КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Магістерська робота на тему:

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

Виконав
Студент групи БІКСм-24
Улянченко Максим
Керівник: к.т.н., доцент Делембовський М.М.
Кафедра: Кібербезпеки та комп’ютерна інженерія

Київ 2025

Актуальність теми Зростання обсягів даних у розподілених системах, підвищення кіберзагроз та ускладнення архітектури корпоративних мереж і хмарних платформ вимагають ефективного адміністрування компонентів захисту інформації відповідно до вимог законодавства України та міжнародних стандартів ISO/IEC 27001.

Мета Розробка науково обґрунтованих методів та рекомендацій щодо адміністрування компонентів захисту інформації в розподілених комп'ютерних системах з урахуванням сучасних загроз та технологічних вимог.

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

Предмет дослідження Методи та засоби адміністрування компонентів захисту інформації в розподілених комп'ютерних системах.

Завдання

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

Методи

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

Обсяг роботи

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

ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

Поняття та класифікація розподілених комп'ютерних систем

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

Класифікація

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

Загрози та вразливості інформаційних ресурсів у розподіленому середовищі

Класифікація загроз та вразливостей інформаційних ресурсів у розподілених середовищах

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

Принципи та моделі захисту інформації

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

Нормативно-правове забезпечення захисту інформації в Україні та міжнародні стандарти

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

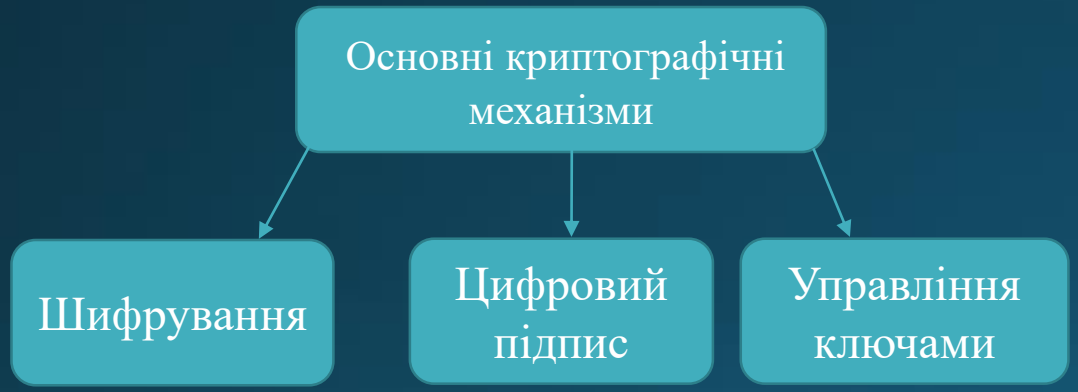
МЕТОДИ ТА ЗАСОБИ АДМІНІСТРУВАННЯ КОМПОНЕНТІВ ЗАХИСТУ ІНФОРМАЦІЇ

Системи керування доступом у розподілених комп'ютерних системах

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

Адміністрування засобів криптографічного захисту та управління ключами

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



Алгоритми шифрування

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

Системи централізованого управління ключами

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

Адміністрування криптографічного захисту

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

Програмні рішення для управління ключами

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

Методи багаторівневої автентифікації та управління ролями

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

Поєднання апаратних та програмних засоби для забезпечення комплексної безпеки

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

Інструменти моніторингу, виявлення вторгнень та реагування на інциденти

Системи моніторингу мережевого трафіку

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

Системи IDS/IPS

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

Інструменти аналізу журналів подій

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

SIEM-системи

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

Інструменти автоматизованого реагування

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

Інструменти аналізу поведінки користувачів

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

Засоби резервування, відновлення та безпечного адміністрування

Види резервного копіювання даних

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

Стратегії відновлення даних

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

Управління доступом

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

Інструменти резервування та відновлення

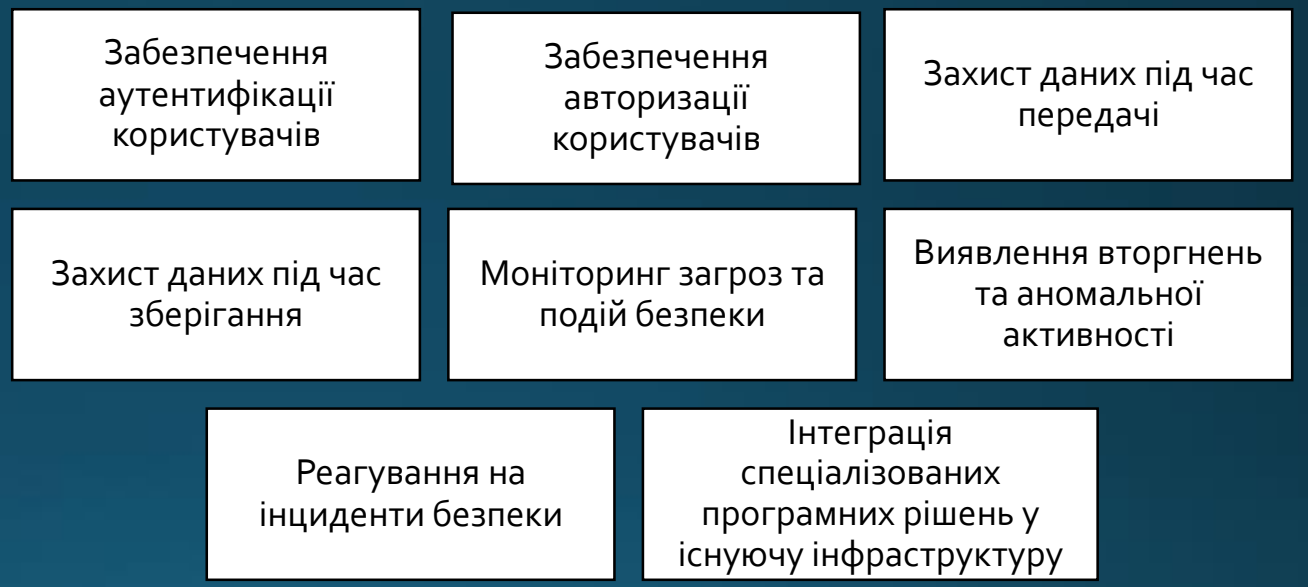
Засіб / технологія	Призначення	Переваги	Особливості використання
Veeam	Резервне копіювання та відновлення віртуальних, фізичних і хмарних середовищ	Автоматизація процесів; висока швидкість роботи з великими обсягами даних	Інтегрується з різними платформами; потребує налаштування політик резервування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

ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДІВ АДМІНІСТРУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Аналіз існуючих програмних рішень для адміністрування безпеки в розподілених системах

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

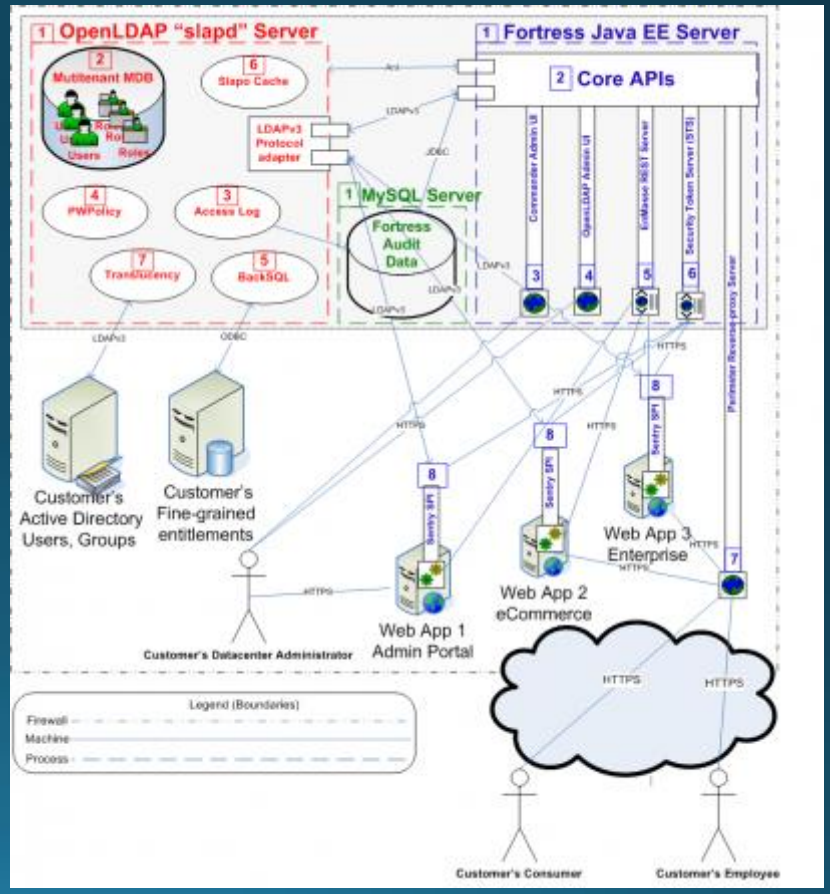
Основні аспекти безпеки в розподілених системах



Apache Fortress

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

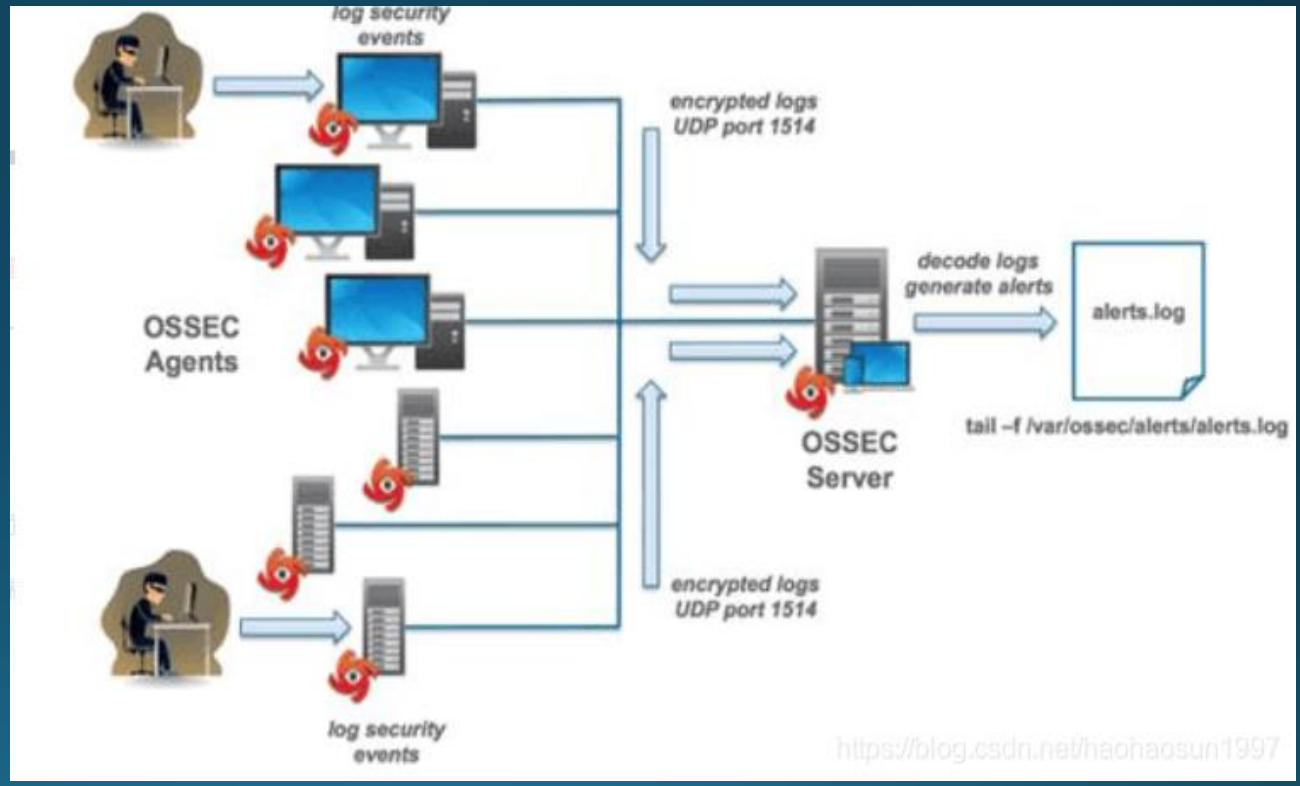
Архітектурне бачення Apache Fortress



OSSEC

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

Система OSSEC



PERMIS

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

Дозволяє використовувати стандарти SAML і XACML

Забезпечує централізоване адміністрування політик без необхідності змінювати код застосунків

Забезпечує сумісність із різними операційними системами та платформами розподілених систем

Quattor

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

Дозволяє централізовано керувати конфігураціями серверів, мережевого обладнання

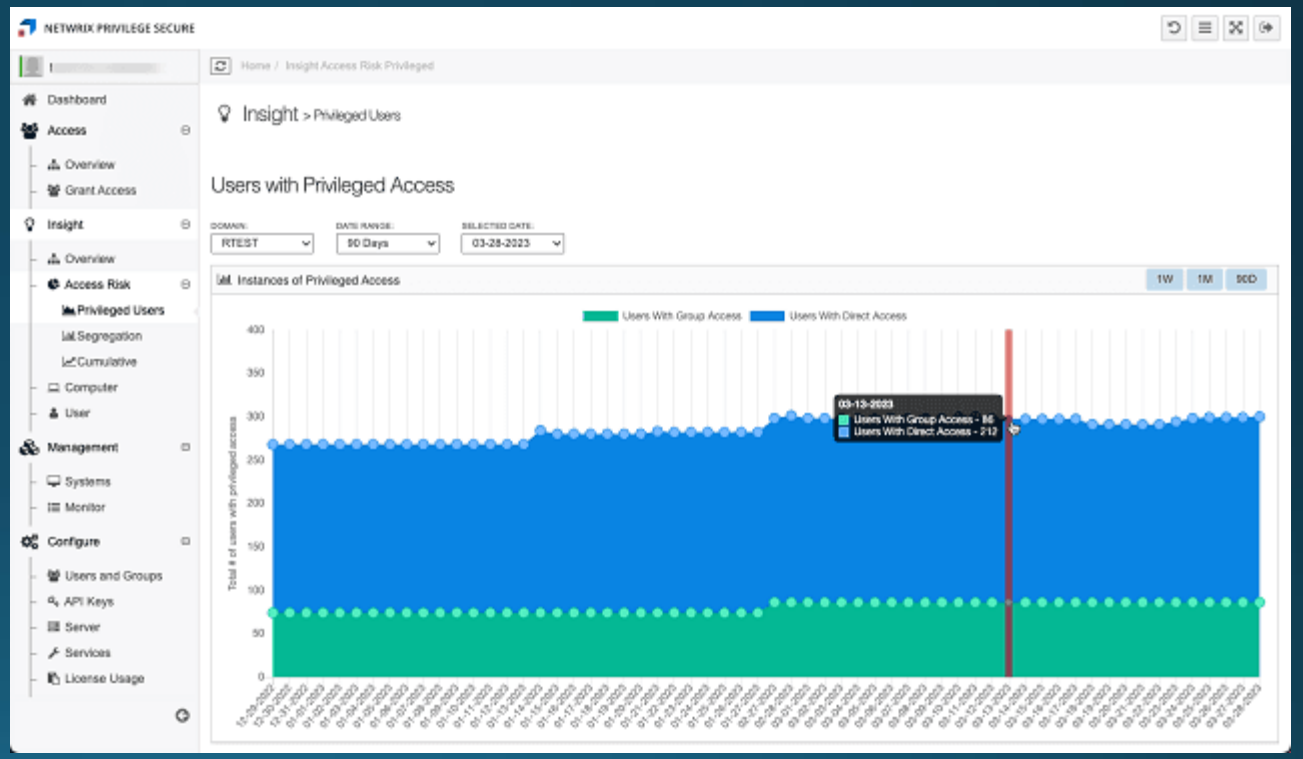
Quattor дозволяє автоматично застосовувати конфігурації, зменшуючи ймовірність людських помилок та підвищуючи надійність системи.

Забезпечує сумісність із різними операційними системами та платформами розподілених систем

Netwrix

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

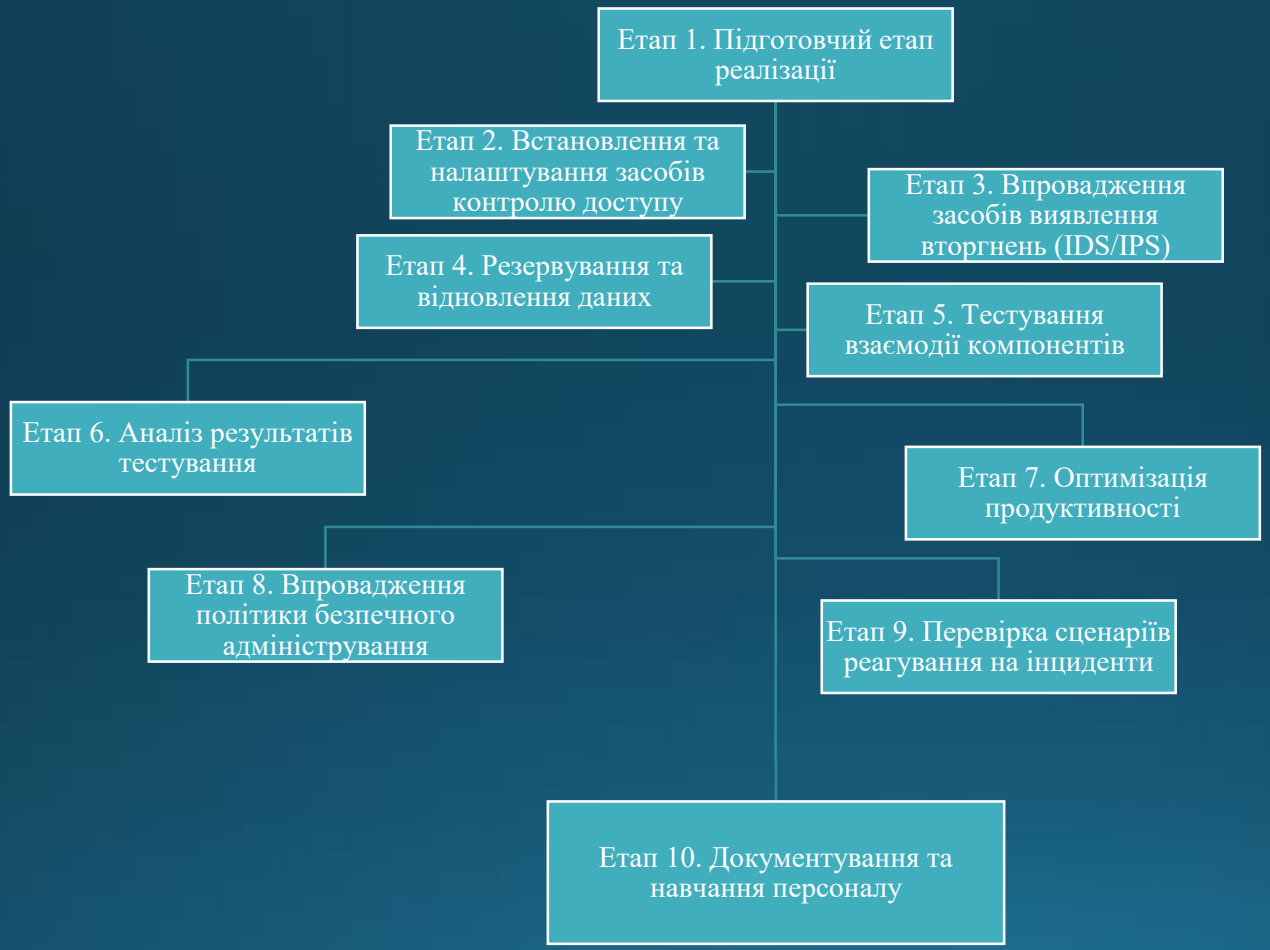
- Відстежує доступ до файлів, налаштувань систем, баз даних та облікових записів, надаючи детальні звіти про активність користувачів.
- Дозволяє централізовано керувати аудитом, забезпечуючи видимість всіх змін у корпоративній інфраструктурі.
- Netwrix підтримує відповідність нормативним вимогам, таким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



Проектування системи адміністрування компонентів захисту для умовної організації

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

Реалізація та тестування обраних засобів захисту



Оцінка ефективності та рекомендації щодо вдосконалення

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

Основні компоненти та їх ефективність

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

ВИСНОВКИ

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

Апробації

СЕРТИФІКАТ

ПРО УЧАСТЬ У КОНФЕРЕНЦІЇ (З ПУБЛІКАЦІЄЮ)

МЦНД

ICSR № 25/2811-387

0,4 ECTS

Рекомендовано Вченою Радою Наукової установи «Інститут науково-технічної інтеграції та співпраці»

Протокол № 47 від 27.11.2025

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

Посвідчення № 497 від 10.06.2025.

Офіційний видавець

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

www.mcnd.org.ua

Улянченко Максим Юрійович

взяв(ла) участь у VI Міжнародній науковій конференції

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

28 листопада 2025 року у м. Полтава, Україна

та опублікував(ла) наукову роботу в збірці конференції

з ISBN 978-617-8312-94-7

DOI 10.62731/mcnd-28.11.2025

ВІЦЕ-ПРЕЗИДЕНТ МЦНД
ГОЛОВА ОРГКОМІТЕТУ
СОТНИК СОЛОМІЯ

МЦНД МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ