожежна безпека

Пожежна безпека критично важлива для захисту людей і майна. Приміщення повинні відповідати документу [3] та містити план евакуації, особливо в зонах підвищеного ризику.

Передбачені засоби пожежогасіння:

- Вуглекислотні вогнегасники (CO_2) – для електрообладнання.
- Порошкові вогнегасники – універсальні для різних типів загорянь.
- Негорючі покривала – для локалізації вогню.
- Відра, бочки з водою, ящики з піском – для первинного гасіння.
- Автоматичні системи пожежогасіння – водяні, газові, порошкові залежно від приміщення.

Дотримання приведених стандартів підвищує безпеку та ефективність роботи персоналу.

ВИСНОВКИ

В ході виконання комплексної роботи було розроблено структуру комплексного захисту інформації в хмарних сховищах даних, яка використовується в приватному секторі бізнесу для зберігання даних організації-власника мережі та її партнерів.

Основні напрями забезпечення захисту:

Контроль доступу: Багатоетапна аутентифікація користувачів в системі.

Контроль дій користувачів: Моніторинг дій користувачів та пов'язаних з ними процесів.

Багаторівнева фільтрація трафіку: Включає модулі пакетної фільтрації, фільтрації за контентом та на основі репутації.

Активний моніторинг мережі: Використання систем виявлення вторгнень та запобігання витоків інформації.

Контроль кінцевих пристроїв: Використання персональних мережевих екранів та антивірусного ПЗ.

Резервування каналів трафіку та даних: На кінцевих пристроях та на окремих серверах.

Перевагами кваліфікаційної роботи є:

1) Створення моделі реактивного захисту шляхом інтеграції Zabbix і Fail2Ban: модель координації моніторингу та реагування підтримує концепцію глибоко ешелонованого захисту (defense in depth), де моніторинг, аналітика та активне реагування працюють у тісній зв’язці, утворюючи єдиний цикл обробки інцидентів: виявлення → аналіз → локалізація → повідомлення → блокування.
2) Використання “пісочниці” з метою налізу вмісту файлів, які завантажуються.

До недоліків можна віднести велику кількість модулів сттворених структурних схем та складна структура їх взаємодії.

Робота може мати подальший розвиток роботи шляхом модернізації систем контролю та виявлення вторгнень за допомогою штучного інтелекту, зокрема машинного навчання та систем прийняття рішень.

Розглянуто заходи з охорони праці та техніки безпеки при експлуатації комп'ютерних мереж та персональних комп'ютерів, що сприяють організації належних, безпечних і здорових умов праці працівників.

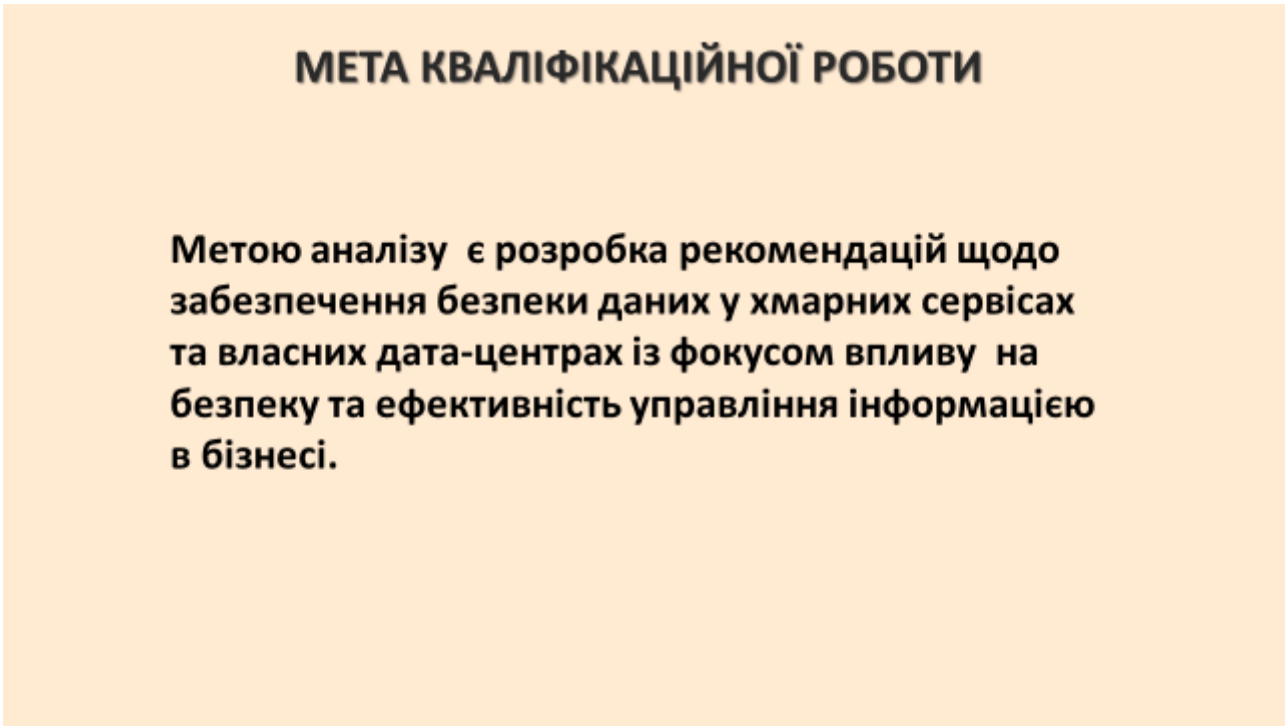
ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Про інформацію: Закон України// Відомості Верховної Ради України. - 2001.- № 11.- С. 25-27.
2. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». [Электронний ресурс] – Режим доступу: http://telekritika.kiev.ua/articles/139/0/8508/zakon_ukraini_pro_osnovni_zasadi_rozvitku_informacijnogo_suspilstva_v_ukraini_na/ (Дата останнього звернення 01. 06.25)
3. ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ ДБН В.2.2-16:201Х. Чинні від 2019. м. Київ Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України
4. Національний стандарт України. Охорона праці. Терміни та визначення основних понять. ДСТУ 2293:2014 Чинний від 01 травня 2015 року. Наказ Мінекономрозвитку України від 02 грудня 2014 р. № 1429 з 2015–05–01 URL: https://web.kpi.kharkov.ua/safetyofliving/wpcontent/uploads/sites/171/2017/10/dstu_2293_2014.pdf (дата останнього звернення 20.05.25)
5. Праворська Н.І. Інформатика та комп’ютерна техніка: Навчально-методичний посібник для студентів вищих навчальних закладів. – Хмельницький, 2002. – 312с.
6. Основи кіберпростору, кібербезпеки та кіберзахисту. Навчальний посібник/ Богуш В.М. , Богуш В.В., Бровко В.Д., Настрадін В.П. Видавництво Ліра-К 2021, 554 с.
7. ДСанПіН 3.3.6.042-99 «Державні санітарні норми мікроклімату виробничих приміщень».
8. ДСанПіН 2.3.6.037-99 «Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку»
9. Катренко П.А., Кіт Ю.В., Пістун І.П. Охорона праці. Курс лекцій. Практикум: Навчальний посібник. - Суми: ВТД “Університетська книга”, 2003. — 496с.

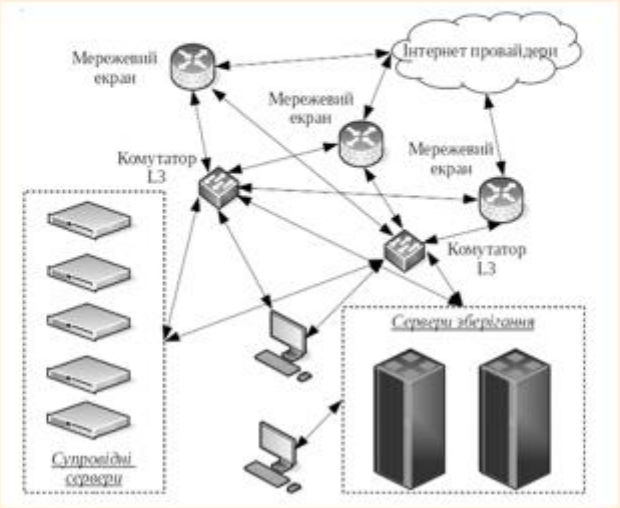
10. Рибальский О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту.// Інформації посібник для курсантів внз мвс україни–2012 URL:https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf (дата останнього звернення 15.05.2025)
11. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников. // Современные тенденции технических наук: материалы I Междунар. науч. конф. —2011. URL: https://moluch.ru/conf/tech/archive/5/1115/ (дата останнього звернення 15.05.2025)
12. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки україни –2020 URL:http://lsej.org.ua/2_2020/54.pdf (дата останнього звернення 15.05.2025)

ДОДАТОК А

Слайди мультимедійної презентації



Функціональна схема мережі із апаратною безпекою даних



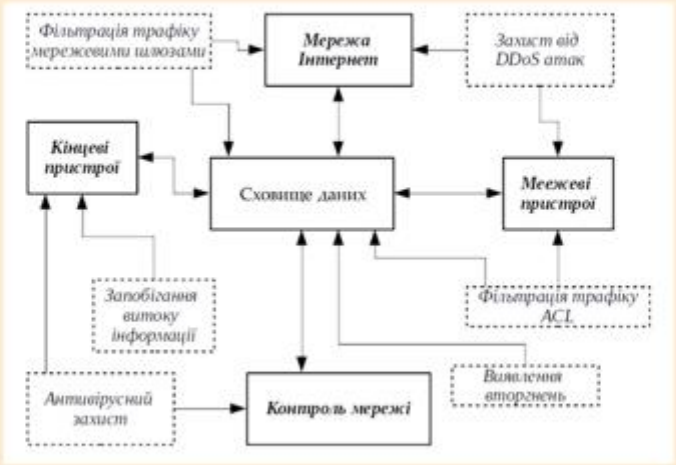
Інструменти для забезпечення кібербезпеки.

Аналіз вразливостей

Таблиця 1.1 Аналіз вразливостей

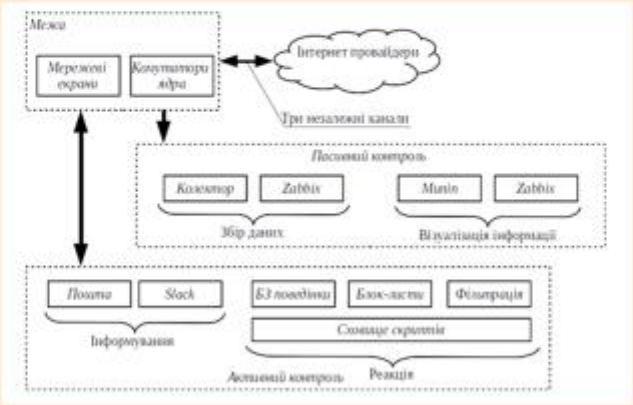
Тип вразливості	*Типовий метод виявлення*	*Інструменти*	*Переваги*	*Обмеження*
Конфігураційні помилки	Аналіз конфігурацій систем/мереж	Nessus, OpenVAS, Lynis	Швидке виявлення потенційних помилок	Можливість помилкових сповіщень (false positives)
Вразливості ОС та програмного забезпечення	Сканування на відомі вразливості з баз даних	Nexpose, Qualys, Microsoft Defender VA	Постійне оновлення баз CVE	Вимагає регулярного оновлення та налаштування
Вразливості вебсервісів	Тестування зовнішніх інтерфейсів і вебпортів	Nikto, Acunetix, Burp Suite	Виявлення специфічних загроз для вебзастосунків	Часто потребує ручної перевірки результатів
Внутрішні порушення доступу	Аналіз прав, активності та журналів	OSSEC, Wazuh, Tripwire	Виявлення аномалій серед внутрішніх користувачів	Потребує інтеграції з SIEM/логами для повного охоплення
Мережеві вразливості	Сканування портів, виявлення відкритих сервісів	Nmap, ZMap, Zenmap	Оцінка доступності та конфігурацій пристроїв	Може бути виявлене системами захисту (IDS/IPS)
Вразливості хмарних середовищ	Аудит конфігурацій, політик доступу, шифрування	ScoutSuite, Prowler, CloudSploit	Спеціалізовані засоби для AWS, Azure тощо	Обмежена підтримка приватних хмар або гібридних моделей

Реалізація програмної моделі безпеки даних

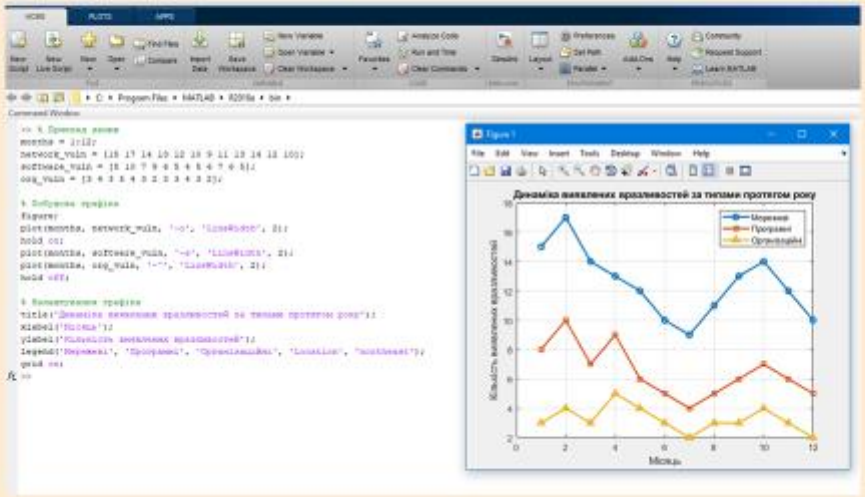


Організація системи внутрішнього контролю трафіку

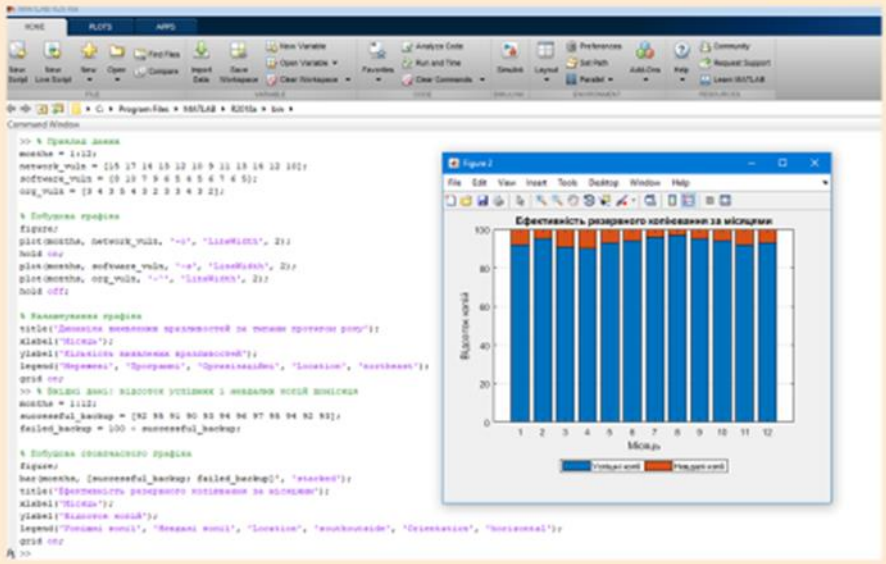
Функціональна схема системи міжмережного контролю трафіку



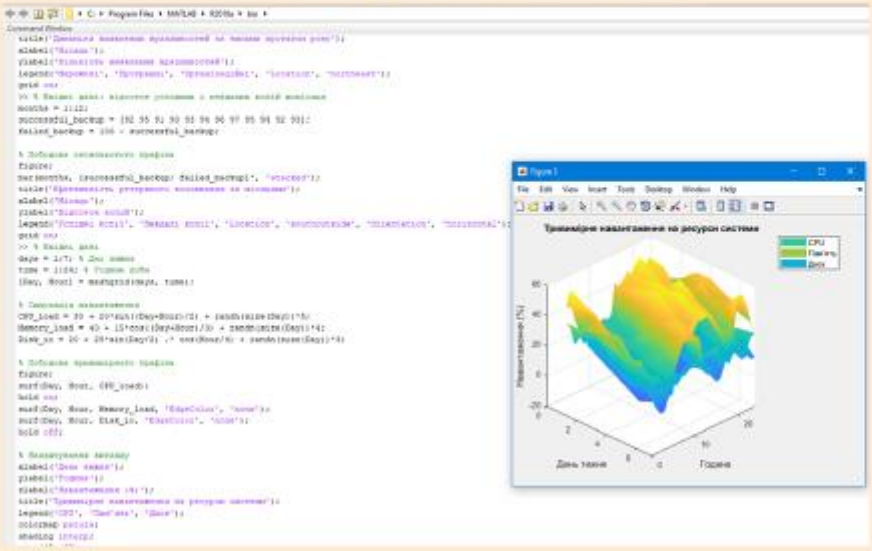
Графік порівняння динаміки виявлень трьох типів вразливостей



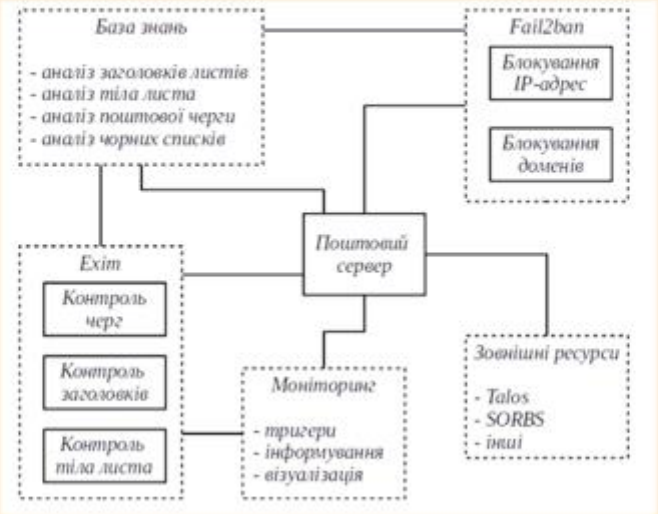
Візуалізація надійності механізмів резервування



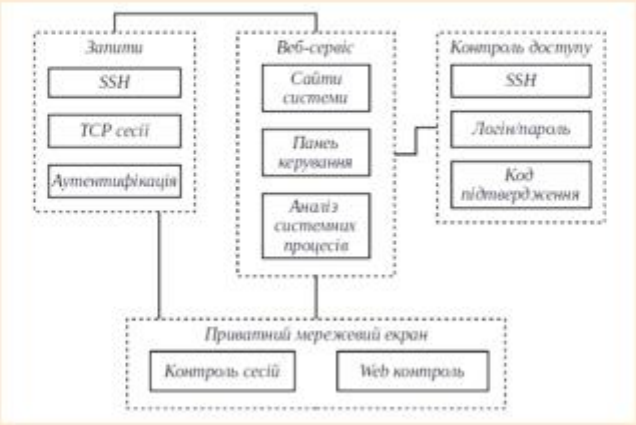
Тривімірна модель навантаження на ресурси системи (CPU, пам’ять, диск) упродовж тижня



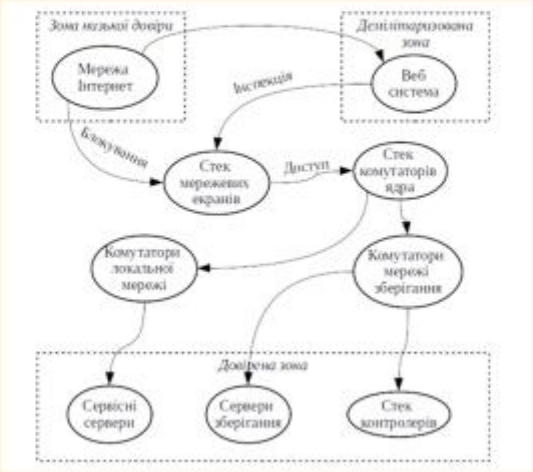
Контроль поштової системи



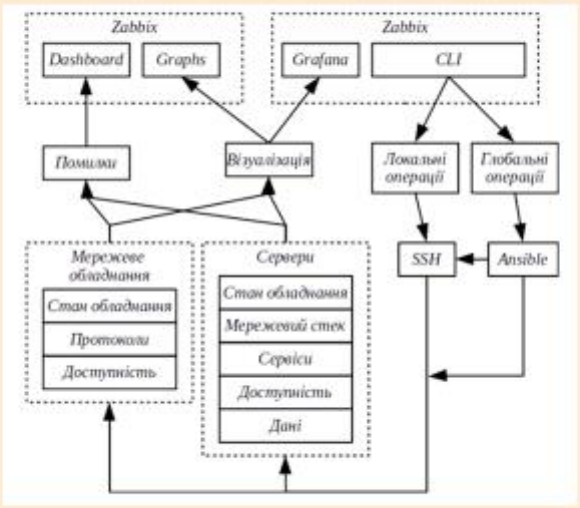
Захист веб-системи сховища



Система фільтрації трафіку



Інтерфейс адміністратора



ВИСНОВКИ

В ході виконання комплексної роботи було розроблено структуру комплексного захисту інформації в хмарних сховищах даних, яка використовується в приватному секторі бізнесу для зберігання даних організації-власника мережі та її партнерів.

Основні напрями забезпечення захисту:

Контроль доступу: Багатоетапна аутентифікація користувачів в системі.

Контроль дій користувачів: Моніторинг дій користувачів та пов'язаних з ними процесів.

Багаторівнева фільтрація трафіку: Включає модулі пакетної фільтрації, фільтрації за контентом та на основі репутації.

Активний моніторинг мережі: Використання систем виявлення вторгнень та запобігання витоків інформації.

Контроль кінцевих пристроїв: Використання персональних мережевих екранів та антивірусного ПЗ.

Резервування каналів трафіку та даних: На кінцевих пристроях та на окремих серверах.

Розглянуто заходи з охорони праці та техніки безпеки при експлуатації мереж та персональних комп'ютерів сприяють організації належних, безпечних і здорових умов праці працівників.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу здобувача (здобувачки) освіти

відділення комп'ютерних систем

Кузнєцова Олександра Олеговича

(прізвище, ім`я та по батькові)

Спеціальність *123 "Комп'ютерна інженерія"*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи *Краснієнко Наталія Володимирівна*

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи *Аналіз методів комплексного захисту інформації в хмарних сховищах даних*

Обсяг розрахунково-пояснювальної записки *66* сторінок

Обсяг графічної (презентаційної) частини *15* аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаного кваліфікаційної роботи завданню

Представлена на рецензію кваліфікаційна робота бакалавра повністю відповідає меті випускної роботи та технічному завданню. Тематика кваліфікаційної роботи є актуальною для своєї галузі та присвячена моделюванню та аналізу п методів комплексного захисту інформації у хмарних середовищах.

б) характеристика виконання кожного розділу кваліфікаційної роботи

Кваліфікаційна робота складається зі вступу, двох розділів, висновків, переліку використаних джерел. У основному розділі розроблено рекомендації щодо створення моделі реактивного захисту шляхом інтеграції Zabbix і Fail2Ban: модель координації моніторингу та реагування підтримує концепцію глибоко ешелонованого захисту (defense in depth), де моніторинг, аналітика та активне реагування працюють у тісній зв'язці, утворюючи єдиний цикл обробки інцидентів: виявлення → аналіз → локалізація → повідомлення → блокування.

в) оцінка якості виконання пояснювальної записки та графічної частини кваліфікаційної роботи

Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та у системі MATLAB. Пояснювальна записка виконана охайно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання документації – добра, академічного плагіату ідей у роботі не виявлено

г) перелік позитивних якостей кваліфікаційної роботи *Робота ґрунтується на ретельно опрацьованій теоретичній базі. В результаті проведеного дослідження було визначено шляхи захисту інформації у хмарних середовищах даних. Робота може мати подальший розвиток роботи шляхом модернізації систем контролю та виявлення вторгнень за допомогою штучного інтелекту, зокрема машинного навчання та систем прийняття рішень.*

д) основні недоліки кваліфікаційної роботи *Велика кількість модулів створених структурних схем та складна структура їх взаємодії. Складність реалізації політик безпеки. Надмірна деталізація «сирого» коду MATLAB у тексті — великі фрагменти скриптів захаращують виклад і відволікають від ключових висновків.*

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *к.т.н. Шибаєва Наталя Олегівна*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис: _____

«23» _____ 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ КОЛЕДЖ ОНАХТ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Кузнєцова Олександра Олеговича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи

«Аналіз методів комплексного захисту інформації в хмарних сховищах даних»

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) обсяг і якість виконання роботи (розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми кваліфікаційної роботи, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дослідженні.

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над кваліфікаційною роботою

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Провів аналіз технологій захисту інформації в хмарних середовищах. Виявив навички самостійно опрацьовувати новий матеріал та виконувати пошук необхідної літератури та інших джерел інформації

в) теоретична підготовка бакалавра

відповідає вимогам, що надаються до бакалавра зі спеціальності 123 «Комп'ютерна інженерія»

г) вміння розв’язувати виробничі та конструкторські питання

У кваліфікаційній роботі проаналізовано основні напрями забезпечення захисту:
Контроль доступу: Багатоетапна аутентифікація користувачів в системі.
Контроль дій користувачів: Моніторинг дій користувачів та пов'язаних з ними процесів.
Багаторівнева фільтрація трафіку: Включає модулі пакетної фільтрації, фільтрації за контентом та на основі репутації.
Активний моніторинг мережі: Використання систем виявлення вторгнень та запобігання витоків інформації.
Контроль кінцевих пристроїв: Використання персональних мережевих екранів та антивірусного ПЗ.
Резервування каналів трафіку та даних.

Оцінка розрахункової частини _____4 (добре)_____

Оцінка графічної (презентаційної) частини _____5(відмінно)_____

Загальна оцінка _____4 (добре)_____

Прізвище, ім’я, по батькові керівника роботи___Краснієнко Наталія Володимирівна

____

_____

Місце роботи і посада керівника роботи _____завідувач лабораторії технічного захисту аналітико-інформаційних технологій ВСП ОТФК ОНТУ, викладач-методист вищої_____ кваліфікаційної категорії_____

«__20__»____06____2025__р. _____ _Краснієнко Н.В.

(підпис) (прізвище та ініціали керівника)

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Кузнєцов Олександр Олегович
здобувач освіти гр. 2БКС-29, та

Краснієнко Наталія Володимірівна,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз методів комплексного захисту інформації в хмарних сховищах даних» (автор роботи – Кузнєцов О.О., керівник роботи – Краснієнко Н.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Кузнєцов О.О./

Керівник _____ / Краснієнко Н.В./

«_20_» ____06_____ 2025 р.

ДОВІДКА

кафедри комп'ютерної інженерії
про допуск до захисту кваліфікаційної роботи
здобувача (здобувачки) освіти II курсу
відділення комп'ютерних систем групи 2БКС-29

Кузнєцова Олександра Олеговича

на тему *Аналіз методів комплексного захисту інформації в хмарних сховищах даних*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до кваліфікаційної роботи виконана з некритичними порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *20.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 20.06.2025 р. значення коефіцієнту подібності в роботі становить 15,89%, коефіцієнт цитування – 0,74%.*

(підпис) *20.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) кваліфікаційної роботи

здобувача (здобувачки) освіти *Кузнєцова О.О.* (П.І.Б.)

проведена « *20* » *червня* 2025 р.

Висновки *Пояснювальна записка до кваліфікаційної роботи виконана у повному обсязі. Випускна кваліфікаційна робота відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Зав. кафедри КІ (підпис) *Іванова Л.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/20/2025
Дата редагування 6/20/2025

Документ прийнятий

Звіт подібності

метадані

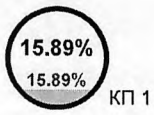
Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Аналіз методів комплексного захисту інформації в хмарних сховищах даних

Автор
Кузнєцов Олександр Олегович
Науковий керівник / Експерт
Краснієнко Наталія Володимирівна

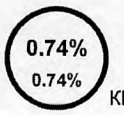
підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1



КЦ

25
Довжина фрази для коефіцієнта подібності 2

8666
Кількість слів

70698
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		15
Інтервали		0
Мікропробіли		0
Білі знаки		12
Парафрази (SmartMarks)		104

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://ref-otpbgo.ucoz.org/publ/okhorona_praci/profesijno_zumovleni_zakhvorjuvannja_u_koristuvachiv_vdt/4-1-0-219	149 1.72 %
2	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	71 0.82 %
3	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	55 0.63 %

4	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	49 0.57 %
5	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	36 0.42 %
6	https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download	33 0.38 %
7	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	31 0.36 %
8	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	28 0.32 %
9	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	27 0.31 %
10	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	26 0.30 %

з домашньої бази даних (0.76 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Аналіз продуктивності блокових криптоалгоритмів у багатоядерній системі [redacted] 6/18/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	49 (4) 0.57 %
2	Розробка анімованої веб-вікторини до 95-річчя ВСП "ОТФК ОНТУ" [redacted] 6/19/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	17 (2) 0.20 %

з програми обміну базами даних (0.24 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	bitstream_bc779a44-9ebd-42be-a403-92e5e368e044 [redacted] 12/8/2024 National Technical University "Kharkiv Polytechnic Institute" students papers (National Technical University "Kharkiv Polytechnic Institute" students papers)	15 (2) 0.17 %
2	101з_Биваліна ЮЄ_КацевичВВ_1.docx [redacted] 6/15/2023 Dnipro State Agrarian and Economic University (Відділ внутрішнього аудиту і контролю якості освітньої діяльності)	6 (1) 0.07 %

з Інтернету (14.89 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	http://dspace.opu.ua/jspui/bitstream/123456789/13200/1/31_%D0%9F%D0%97%20%D0%9E%D0%B7%D0%B5%D0%BB.pdf	**767 (47) 8.85 %**
2	https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download	**159 (10) 1.83 %**
3	https://ref-otpbgo.ucoz.org/publ/okhorona_praci/profesijno_zumovleni_zakhvorjuvannja_u_koristuvachiv_vdb/4-1-0-219	**154 (2) 1.78 %**
4	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	**45 (2) 0.52 %**

5	https://card-file.ontu.edu.ua/bitstreams/21173711-5b67-4b87-b17f-6302c25e7a31/download	30 (3) 0.35 %
6	https://card-file.ontu.edu.ua/bitstreams/8999d5af-6274-44f4-ae78-d23e08048d38/download	29 (3) 0.33 %
7	https://www.ukrbanks.info/article/Sertifikaciya-ISO-27001-27701-Sho-ce-take-i-chomu-vona-vazhliva.html	24 (2) 0.28 %
8	https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download	19 (1) 0.22 %
9	https://nupp.edu.ua/uploads/files/0/main/struct/nniab/specialities/191/syllabuses/2024/192bbciok31.pdf	15 (2) 0.17 %
10	http://zakon2.rada.gov.ua/laws/show/537-16	14 (1) 0.16 %
11	https://dnaop.com/html/57320/doc-%D0%94%D0%A1%D0%B0%D0%BD%D0%9F%D0%86%D0%9D_3.3.2.007-98	13 (1) 0.15 %
12	https://thelib.info/psihologiya/248148-parametri-mikroklimatu-virobnichih-primishhen-z-vikoristannyam-vdt/	10 (1) 0.12 %
13	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	6 (1) 0.07 %
14	https://conferences.vntu.edu.ua/public/files/1/vntu_2016_netpub.pdf	5 (1) 0.06 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: **«Комп'ютерна інженерія» Група:** 2БКС- 29

КВАЛІФІКАЦІЙНА
РОБОТА
здобувача **освіти денної форми навчання БКС.** 29.14.000.ДП

КУЗНЄЦОВА
ОЛЕКСАНДРА ОЛЕГОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Комп'ютерна інженерія»
Група: 2 БКС-29

ПОЯСНЮВАЛЬНА ЗАПИСКА
до кваліфікаційної роботи бакалавра на тему:
Аналіз методів комплексного захисту інформації в хмарних сховищах даних

Проєктний матеріал складається з пояснювальної записки на 66 сторінках та графічного (презентаційного) матеріалу на 15 аркушах (слайдах).

Виконавець _____ (Кузнєцов О.О.)
Керівник _____ (Краснієнко Н.В.)

Консультанти:
з розділу охорони праці та техніки безпеки_____ **(Чорновол Н.І.)** з нормоконтролю _____(Петрашова **В.І.) старший** консультант _____(Кривченко Ю. В.) **До захисту допущений**
Завідувач кафедри_____ **(Іванова Л.В.) Завідувач відділення** _____ (