ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління ризиками інформаційної безпеки в корпоративних мережах»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми: *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр ЧОРНІЙ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
ЧОРНІЙ Олександр
(прізвище, ім'я)

Керівник д.т.н., проф., ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ – 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SNMP – Simple Network Management Protocol

CPU – Central Processing Unit

RAM – Random Access Memory

NAC – Network Access Control

Triggers – Сповіщення про події у системі моніторингу

Events – Події, зареєстровані системою моніторингу

SSH – Secure Shell

TCP/IP – Transmission Control Protocol

JSON – JavaScript Object Notation

ВСТУП

Актуальність дослідження. Традиційні підходи до управління інформаційною безпекою, орієнтовані на статичні методи захисту та обмеження доступу, стають недостатніми в умовах постійного зростання складності кіберзагроз і ризиків. Сучасні кіберзагрози динамічні та багатогранні, включаючи атаки на мережі, системи зберігання даних, мобільні пристрої та хмарні платформи. У зв'язку із цим, організації стикаються з необхідністю впровадження ефективних моделей управління ризиками, що дозволяють не тільки оперативно виявляти загрози, але й мінімізувати потенційні наслідки.

Система моніторингу Zabbix надає сучасні можливості для моніторингу корпоративних мереж, виявлення вразливостей та реагування на ризики в реальному часі. Завдяки інтеграції з корпоративними інформаційними системами, Zabbix забезпечує збір даних, автоматизацію аналізу та централізоване управління подіями безпеки.

Технологія управління ризиками інформаційної безпеки на основі Zabbix забезпечує комплексний підхід до моніторингу, виявлення та мінімізації ризиків. Особливістю Zabbix є його адаптивність до змін у корпоративних мережах та можливість інтеграції з іншими системами безпеки. Вона дозволяє виявляти вразливості, формувати звіти, аналізувати журнали подій і оптимізувати заходи реагування. В умовах, коли швидкість реагування на інциденти визначає рівень безпеки організації, використання Zabbix є необхідним для захисту даних та безперервності бізнес-процесів.

Вищезазначене підтверджує актуальність теми дослідження, основний зміст якої становлять розробка та впровадження моделі управління ризиками інформаційної безпеки корпоративних мереж із використанням системи Zabbix.

Об'єкт дослідження – управління ризиками інформаційної безпеки в

корпоративних мережах.

Предмет дослідження – технологія управління ризиками інформаційної безпеки корпоративних мереж із використанням системи моніторингу Zabbix.

Мета роботи – розробити модель управління ризиками інформаційної безпеки корпоративної мережі та рекомендації щодо її впровадження.

Наукові завдання:

дослідити актуальність проблеми управління ризиками в корпоративних мережах;

проаналізувати сучасні підходи до управління ризиками інформаційної безпеки;

дослідити функціональні можливості системи моніторингу Zabbix для забезпечення інформаційної безпеки;

проаналізувати методи та засоби управління ризиками ІБ із застосуванням технологій Zabbix;

розробити модель управління ризиками інформаційної безпеки з використанням Zabbix.

Методи дослідження – опрацювання наукової та технічної літератури, аналіз міжнародних стандартів, дослідження можливостей системи Zabbix, експериментальне налаштування та тестування функціоналу.

Практичне значення одержаних результатів: Запропоновано модель управління ризиками, що враховує специфіку корпоративних мереж і дозволяє виявляти, аналізувати та мінімізувати ризики інформаційної безпеки з використанням Zabbix. Розроблено практичні рекомендації для фахівців у сфері кібербезпеки щодо впровадження системи моніторингу Zabbix, як інструмента для зниження ризиків інформаційної безпеки.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ТЕХНОЛОГІЙ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Сутність і класифікація ризиків інформаційної безпеки

Сутність ризиків інформаційної безпеки.

Ризики інформаційної безпеки (ІБ) визначаються як потенційна можливість настання подій, які можуть негативно вплинути на конфіденційність, цілісність або доступність інформаційних активів. Ризики виникають унаслідок вразливостей, які експлуатуються загрозами.

Основні компоненти ризиків:

1. **Активи** – ресурси, які необхідно захищати (дані, апаратне забезпечення, програми, співробітники);

2. **Загрози** – дії або події, які можуть спричинити шкоду активам (хакерські атаки, технічні збої);

3. **Вразливості** – слабкі місця в системі, які дозволяють загрозам завдати шкоди;

4. **Наслідки** – результат реалізації ризику (фінансові збитки, репутаційні втрати).

Ризик можна описати формулою: $R=P\times I$ де:

- R – рівень ризику,
- P – ймовірність загрози,
- I – ступінь впливу (наслідки).

Ймовірність реалізації загрози (P):

Відображає, наскільки вірогідно, що конкретна загроза буде реалізована.

Значення може варіюватися від 0 (загроза нереалізована) до 1 (загроза обов’язково відбудеться).

Ймовірність залежить від таких факторів:

- Стану захисних механізмів (наприклад, наявність антивірусного ПЗ знижує ймовірність зараження);
- Типу загрози (деякі атаки, як-от фішинг, мають високий відсоток успіху);
- Частоти взаємодії з уразливими елементами системи.

Вплив(*I*):

Відображає рівень шкоди, завданої активам у разі реалізації загрози. Вимірюється за різними шкалами: фінансова шкода (грошовий еквівалент), операційні втрати (зупинка бізнес-процесів), репутаційні збитки тощо.

Приклади оцінки впливу:

- **Критичний вплив:** втрата доступу до серверів призводить до значних фінансових втрат;
- **Середній вплив:** пошкодження одного робочого місця впливає на окремий департамент;
- **Низький вплив:** короткочасне уповільнення мережі, яке не викликає значних проблем.

Стосовно класифікації ризиків інформаційної безпеки, є важливим етапом у процесі управління ризиками. Вона дозволяє структурувати ризики, визначати їхню природу, пріоритетність, а також вибирати відповідні методи їх зменшення (див. таб. 1.1).

Основні аспекти класифікації ризиків:

За рівнем реалізації загроз:

- **Потенційні загрози:** ризики, що можуть реалізуватися за певних умов (наприклад, вразливість у програмному забезпеченні, яка ще не використовується);
- **Активні загрози:** ризики, що вже реалізуються (DDoS-атака, яка триває);
- **Латентні загрози:** ризики, які можуть залишитися непоміченими (встановлений бекдор).

За типом впливу на організацію:

- **Стратегічні:** довгостроковий вплив, наприклад, витік комерційної таємниці.
- **Операційні:** короткострокові наслідки, наприклад, збій у роботі сервера.

За джерелом загроз:

- **Внутрішні загрози:** дії співробітників компанії, недотримання політик.
- **Зовнішні загрози:** атаки ззовні, зокрема кібершпигунство.

Таблиця 1.1 – Приклади ризиків інформаційної безпеки

Категорія	**Приклад**	**Ймовірність**	**Вплив**
Внутрішні ризики	Витік даних через USB-пристрої	Середня	Високий
Загрози хмарних рішень	Несанкціонований доступ до хмарних облікових записів	Висока	Критичний
Ризики IoT (Internet of Things)	Використання вразливих пристроїв (розумні камери тощо)	Середня	Високий
Фізичні ризики	Викрадення або пошкодження обладнання	Низька	Середній
Латентні загрози	Наявність невиявлених бекдорів у програмному забезпеченні	Низька	Критичний

1. За походженням загроз.

Ця класифікація базується на джерелах, звідки виникають загрози для інформаційної безпеки:

1) Технічні загрози:

Пов’язані з несправностями або особливостями технічних систем.

- Збої обладнання (жорсткі диски, сервери);
- Помилки у програмному забезпеченні;
- Вразливості мережевого обладнання.

2) Людські загрози: Виникають через дії або бездіяльність людей. Вони поділяються на:

- Навмисні загрози: хакерські атаки, саботаж, промислове шпигунство.
- Ненавмисні загрози: помилки користувачів, неправильна конфігурація систем, нехтування політиками безпеки.

3) Природні загрози: Ризики, які не залежать від людської діяльності.

- Пожежі, землетруси, повені;
- Актуальні перебої в електропостачанні через природні катаклізми.

1.2 Методи і моделі управління ризиками в корпоративних мережах

Управління ризиками інформаційної безпеки в корпоративних мережах — це комплексний процес, який включає ідентифікацію, оцінку, контроль та моніторинг ризиків, пов’язаних із захистом інформаційних активів. В основі цього процесу лежать методи та моделі, які дозволяють структурувати та організувати управління ризиками, забезпечуючи їх ефективне зниження.

Методи та моделі управління ризиками в корпоративних мережах є важливим інструментом для забезпечення інформаційної безпеки організацій. Корпоративні мережі стають все складнішими, інтегруючи хмарні технології, мобільні пристрої та розподілену інфраструктуру. У цьому контексті управління ризиками виступає основним процесом, який дозволяє передбачити, оцінити та мінімізувати потенційні загрози.

Основою управління ризиками є ідентифікація критичних активів організації. Це можуть бути сервери, бази даних, інформаційні системи або мережеві пристрої. Після визначення активів наступним кроком є оцінка загроз. Загрози можуть походити як із зовнішнього середовища (кібератаки, DDoS, хакерські зломи), так і бути внутрішніми (помилки співробітників, інсайдерські загрози). Також розглядаються природні катаклізми, такі як пожежі або затоплення дата-центрів.

Після ідентифікації загроз відбувається аналіз вразливостей. Це слабкі місця у системі, які можуть бути використані для реалізації загроз. Наприклад, відсутність оновлень програмного забезпечення, слабкі паролі або неправильно налаштовані мережеві пристрої створюють умови для атак. Оцінка вразливостей дозволяє зрозуміти, наскільки система готова протистояти загрозам.

Методи управління ризиками.

Методи управління ризиками спрямовані на мінімізацію або повне усунення потенційних загроз. Основні підходи до управління ризиками включають:

1. Уникнення ризику (*Risk Avoidance*) - суть методу полягає в повному виключенні діяльності, яка може спричинити ризик. На прикладі відмови від використання незахищених протоколів передачі даних.

2. Зменшення ризику (*Risk Reduction*) - впровадження заходів, що знижують ймовірність реалізації загрози або зменшують її вплив. Використання фаєрволів, систем виявлення та запобігання вторгнень (IDS/IPS).

3. Передача ризику (*Risk Transfer*) - перенесення відповідальності за можливі збитки на третю сторону. Страхування кіберризиків або аутсорсинг захисту інформації.

4. Прийняття ризику (*Risk Acceptance*) - визнання ризику та погодження з можливими наслідками. Використовується, коли вартість усунення ризику перевищує потенційні збитки.

Моделі управління ризиками.

Моделі забезпечують структурований підхід до управління ризиками, дозволяючи ефективніше оцінювати та контролювати їх. Найпопулярніші моделі включають (див. таб. 1.2):

✓ FAIR (Factor Analysis of Information Risk). FAIR орієнтована на кількісну оцінку ризиків, надаючи бізнесу чітке розуміння фінансових втрат,

пов’язаних із ризиками. Ця модель підходить для організацій, які прагнуть отримати конкретні числові дані для прийняття обґрунтованих рішень.

Основні компоненти моделі FAIR:

1. Частота загрози: як часто загроза може реалізуватися.
2. Ймовірність експлуатації вразливості: наскільки легко загрозі скористатися слабкістю системи.
3. Потенційні втрати**:** оцінка можливих збитків у разі реалізації загрози.

FAIR також дозволяє враховувати зовнішні та внутрішні фактори, які впливають на ризики. Наприклад, організація може врахувати не лише технічний аспект ризику, але й економічний чи репутаційний вплив.

✓ OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). OCTAVE призначена для стратегічного управління ризиками, враховуючи пріоритетність активів і загроз. Ця модель є гнучкою, що дозволяє адаптувати її до потреб середніх і великих організацій.

Основні етапи OCTAVE:

1. Ідентифікація критичних активів: визначення активів, від яких залежить діяльність організації.
2. Аналіз загроз і вразливостей: оцінка загроз, які можуть вплинути на ці активи, та виявлення вразливостей.
3. Визначення заходів зниження ризику: формування конкретних рекомендацій для зменшення впливу загроз.

OCTAVE враховує не лише технічні аспекти ризиків, а й людський фактор. Наприклад, модель дозволяє оцінити ризики, пов’язані з недостатньою підготовкою персоналу.

✓ **ISO/IEC 27005 Risk Management Framework**. Ця модель інтегрує управління ризиками у систему управління інформаційною безпекою (ISMS) і базується на циклі PDCA (Plan-Do-Check-Act), що забезпечує постійне вдосконалення процесів.

Основні етапи моделі ISO/IEC 27005:

1. Встановлення контексту: визначення цілей, активів і зовнішніх факторів, які впливають на ризики.

2. Оцінка ризиків: аналіз загроз, вразливостей та впливу на активи.

3. Обробка ризиків: вибір заходів для мінімізації або усунення ризиків.

4. Моніторинг і перегляд: регулярний контроль за ефективністю впроваджених заходів.

Ця модель широко використовується в організаціях, які прагнуть відповідати міжнародним стандартам інформаційної безпеки.

- ✓ NIST SP 800-30 Risk Management Guide.

Ця модель була розроблена Національним інститутом стандартів і технологій США (NIST) для управління ризиками в інформаційних системах, зокрема для державних структур. Вона базується на глибокому аналізі ризиків і детальному документуванні процесу.

Ключові етапи NIST SP 800-30:

1. Підготовка до оцінки ризиків: визначення цілей оцінки, меж аналізу, залучення відповідальних осіб.

2. Ідентифікація загроз: класифікація загроз (людські, технічні, природні) та оцінка їхньої актуальності.

3. Аналіз вразливостей: виявлення слабких місць у системі та їхнього впливу на організацію.

4. Визначення ймовірності реалізації загроз: використання статистичних даних та експертних оцінок.

5. Оцінка впливу: визначення наслідків для бізнесу у разі реалізації загроз.

6. Визначення рівня ризику: комбінація ймовірності та впливу.

7. Документування та звітність: створення детального звіту з рекомендаціями.

Особливості NIST SP 800-30:

- ➢ Ретельний аналіз і документація дозволяють враховувати всі можливі аспекти ризиків.

- Акцент на формалізації процесу робить цю модель особливо корисною для великих організацій і державних установ.

Таблиця 1.2 – Порівняння моделей управління ризиками

Модель	Ціль	Метод	Переваги	Недоліки
FAIR	Кількісна оцінка ризиків	Статистичний аналіз	Точна оцінка впливу ризиків	Вимагає великого обсягу даних
OCTAVE	Стратегічне управління ризиками	Інтерв'ю, аналіз активів	Оцінка критичних активів	Трудомісткий процесс
ISO/IEC 27005	Управління ризиками в рамках ISMS	Циклічний підхід	Відповідність міжнародним стандартам	Загальні рекомендації
NIST SP 800-30	Комплексна оцінка ризиків у державних структурах	Документована процедура оцінки	Простота інтеграції	Може бути складним у великих мережах

У корпоративних мережах методи та моделі управління ризиками мають бути адаптовані до специфіки організації. Наприклад, для компаній, які використовують хмарні сервіси, критичними є ризики доступності та конфіденційності. У таких випадках важливо впроваджувати заходи щодо забезпечення резервного копіювання, а також використовувати багатофакторну автентифікацію для захисту доступу до хмарних облікових записів. Для організацій, які залежать від фізичної інфраструктури, важливим є забезпечення її фізичного захисту, наприклад, шляхом встановлення систем відеоспостереження та контролю доступу.

Процес управління ризиками не завершується впровадженням захисних заходів. Постійний моніторинг ризиків і перегляд політик безпеки є

необхідним для того, щоб адаптуватися до нових загроз та умов. Кіберзагрози постійно еволюціонують, і організація, яка не здійснює регулярного аудиту своєї системи, залишається вразливою. Таким чином, ефективне управління ризиками інформаційної безпеки в корпоративних мережах є не лише технічним, а й стратегічним завданням, яке впливає на загальний успіх бізнесу.

Один із ключових аспектів управління ризиками — це формування контексту, в якому вони оцінюються. Для корпоративних мереж контекст включає аналіз бізнес-процесів, визначення ролі інформаційних активів і оцінку впливу ризиків на організаційні цілі. Наприклад, для компанії, що працює у фінансовому секторі, найважливішими активами є клієнтські дані, а головною загрозою — витік або викрадення цієї інформації. У цьому випадку ризик має не лише фінансові наслідки, але й репутаційні, які важко оцінити в грошовому еквіваленті.

Після формування контексту проводиться оцінка ризиків. Сучасні корпоративні мережі характеризуються високою динамікою змін: додаються нові сервери, інтегруються хмарні сервіси, співробітники працюють з різних місць через VPN. Це вимагає гнучкості в підходах до оцінки ризиків. Наприклад, статичні моделі ризиків, які враховують лише поточний стан інфраструктури, поступаються місцем динамічним моделям. Такі моделі дозволяють адаптувати оцінку ризиків у реальному часі, враховуючи зміни у конфігурації мережі та нові загрози.

Однією з проблем управління ризиками в корпоративних мережах є їхній міждисциплінарний характер. Наприклад, багато загроз виникають через людський фактор, як-от недостатнє навчання персоналу, нехтування політиками безпеки або фішингові атаки. У таких випадках технічних заходів, як-от встановлення фаєрволів чи антивірусного ПЗ, недостатньо. Важливо впроваджувати програми підвищення обізнаності співробітників про ризики, розробляти політики безпеки та проводити регулярні тренінги.

Ще одним викликом є оцінка залишкових ризиків, які залишаються навіть після впровадження заходів захисту. Це такі ризики, які не можна повністю усунути через технічні або фінансові обмеження. Наприклад, організація може впровадити систему резервного копіювання для захисту даних, але залишковий ризик втрати даних через збій у резервному сервері залишається. Для зменшення цього ризику часто використовується підхід комбінованого захисту — резервування не лише даних, але й обладнання, програмного забезпечення та навіть персоналу, відповідального за обслуговування.

Окрему увагу варто приділити автоматизації управління ризиками. Сучасні корпоративні мережі генерують величезну кількість даних, які можуть використовуватися для аналізу ризиків. Інструменти типу SIEM (Security Information and Event Management) дозволяють збирати, обробляти та аналізувати ці дані в реальному часі. Наприклад, SIEM-система може виявити аномальну активність у мережі, яка може бути ознакою внутрішньої загрози, наприклад, компрометації облікового запису співробітника.

Ще одним важливим напрямом є інтеграція управління ризиками з бізнес-аналітикою. Сьогодні ризики інформаційної безпеки дедалі частіше розглядаються в ширшому контексті загальних бізнес-ризиків. Це означає, що управління ризиками ІБ має враховувати економічні, репутаційні, правові та соціальні наслідки. Наприклад, витік конфіденційних даних у компанії, яка працює з міжнародними клієнтами, може призвести до штрафів за порушення регуляторних вимог, як-от GDPR. Інтеграція бізнес-аналітики дозволяє враховувати ці наслідки у процесі прийняття рішень.

Ключовим фактором успіху управління ризиками є постійний моніторинг та оцінка ефективності впроваджених заходів. Регулярний аудит системи безпеки, тестування на проникнення (penetration testing) та аналіз журналів подій дозволяють виявляти нові загрози та вдосконалювати політики безпеки. Наприклад, регулярне тестування може показати, що певний сегмент мережі є більш вразливим до атак через застаріле

обладнання. У цьому випадку рішенням може бути модернізація обладнання або посилення захисту цієї ділянки.

Однак управління ризиками в корпоративних мережах не є завершеним процесом. Це постійний, регулярний цикл роботи, який включає в себе аналіз нових загроз в реаліях світу, оцінку існуючих заходів захисту, впровадження нових технологій і регулярний моніторинг. Такий підхід забезпечує гнучкість і адаптивність системи управління ризиками, дозволяючи ефективно реагувати на виклики сучасного кіберсередовища.

1.3 Огляд існуючих систем управління ризиками інформаційної безпеки

Системи управління ризиками інформаційної безпеки (ІБ) створені для автоматизації та вдосконалення процесів оцінки, моніторингу та обробки ризиків. Вони допомагають компаніям ідентифікувати потенційні загрози, оцінювати їхній вплив і впроваджувати відповідні заходи захисту. У сучасному світі ці системи є невід’ємною частиною ефективної стратегії кіберзахисту. Вибір відповідної системи управління залежить від багатьох факторів: масштабу мережі, фінансових ресурсів організації, наявності експертів для налаштування та підтримки системи, а також специфічних вимог до безпеки. Порівняння цих платформ дозволяє зрозуміти, яка з них найкраще відповідає конкретним потребам організації (див. таб 1.3).

Zabbix – одна з популярних платформ для моніторингу мережевої інфраструктури, яка також може бути використана для управління ризиками інформаційної безпеки. Хоча Zabbix здебільшого асоціюється з моніторингом продуктивності серверів і мереж, її можливості дозволяють ефективно використовувати систему для оцінки ризиків у реальному часі.

Zabbix надає функціонал для збору даних із різних джерел, таких як сервери, мережеві пристрої, бази даних та додатки, і відстежує аномалії у функціонуванні. Наприклад, у разі перевищення допустимого рівня

використання ресурсів або раптових змін у мережевій активності, Zabbix може автоматично створювати повідомлення про можливу загрозу. Ця функція є важливою для управління ризиками, оскільки дозволяє виявляти проблеми до їхнього переростання у критичні інциденти.

Сильна сторона Zabbix — це її **гнучка система звітності**, яка дозволяє створювати детальні графіки та таблиці, відображаючи зміни у параметрах мережі. Це допомагає оцінювати залишкові ризики та планувати заходи для їхнього усунення.

IBM OpenPages - орієнтована на автоматизацію процесів управління ризиками та забезпечення відповідності регуляторним стандартам. Завдяки інтеграції з IBM Watson ця платформа використовує штучний інтелект для аналізу великих обсягів даних, що дозволяє прогнозувати ризики та ідентифікувати потенційні загрози. Підтримка багатьох мов і регіональних стандартів робить OpenPages універсальним рішенням для великих організацій, які працюють у різних країнах. Проте її висока вартість та вимоги до апаратного забезпечення можуть стати бар’єром для впровадження в середніх і малих компаніях.

RiskWatch - приклад більш гнучкого рішення, орієнтованого на постійний моніторинг і оцінку ризиків. Її перевага полягає в простоті інтеграції з існуючими системами та підтримці стандартів, таких як ISO/IEC 27001 і NIST. RiskWatch дозволяє організаціям автоматично формувати звіти, спрощуючи процес документування. Завдяки можливості роботи в хмарному середовищі ця система забезпечує легкий доступ до інструментів аналізу ризиків для компаній, які мають обмежений бюджет або технічні ресурси.

Проте вона може поступатися за функціональністю потужнішим платформам, відносно RSA Archer, що робить її менш придатною для великих організацій із складною інфраструктурою.

RSA Archer, яка надає комплексні рішення для інтеграції процесів управління ризиками в загальну стратегію бізнесу. Її модульний підхід дозволяє адаптувати платформу до специфічних потреб організації,

інтегруючи її з іншими системами, такими як SIEM або рішеннями для виявлення вразливостей. Завдяки підтримці стандартів, на прикладі ISO або GDPR, компанії отримують інструмент для ефективного управління відповідністю нормативним вимогам. Однак платформа має певні недоліки, зокрема високу вартість, що обмежує її доступність для малих підприємств, а також складність впровадження, яка вимагає залучення кваліфікованих спеціалістів.

Splunk - відома своєю здатністю обробляти великі обсяги даних у реальному часі. Її аналітичні інструменти дозволяють швидко виявляти аномальну активність у мережі, що може свідчити про можливі загрози. Splunk ефективно інтегрується з існуючими рішеннями безпеки, дозволяючи компаніям отримувати централізований контроль над усіма аспектами інформаційної безпеки. Проте ця система вимагає значних інвестицій як у впровадження, так і в навчання персоналу для роботи з нею, що обмежує її використання в невеликих компаніях.

Таблиця 1.3 - Таблиця порівняння систем управління ризиками

Система	Основний фокус	Переваги	Обмеження
RSA Archer	Управління ризиками в корпоративному масштабі	Потужна аналітика, відповідність стандартам	Висока вартість
IBM OpenPages	Інтеграція штучного інтелекту для прогнозування	Розширений функціонал, гнучкість	Вимоги до ресурсів
RiskWatch	Простота використання для середніх організацій	Доступність, хмарні рішення	Обмежені функції для великих мереж
Splunk	Аналіз даних у реальному часі	Швидке виявлення аномалій	Вартість впровадження
Zabbix	Моніторинг продуктивності та базовий аналіз ризиків	Гнучкість, інтеграція, безкоштовна основа	Обмежені функції для повного управління ризиками

Таблиця демонструє, як різні компоненти корпоративної мережі (сервери, клієнтські пристрої, хмарні сервіси) взаємодіють із системами управління ризиками. Кожна система представлена як центральний вузол, пов'язаний із точками моніторингу, оцінки ризиків та інструментами звітності.

Ефективність систем управління ризиками залежить від здатності організації правильно інтегрувати їх у свою інфраструктуру, враховуючи особливості мережі, обсяг даних і бюджет. Використання таких систем дозволяє компаніям зменшувати ймовірність реалізації загроз і мінімізувати їхній вплив на бізнес-процеси.

1.4 Стандарти та нормативні документи в галузі управління ризиками

Стандарти та нормативні документи в управлінні ризиками інформаційної безпеки відіграють ключову роль у забезпеченні системного та організованого підходу до оцінки, моніторингу та мінімізації ризиків. Вони створюють універсальні рекомендації для організацій різного масштабу, допомагаючи інтегрувати управління ризиками у загальну стратегію інформаційної безпеки. Вони допомагають структурувати підходи до ідентифікації, оцінки, зменшення та моніторингу ризиків, що виникають у корпоративних мережах.

Використання стандартів дозволяє організаціям адаптувати найкращі світові практики до власних потреб, забезпечуючи відповідність міжнародним та регіональним регуляторним вимогам.

Корпоративні мережі, які працюють у динамічному середовищі кіберзагроз, потребують універсальних і детальних рекомендацій для мінімізації ризиків. Вибір відповідного стандарту залежить від типу організації, її масштабів та специфіки. Наприклад, компанії, що працюють у фінансовому секторі, можуть віддавати перевагу стандартам з детальним аналізом ризиків, на прикладі **NIST SP 800-30**, у той час як організації з

глобальною присутністю можуть зосередитися на впровадженні **ISO/IEC 27005** для інтеграції управління ризиками у свою загальну систему управління інформаційною безпекою.

Однією з важливих переваг використання стандартів є їхня здатність створювати єдиний підхід до вирішення проблем. Це дозволяє організаціям узгоджувати свої дії з міжнародними партнерами, клієнтами та регуляторами. Наприклад, застосування ISO 31000 може бути корисним для компаній, які працюють у багатьох юрисдикціях, де управління ризиками охоплює не лише технічні, але й правові, репутаційні та соціальні аспекти.

Ще одним ключовим аспектом стандартів є їхнє спрямування на постійне вдосконалення. Більшість стандартів, таких як **ISO/IEC 27005**, базуються на циклі PDCA (Plan-Do-Check-Act), який дозволяє організаціям не лише визначати поточні ризики, але й адаптуватися до нових викликів. Наприклад, зростання популярності хмарних сервісів, мобільних пристроїв і віддаленої роботи створює нові ризики, які потребують оперативного реагування.

Крім того, стандарти створюють можливість для формалізації управління ризиками. Це означає, що організація може задокументувати свої процеси, що важливо для проходження аудитів, отримання сертифікації та підтримки довіри з боку клієнтів і партнерів. Наприклад, відповідність **ISO/IEC 27001**, що включає аспекти ISO/IEC 27005, часто є обов’язковою умовою для компаній, які працюють із великими корпораціями або урядовими структурами.

Важливо розуміти, що стандарти не є універсальними рецептами, які повністю вирішують усі проблеми кібербезпеки. Вони надають рамкові рекомендації, які організації мають адаптувати до своїх конкретних потреб. Наприклад, хоча **NIST SP 800-30** забезпечує детальний аналіз ризиків, він може бути надто складним для малих компаній із обмеженими ресурсами. У таких випадках кориснішим може бути використання більш загальних стандартів, як-от ISO 31000, який дозволяє зосередитися на ключових аспектах управління ризиками без надмірної деталізації.

Інтеграція кількох стандартів також є поширеною практикою. Наприклад, організація може використовувати **COBIT** для управління IT-процесами, одночасно застосовуючи **ISO/IEC 27005** для управління ризиками у своїй системі інформаційної безпеки. Такий підхід дозволяє забезпечити гармонійне поєднання стратегічного та операційного рівнів управління.

Стандарти та нормативні документи створюють основу для ефективного управління ризиками, сприяючи зменшенню кількості інцидентів і збитків, а також покращуючи репутацію та конкурентоспроможність організацій у цифрову епоху (див. таб. 1.4).

ISO/IEC 27005 — це міжнародний стандарт, який спеціалізується на управлінні ризиками в контексті системи управління інформаційною безпекою (ISMS). Цей стандарт забезпечує структурований підхід до ідентифікації, оцінки та мінімізації ризиків, що дозволяє організаціям відповідати вимогам ISO/IEC 27001.

Ключові елементи ISO/IEC 27005:

1. Встановлення контексту - організація визначає мету управління ризиками, межі аналізу та зовнішні/внутрішні фактори.

2. Оцінка ризиків - включає ідентифікацію активів, загроз і вразливостей, оцінку ймовірності реалізації ризику та його впливу.

3. Обробка ризиків - розробка заходів для мінімізації, передачі, уникнення або прийняття ризиків.

4. Моніторинг і перегляд - регулярне оновлення оцінок ризиків та заходів захисту для врахування змін у бізнес-середовищі.

Особливість ISO/IEC 27005 в тому, що він орієнтований на інтеграцію ризик-менеджменту в загальну стратегію інформаційної безпеки, що робить його придатним для організацій різного масштабу.

Документ **NIST SP 800-30** від Національного інституту стандартів і технологій США (NIST) є основою для управління ризиками в державних установах і приватних компаніях США. Він забезпечує детальну методологію оцінки ризиків для інформаційних систем.

Ключові етапи NIST SP 800-30:

1. Підготовка - визначення цілей, меж аналізу та ролей відповідальних осіб.

2. Ідентифікація ризиків - аналіз загроз, вразливостей і впливу на організацію.

3. Аналіз ймовірності та впливу – оцінка можливості реалізації ризиків та їхнього впливу на інформаційні активи.

4. Розробка плану управління ризиками - Вибір заходів для зниження ризиків.

5. Документування результатів - Створення звітів, які містять оцінки ризиків та рекомендації.

NIST SP 800-30 підходить для глибокого аналізу ризиків, особливо у великих організаціях із багаторівневою інфраструктурою.

ISO 31000 — це стандарт, орієнтований на загальні принципи управління ризиками, який можна адаптувати до будь-якої галузі, включаючи інформаційну безпеку. Він надає рекомендації щодо процесу управління ризиками та включає детальні кроки для ідентифікації, оцінки та обробки ризиків.

Основні аспекти ISO 31000:

1. Принципи управління ризиками - визначення основних цінностей, таких як систематичність, прозорість і адаптивність.
2. Процес управління ризиками - включає встановлення контексту, оцінку ризиків, моніторинг і перегляд.
3. Фреймворк - інтеграція управління ризиками в корпоративну культуру організації.

ISO 31000 застосовується до будь-якої галузі, що робить його універсальним інструментом для побудови політики управління ризиками.

COBIT (Control Objectives for Information and Related Technologies) є фреймворком, який визначає контрольні механізми для управління інформаційними технологіями. COBIT інтегрує управління ризиками в

управління IT-процесами організації. COBIT підходить для організацій, які прагнуть інтегрувати управління ризиками в загальне управління IT.

Основні компоненти:

1. Контрольні цілі - забезпечують стандартизований підхід до управління інформаційними ризиками.
2. Ролі та відповідальність - визначення відповідальних осіб для кожного процесу.
3. Метрики - вимірювання ефективності управління ризиками.

Таблиця 1.4- Порівняння ключових стандартів управління ризиками ІБ

Стандарт	**Основний фокус**	**Переваги**	**Обмеження**
ISO/IEC 27005	Управління ризиками в контексті ISMS	Ітеграція з ISO 27001,систематичність	Загальні рекомендації без деталей
NIST SP 800-30	Оцінка ризиків для інформаційних систем	Глибина аналізу, формалізація процесів	Орієнтований на специфічні сфери
ISO 31000	Загальні принципи управління ризиками	Універсальність, адаптивність	Не містить специфічних методик ІБ
COBIT	Інтеграція управління ризиками в IT-процеси	Орієнтація на бізнес-цілі, деталізація	Складність впровадження у великих мережах

Стандарти та нормативні документи створюють міцну основу для управління ризиками інформаційної безпеки. Вибір відповідного стандарту залежить від специфіки організації, її масштабів, регуляторних вимог та інфраструктури. Наприклад, ISO/IEC 27005 є ідеальним вибором для організацій, які використовують систему управління інформаційною безпекою, тоді як NIST SP 800-30 підходить для детального аналізу ризиків у

складних мережах. Інтеграція цих стандартів забезпечує всебічний підхід до управління ризиками, що відповідає сучасним викликам кібербезпеки.

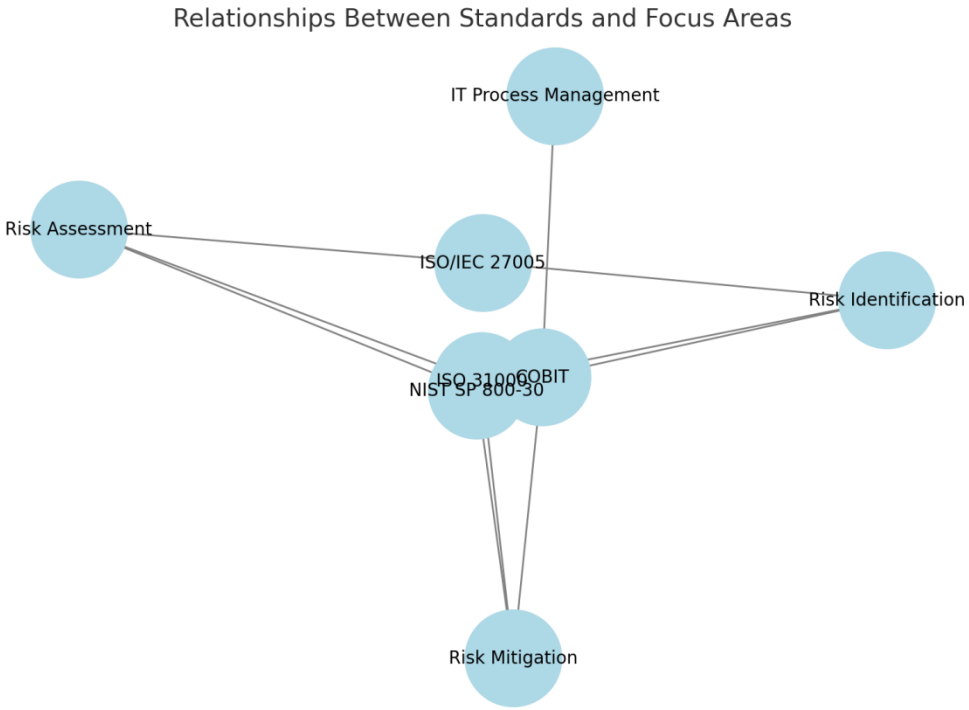


Рис.1.1 - Взаємозв'язок між основними стандартами управління ризиками ІБ

Це допомагає візуалізувати, які стандарти покривають певні етапи процесу управління ризиками, такі як ідентифікація, оцінка, пом'якшення ризиків та управління IT-процеса

- **ISO/IEC 27005:** Основний акцент на ідентифікації та оцінці ризиків у рамках системи управління інформаційною безпекою.
- **NIST SP 800-30:** Покриває всі аспекти: від ідентифікації до пом'якшення ризиків.
- **ISO 31000:** Фокусується на загальних принципах управління ризиками, охоплюючи всі ключові аспекти.
- **COBIT:** Спрямований на інтеграцію управління ризиками в управління IT-процесами.

Висновок до першого розділу

Проаналізовано сутність і класифікацію ризиків інформаційної безпеки, що дозволило визначити їх вплив на функціонування корпоративних мереж.

Встановлено, що управління ризиками інформаційної безпеки є важливим елементом загальної стратегії захисту, оскільки потенційні загрози можуть мати значний вплив на фінансовий стан організації, її репутацію та відповідність законодавчим нормам.

Зроблено висновок, що сучасні загрози інформаційним системам постійно змінюються, і це вимагає динамічного підходу до їх виявлення та мінімізації. Використання методів і моделей управління ризиками, включаючи ISO/IEC 27005 і NIST SP 800-30, дозволяє створити комплексну систему ідентифікації та контролю ризиків.

Підкреслено важливість впровадження стандартів та нормативних документів у процеси забезпечення інформаційної безпеки. Аналіз існуючих систем управління ризиками продемонстрував, що їх інтеграція в корпоративні мережі є необхідною умовою для ефективного протистояння сучасним загрозам і забезпечення стабільності роботи інформаційної інфраструктури.

2 ВИКОРИСТАННЯ ZABBIX ДЛЯ МОНІТОРИНГУ ТА УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Огляд системи моніторингу Zabbix

Zabbix — це відкрита платформа для моніторингу продуктивності та стану IT-інфраструктури. Вона дозволяє здійснювати централізований контроль за серверами, мережевим обладнанням, додатками, базами даних та іншими елементами інфраструктури в реальному часі. Система широко використовується у корпоративних мережах завдяки своїй гнучкості, масштабованості та безкоштовному базовому функціоналу.

Zabbix займає провідні позиції серед інструментів моніторингу завдяки своїй гнучкості, доступності та функціоналу. Система здатна інтегруватися з різними типами інфраструктури, включаючи фізичні сервери, віртуальні машини, мережеве обладнання та хмарні сервіси. Це робить її універсальним рішенням для компаній будь-якого масштабу, які прагнуть забезпечити стабільну роботу своїх IT-ресурсів.

Однією з найважливіших переваг Zabbix є його здатність працювати у реальному часі, що дозволяє адміністраторам оперативно реагувати на інциденти. Наприклад, система може відстежувати перевантаження мережі, збої в роботі серверів або проблеми з підключенням до баз даних. У разі виявлення події, яка може вплинути на стабільність мережі, Zabbix автоматично генерує попередження або тригер, які можуть бути налаштовані для відправлення відповідальним особам через SMS, електронну пошту або месенджери.

У корпоративних мережах Zabbix застосовується для забезпечення постійного моніторингу критичних систем. Завдяки відкритому коду, компанії можуть адаптувати систему до своїх унікальних потреб. Наприклад,

Zabbix дозволяє створювати власні шаблони для моніторингу специфічних пристроїв або застосунків, які не підтримуються стандартними налаштуваннями.

Zabbix активно використовується для забезпечення високої доступності сервісів. Здатність аналізувати історичні дані дає змогу організаціям визначати тенденції у використанні ресурсів, що допомагає прогнозувати потенційні збої. Наприклад, якщо сервер стабільно наближається до 90% використання процесора, система може створити попередження для адміністраторів із рекомендацією масштабувати ресурси або оптимізувати навантаження.

Розгортання системи моніторингу Zabbix розпочинається з підготовки серверного середовища. Одним із найзручніших варіантів для швидкого запуску є використання готового віртуального образу Zabbix Appliance. Цей підхід значно спрощує налаштування, оскільки користувачу не потрібно вручну встановлювати операційну систему, сервер баз даних, вебінтерфейс або інші компоненти, необхідні для повноцінної роботи Zabbix. Віртуальний образ уже містить усі ці компоненти, попередньо налаштовані для зручності адміністрування.

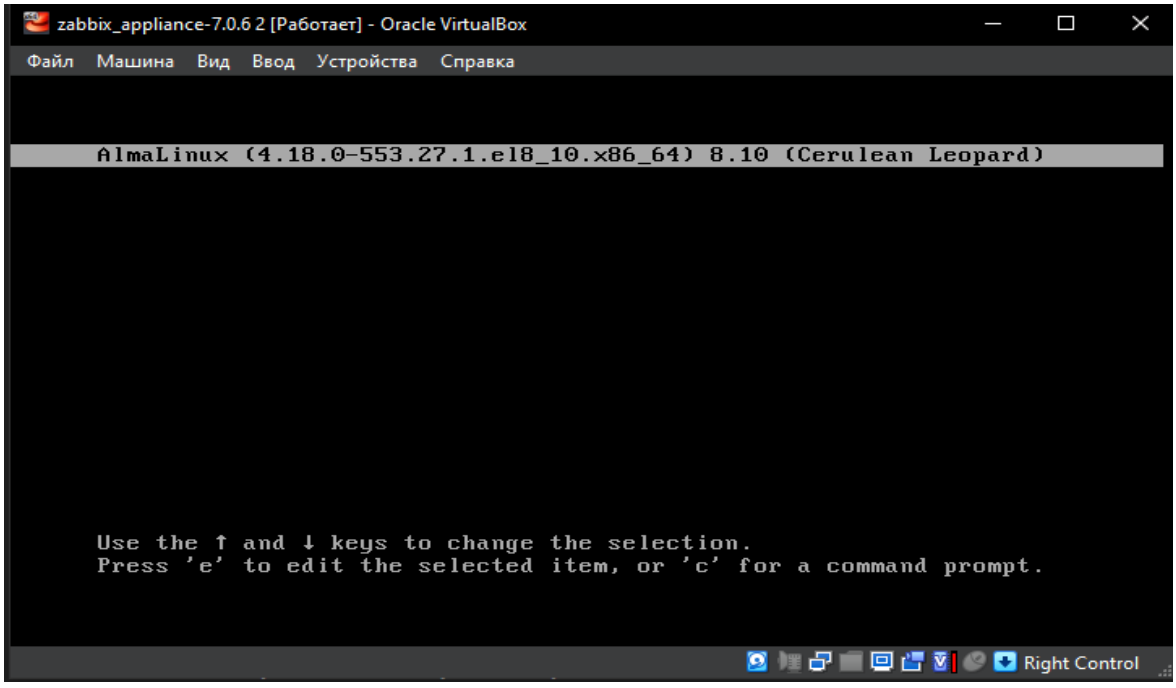


Рис.2.1 - Процес завантаження Zabbix Appliance у VirtualBox

Процес налаштування Zabbix Appliance передбачає використання спеціально підготовленого віртуального образу, який містить усі необхідні компоненти для запуску системи моніторингу. Використання готового рішення Zabbix Appliance значно скорочує час на підготовку серверної частини, оскільки всі необхідні залежності, включаючи базу даних і вебінтерфейс, інтегровані в один пакет.

Сервер працює на базі операційної системи AlmaLinux, яка забезпечує стабільність і безпеку роботи. Завдяки простоті процесу розгортання, навіть початківці в адмініструванні можуть швидко налаштувати систему для початку моніторингу.

Zabbix Appliance у віртуальній машині AlmaLinux адміністратор отримує доступ до базових налаштувань системи через консольний інтерфейс. У цьому інтерфейсі користувачу надаються основні облікові дані для доступу до вебінтерфейсу Zabbix, а також інформація про документацію, що може бути використана для подальшої роботи.

Ключовими елементами на цьому етапі є:

- Облікові дані для вебінтерфейсу (логін: Admin, пароль: zabbix), які необхідні для першого входу в систему.
- Вхід під обліковим записом "root" у локальну консоль для виконання адміністративних команд.
- Інформація про офіційну документацію Zabbix, що надає додаткову підтримку під час налаштування та використання системи.

Даний етап забезпечує доступ до функціоналу Zabbix та базові інструменти для подальшої інтеграції.

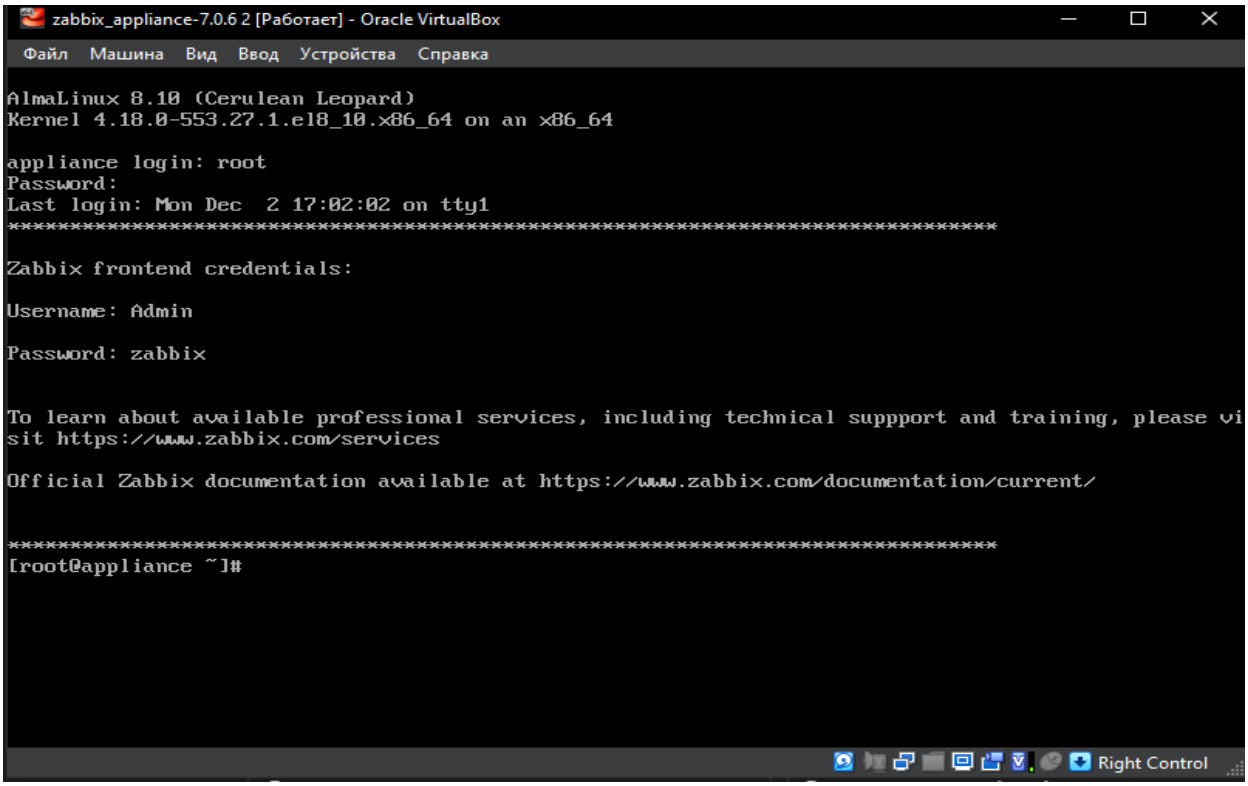


Рис.2.2 - Початковий інтерфейс Zabbix Appliance після входу в систему

Консольний доступ дозволяє виконувати первинні налаштування Zabbix, перевіряти стан операційної системи та виконувати команди для інтеграції сервера в корпоративну мережу. Надані облікові дані для вебінтерфейсу дозволяють розпочати роботу з графічною панеллю Zabbix, яка надає зручний спосіб моніторингу та управління мережею.

Демонстрація зручності використання готового рішення, такого як Zabbix Appliance, оскільки всі необхідні налаштування вже виконані, а адміністратору залишається лише здійснити базову інтеграцію сервера. Документація, доступна за вказаним посиланням, допомагає новим користувачам швидко освоїти основи роботи із системою та розширити її можливості.

Подальша перевірка налаштувань мережі для забезпечення стабільного з'єднання сервера з іншими компонентами корпоративної мережі. Для цього використовуються консольні команди, які дозволяють отримати детальну інформацію про стан мережевих інтерфейсів. У даному випадку команда `ip a` використовується для перевірки IP-адреси, прив'язаної до мережевого

інтерфейсу сервера, а також інших важливих параметрів, таких як статус інтерфейсу та його MAC-адреса.

Це є критичним етапом під час налаштування Zabbix Appliance, оскільки коректна робота мережі є основою для інтеграції сервера в корпоративну інфраструктуру та подальшого збору даних із мережевих пристроїв і хостів.

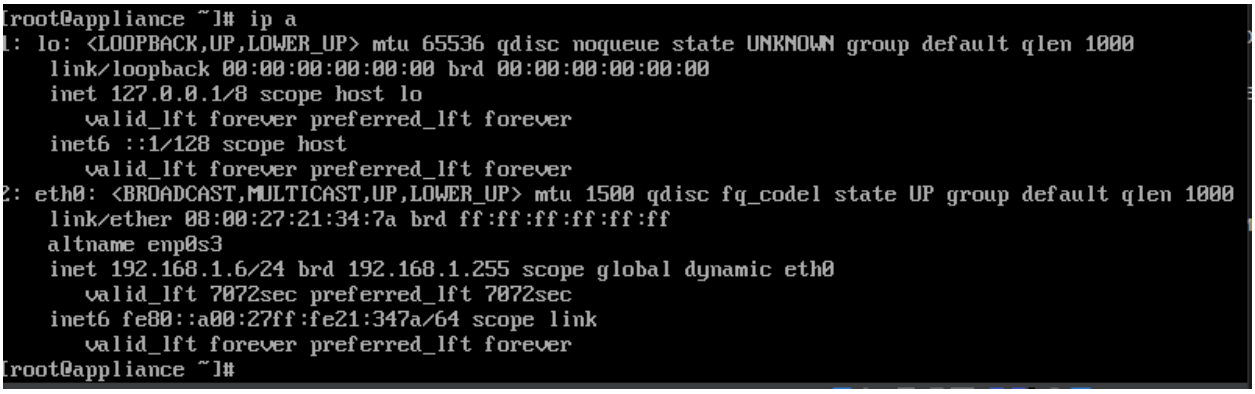


Рис. 2.3- Виведення мережевих налаштувань Zabbix Appliance командою *ip a*

На рисунку представлено мережеві параметри сервера Zabbix Appliance. Інтерфейс eth0 має IP-адресу 192.168.1.6, яка належить до локальної мережі, що дозволяє серверу взаємодіяти з іншими пристроями. Стан інтерфейсу позначено як "UP", що свідчить про активний стан мережевого з'єднання.

Відповідь системи є важливою для налаштування доступу до вебінтерфейсу Zabbix, а також для подальшого підключення агентів, налаштування моніторингу та збору даних. Перевірка мережевих налаштувань дозволяє уникнути можливих проблем із доступом до системи та забезпечити її стабільну роботу в корпоративному середовищі. У разі виявлення помилок, адміністратор може оперативно внести необхідні зміни, використовуючи інші інструменти налаштування мережі.

Для забезпечення стабільної роботи Zabbix-сервера важливо регулярно перевіряти його статус та стан роботи окремих компонентів. Команда *systemctl status zabbix-server* є базовим інструментом для діагностики роботи сервісу. Виконання цієї команди дозволяє отримати детальну інформацію про активність сервера, його стан (наприклад, чи знаходиться він у статусі

"*running*"), а також ідентифікувати можливі помилки, якщо сервер не функціонує належним чином.

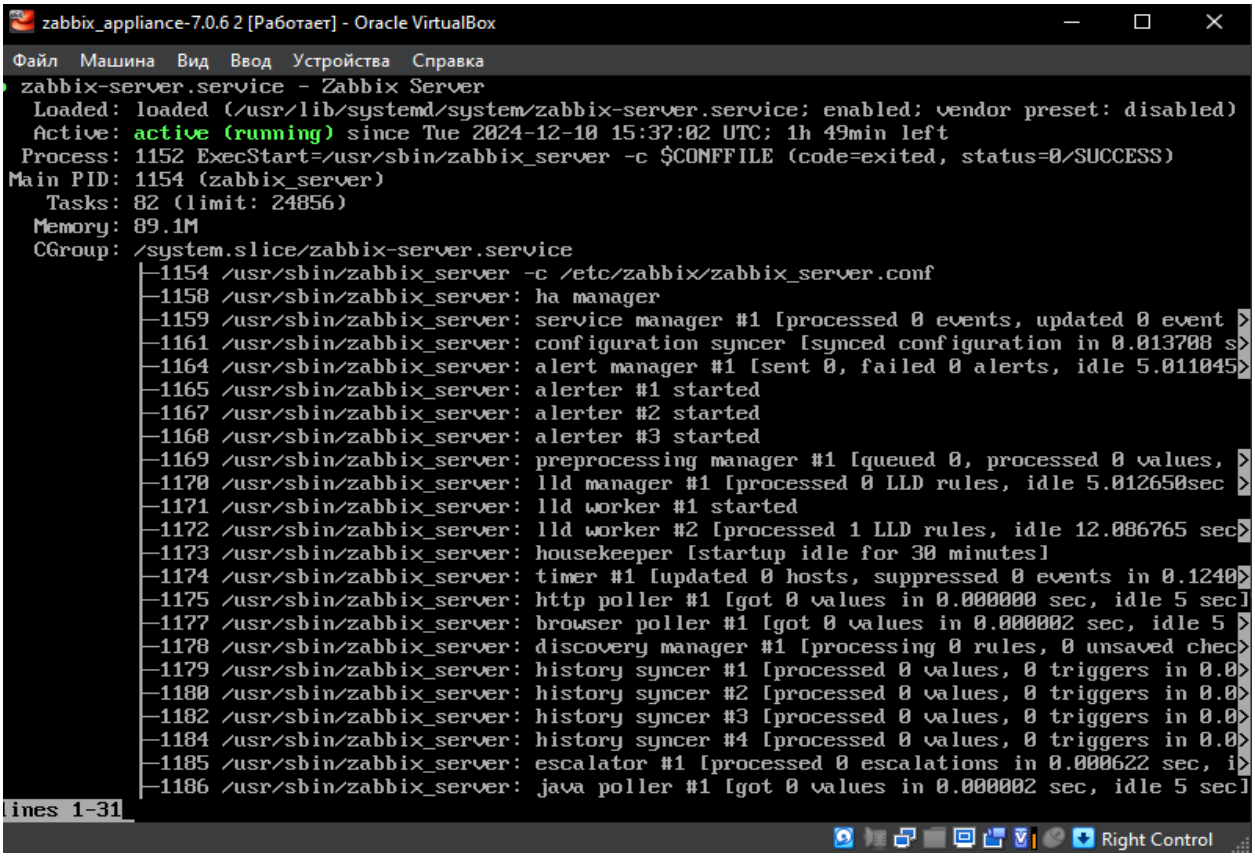


Рис.2.4 - Перевірка статусу Zabbix-сервера за допомогою команди `systemctl status zabbix-server`

Сервер знаходиться у статусі "active (running)", що свідчить про його коректну роботу. У списку завдань зазначено різні компоненти Zabbix, зокрема:

- **Alert manager** – модуль, що відповідає за управління сповіщеннями;
- **Housekeeper** – процес очищення історичних даних для оптимізації роботи сервера;
- **History syncer** – модуль синхронізації даних з історії;
- **Poller** – обробляє запити від хостів та агентів.

Також представлено використання ресурсів сервера, наприклад, споживана пам’ять (89.1 МБ) та кількість запущених завдань (82). Ці параметри дозволяють оцінити навантаження на сервер і вчасно виявити потенційні проблеми.

У контексті управління ризиками інформаційної безпеки, подібна діагностика допомагає забезпечити безперервність роботи системи моніторингу, вчасно реагувати на помилки в роботі сервера та підтримувати його налаштування у відповідності до потреб корпоративної мережі.

Після запуску та перевірки працездатності сервера Zabbix наступним кроком є доступ до графічного інтерфейсу системи. Цей інтерфейс надає користувачам широкий функціонал для моніторингу, аналізу та управління ресурсами корпоративної мережі. Головна панель (Global View) є центральним елементом управління, що дозволяє отримати загальну інформацію про стан системи, наявність активних проблем, завантаження ресурсів та географічне розташування моніторованих хостів.

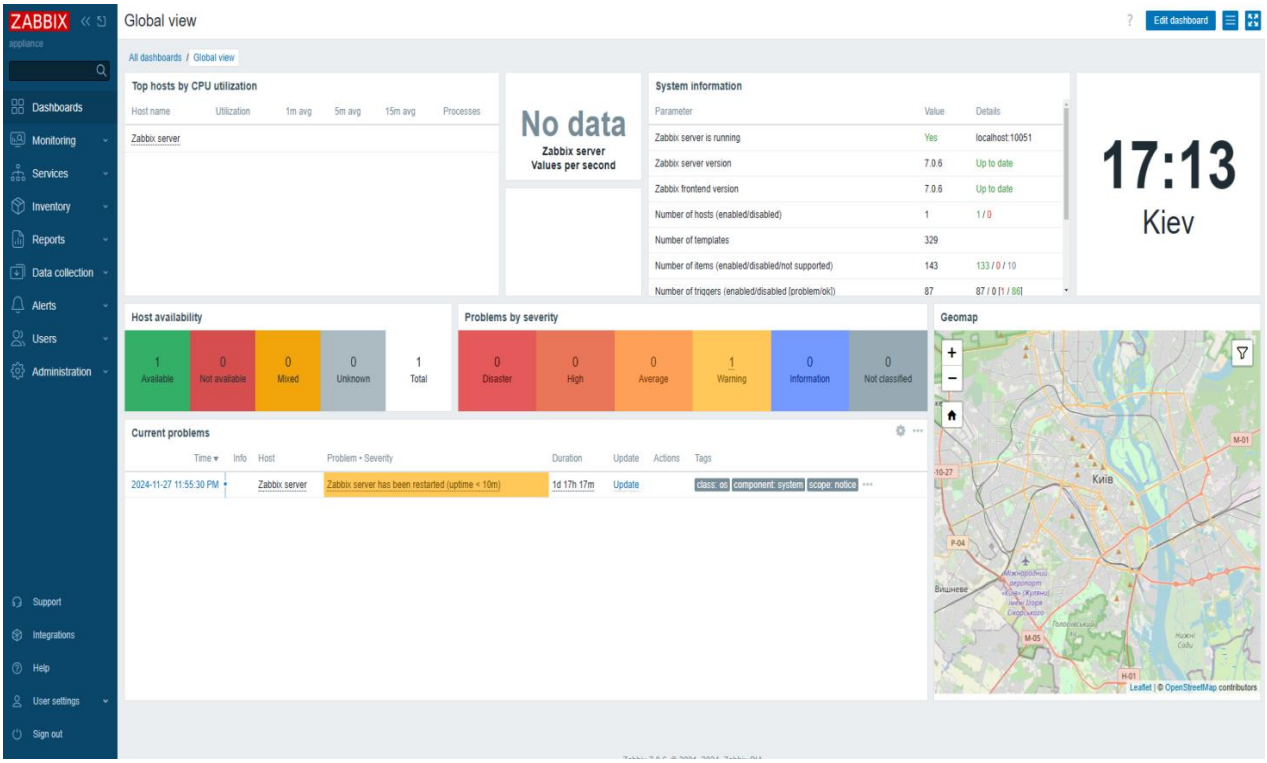


Рис.2.5 - Головна панель інтерфейсу Zabbix (Global View)

1. **Top hosts by CPU utilization** – інформація про хости з найвищим використанням процесорних ресурсів.

2. **System information** – статус роботи сервера, версія Zabbix, кількість підключених хостів, шаблонів, тригерів тощо.

3. **Host availability** – доступність хостів в системі, включаючи активні та недоступні.

4. **Problems by severity** – категоризація проблем за рівнем їх серйозності (від Warning до Disaster).

5. **Current problems** – деталі про активні проблеми в системі, їх тривалість та статус.

6. **Geomap** – карта з розташуванням хостів (залежно від налаштувань).

Ця панель є основним джерелом оперативної інформації для системного адміністратора. У контексті управління ризиками інформаційної безпеки використання головної панелі Zabbix дозволяє швидко виявляти потенційні загрози, оцінювати їхній рівень серйозності та забезпечувати відповідне реагування. Вона також дозволяє централізовано спостерігати за станом мережі, що є важливим компонентом ефективного управління ризиками.

Взаємодія компонентів: Zabbix Server у центрі, з’єднаний із базою даних, вебінтерфейсом, агентами та проксі-серверами, пристрої, які передають дані через агентів до серверу. (див. таб. 2.1).

Zabbix забезпечує широкі можливості для моніторингу, які включають:

- Збір даних: Zabbix збирає метрики з тисяч джерел, включаючи сервери, мережеве обладнання, хмарні сервіси та інші пристрої.
- Аналіз даних у реальному часі: Система виявляє аномалії та генерує тригери для швидкого реагування.
- Автоматичне сповіщення: Інтеграція зі службами сповіщення (SMS, e-mail, месенджери) дозволяє миттєво повідомляти відповідальних осіб про проблеми.
- Графіки та звіти: Інтерфейс Zabbix дозволяє створювати графічні звіти для аналізу історичних даних.
- Інтеграція з іншими системами: Система підтримує API для взаємодії з іншими рішеннями, такими як SIEM або інструменти управління ризиками.

Архітектура системи Zabbix побудована на основі клієнт-серверної архітектури та складається з наступних компонентів:

1. Zabbix Server: Центральний компонент, що здійснює збір, аналіз та зберігання даних.

2. Агенти Zabbix: Легковагові програми, які встановлюються на моніторовані пристрої для збору даних.

3. База даних: Використовується для зберігання всіх даних, які збирає система, включаючи конфігурації, метрики та журнали.

4. Вебінтерфейс: Інструмент для адміністрування та візуалізації даних у режимі реального часу.

5. Проксі-сервери: Використовуються для масштабованості та зменшення навантаження на центральний сервер.

Zabbix пропонує численні переваги, що робить його популярним вибором для моніторингу корпоративних мереж, особливо в Україні:

1. Відкритий код: Zabbix є безкоштовним, що зменшує витрати на впровадження.

2. Масштабованість: Система може моніторити як малі мережі, так і великі корпоративні інфраструктури.

3. Гнучкість у налаштуванні: Користувачі можуть налаштовувати тригери, звіти та інші функції відповідно до потреб організації.

4. Автоматизація: Можливість автоматичного виконання дій на основі попередньо визначених правил.

5. Підтримка різноманітних платформ: Система сумісна з Linux, Windows, Unix та іншими операційними системами.

Попри свої переваги, Zabbix має певні обмеження:

1. Складність налаштування: Впровадження Zabbix може вимагати значних технічних знань.

2. Обмежений функціонал управління ризиками: Zabbix більше орієнтований на моніторинг, ніж на повноцінне управління ризиками інформаційної безпеки.

3. Висока залежність від бази даних: Перевантаження бази може знижувати продуктивність системи.

4. Відсутність вбудованих засобів аналітики ризиків: Для глибокого аналізу потрібно інтегрувати Zabbix з іншими системами.

У корпоративних мережах Zabbix виконує роль інструменту для моніторингу та раннього виявлення загроз. Наприклад:

- Моніторинг стану серверів дозволяє ідентифікувати апаратні збої до їхнього впливу на бізнес-процеси.
- Відстеження мережевого трафіку дає змогу виявити підозрілу активність, яка може свідчити про потенційну атаку.
- Інтеграція з SIEM-системами дозволяє використовувати Zabbix як джерело даних для аналізу кіберзагроз.

Таблиця 2.1 – Основні характеристики Zabbix

Характеристика	**Опис**
Тип ліцензії	Відкрите програмне забезпечення (безкоштовне)
Основні функції	Моніторинг мережі, серверів, додатків
Підтримка платформ	Linux, Windows, Unix
Масштабованість	Підтримка тисяч вузлів
Інтеграція	API для підключення до інших систем
Основні недоліки	Складність налаштування, обмежений функціонал для управління ризиками

Додаткові можливості Zabbix

1. **Налаштування SLA -** Zabbix може використовуватися для моніторингу рівня обслуговування (SLA) шляхом створення метрик, які відображають доступність і продуктивність критичних сервісів.

2. **Моніторинг IoT-пристроїв -** завдяки підтримці різних протоколів (SNMP, Modbus), Zabbix може бути використаний для моніторингу IoT-пристроїв, таких як камери спостереження, сенсори або промислові контролери.

3. **Розширення функціоналу через модулі -** Zabbix підтримує додавання сторонніх модулів, що дозволяє інтегрувати його з будь-якими нестандартними пристроями чи програмами.

Zabbix є потужним інструментом для моніторингу корпоративних мереж, який може стати основою для виявлення потенційних загроз та підтримки управління ризиками. Проте його функціонал орієнтований переважно на технічний моніторинг, і для повноцінного управління ризиками доцільно інтегрувати Zabbix із іншими платформами.

2.2 Архітектура та принципи роботи Zabbix

Система моніторингу **Zabbix** побудована на модульній архітектурі, яка дозволяє масштабувати її для мереж будь-якого розміру та складності. Основною метою Zabbix є забезпечення цілісного моніторингу інформаційної інфраструктури організації, своєчасного виявлення проблем та швидкого реагування на них. Архітектура Zabbix складається з декількох компонентів, які забезпечують безперервний збір, обробку, зберігання та аналіз даних.

Кожен компонент виконує свою специфічну функцію, яка інтегрується в загальний процес моніторингу, забезпечуючи гнучкість і ефективність системи. Розуміння ролі та взаємодії цих компонентів є ключовим для оптимального налаштування та використання Zabbix у корпоративному середовищі. У цьому розділі детально розглядається структура системи, а також принципи її роботи.

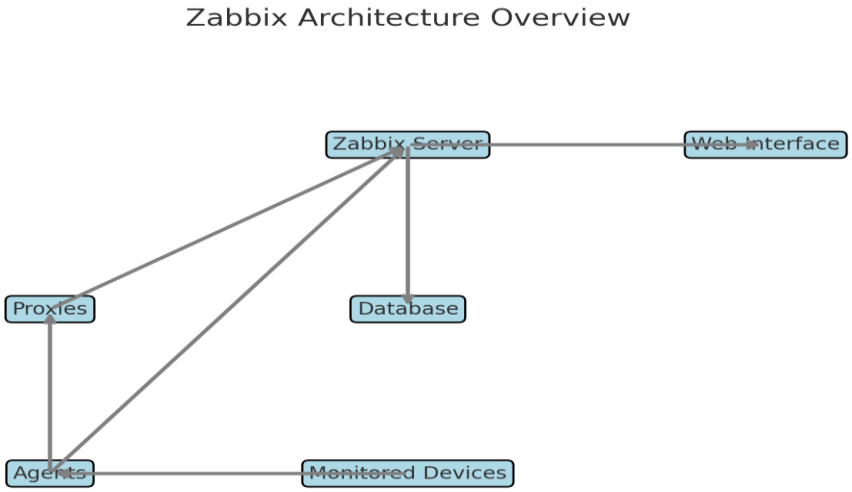


Рис.2.6 - Архітектуру системи **Zabbix**

1) **Моніторовані пристрої (Monitored Devices).**

Моніторовані пристрої є джерелом даних для системи Zabbix. Це можуть бути сервери, мережеве обладнання, бази даних або програми. Вони генерують ключові метрики, такі як завантаження процесора, використання пам'яті, обсяг мережевого трафіку та інші параметри. Дані з цих пристроїв передаються до агентів, які виконують їх первинну обробку. Моніторовані пристрої є основою для аналізу стану всієї мережі.

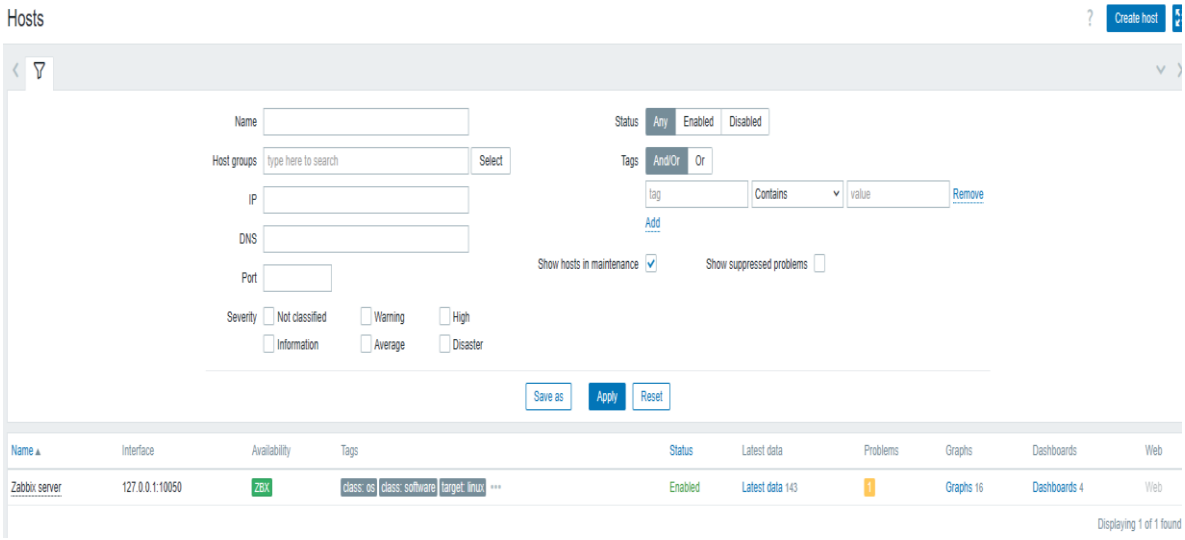


Рис. 2.7 - Monitoring > Hosts відображає поточний стан і доступність

2) **Zabbix Agent.**

Zabbix Agent — це легкий програмний компонент, що встановлюється на моніторовані пристрої. Він збирає локальні метрики (стан процесора, пам’яті, дисків тощо) і передає їх на Zabbix Server або Proxy. Агенти можуть працювати в активному або пасивному режимі, залежно від налаштувань. Це дозволяє збирати як базову інформацію, так і специфічні параметри для кожного пристрою.

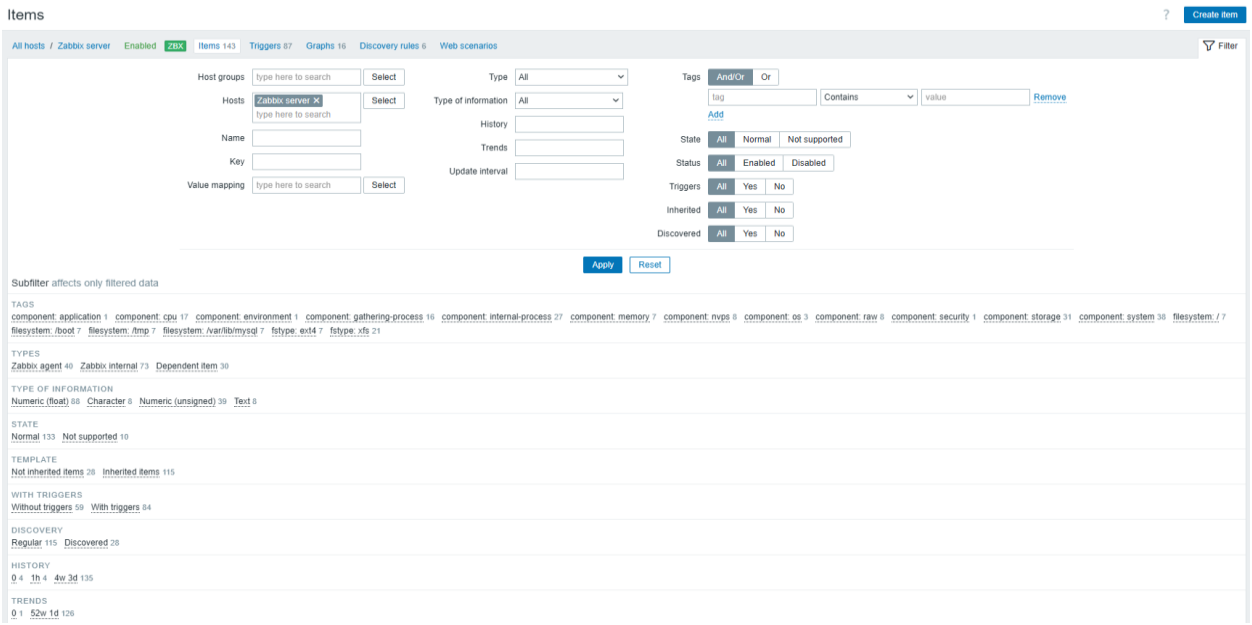


Рис.2.8 - Список параметрів для моніторингу на хості Zabbix server

3) Zabbix Proxy.

Proxy використовується для масштабування системи у великих розподілених мережах. Він приймає дані від агентів у віддалених мережах і передає їх на центральний сервер. Це допомагає зменшити навантаження на Zabbix Server, забезпечуючи стабільність навіть за умови моніторингу тисяч пристроїв. Proxy також дозволяє продовжувати збір даних у разі втрати зв’язку з центральним сервером.

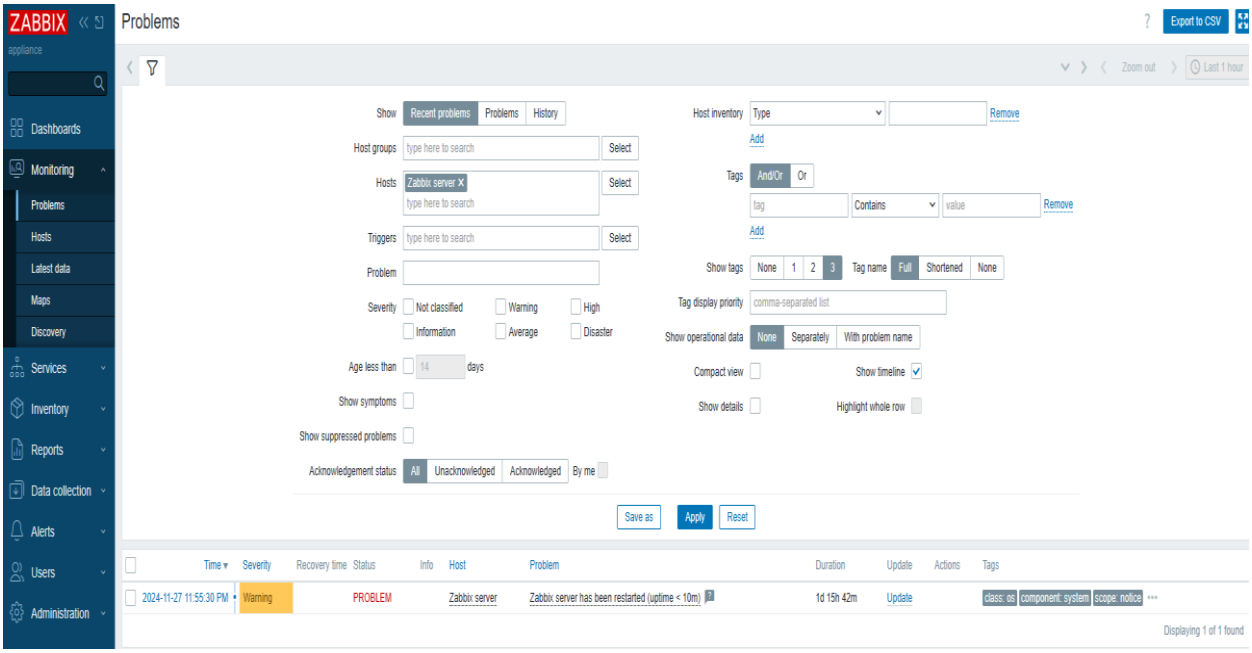


Рис.2.9 - Список активних проблем із деталями про їхній стан, тривалість і рівень серйозності

4) Zabbix Server.

Центральний компонент Zabbix, який обробляє отримані дані, порівнює їх із заданими тригерами та формує сповіщення. Сервер також відповідає за запис даних у базу, обробку сповіщень та виконання завдань, таких як перезавантаження пристрою. Він є ядром системи, що забезпечує взаємодію між усіма компонентами.

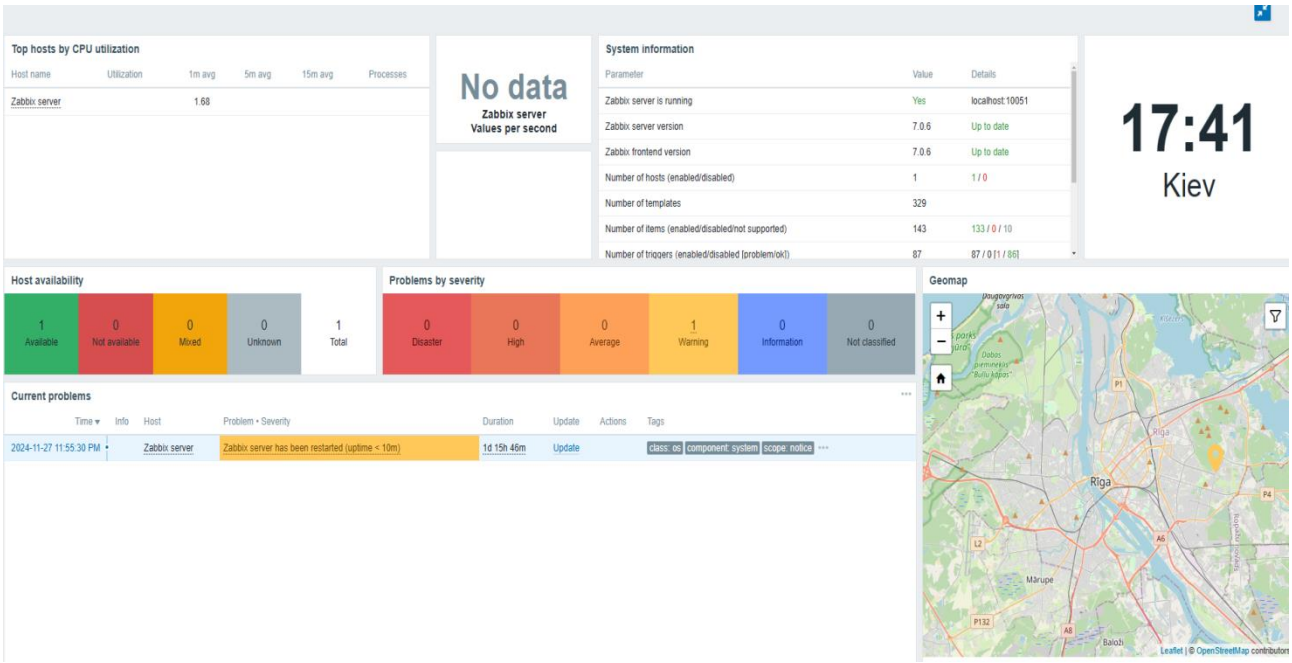


Рис.2.10 - Загальний огляд стану системи

5) Параметри конфігурації системи Zabbix.

Other Configuration Parameters у вкладці **Administration > General**, який дозволяє налаштувати важливі системні параметри Zabbix для забезпечення стабільної роботи моніторингової інфраструктури. Цей розділ містить декілька категорій налаштувань:

Ключові параметри:

1. **Frontend URL:**
   - Використовується для налаштування URL інтерфейсу Zabbix. Це важливо для інтеграції з іншими системами або для доступу користувачів через браузер.
2. **Group for Discovered Hosts:**
   - Група, до якої автоматично додаються хости, виявлені через правила виявлення.
3. **Default Host Inventory Mode:**
   - Режим обліку хостів, який може бути:
     - **Disabled:** Інвентаризація хостів не ведеться.
     - **Manual:** Вимагає ручного введення даних.
4. **Authorization:**
   - Параметри безпеки для авторизації:
     - Максимальна кількість спроб входу (**Login attempts**).
     - Інтервал блокування облікового запису після невдалих спроб (**Login blocking interval**).
5. **Storage of Secrets:**
   - Підтримка сховищ секретів, таких як **HashiCorp Vault** або **CyberArk Vault**, для безпечного зберігання даних.
6. **Security:**
   - Налаштування URI-схем, які система вважає допустимими для роботи.
   - Політики безпеки для HTTP-заголовків та iframe sandboxing.

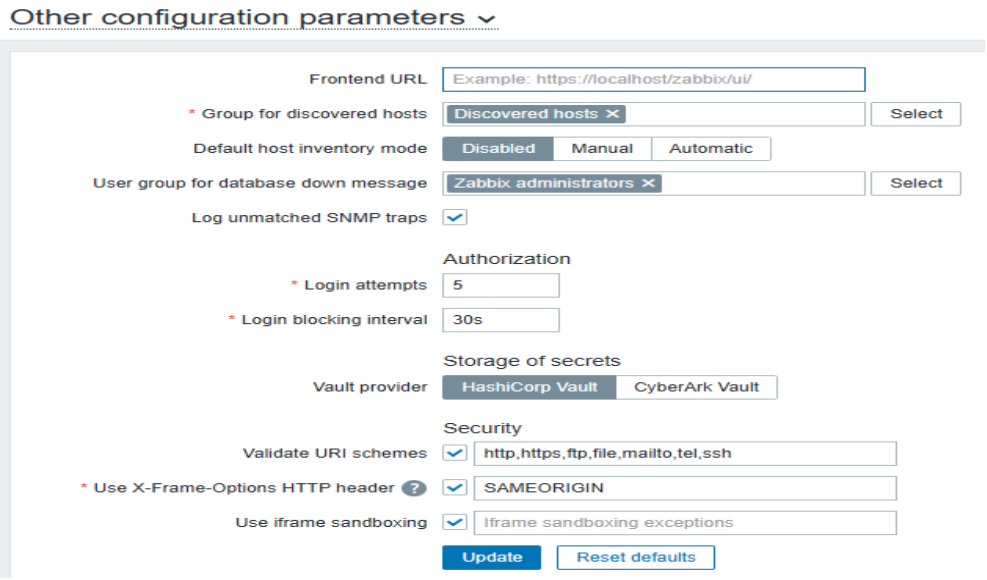


Рис.2.11 – Системні параметри конфігурації

2.3 Інтеграція Zabbix у корпоративну мережу для моніторингу ризиків

Інтеграція Zabbix у корпоративну мережу є важливим етапом для побудови надійної системи моніторингу ризиків. Zabbix, як система з відкритим вихідним кодом, пропонує інструменти для виявлення, аналізу та реагування на потенційні загрози інформаційній безпеці. Навіть без доступу до розширених функцій конфігурації, використання стандартного сервера Zabbix дозволяє провести базовий моніторинг метрик і продемонструвати принципи роботи системи.

Після інтеграції Zabbix у корпоративну мережу, необхідним кроком є додавання хостів до системи моніторингу. На скріншоті представлено налаштування хоста **Zabbix server**, який було підключено до системи. Це демонструє, як інформація про хост відображається у вкладці **Host Inventory**, що включає основні параметри, такі як IP-адреса, DNS-ім’я та порт, через який здійснюється моніторинг.

У цьому випадку, хост **Zabbix server** підключений за IP-адресою **127.0.0.1**, що вказує на моніторинг самого сервера Zabbix. Зазначено, що моніторинг здійснюється через порт **10050**. Додаткова інформація про хост включає дані про операційну систему, зокрема її версію та конфігурацію ядра. Це дає змогу адміністраторам швидко отримувати загальні відомості про стан хоста та впевнитися, що він підключений і готовий до моніторингу.

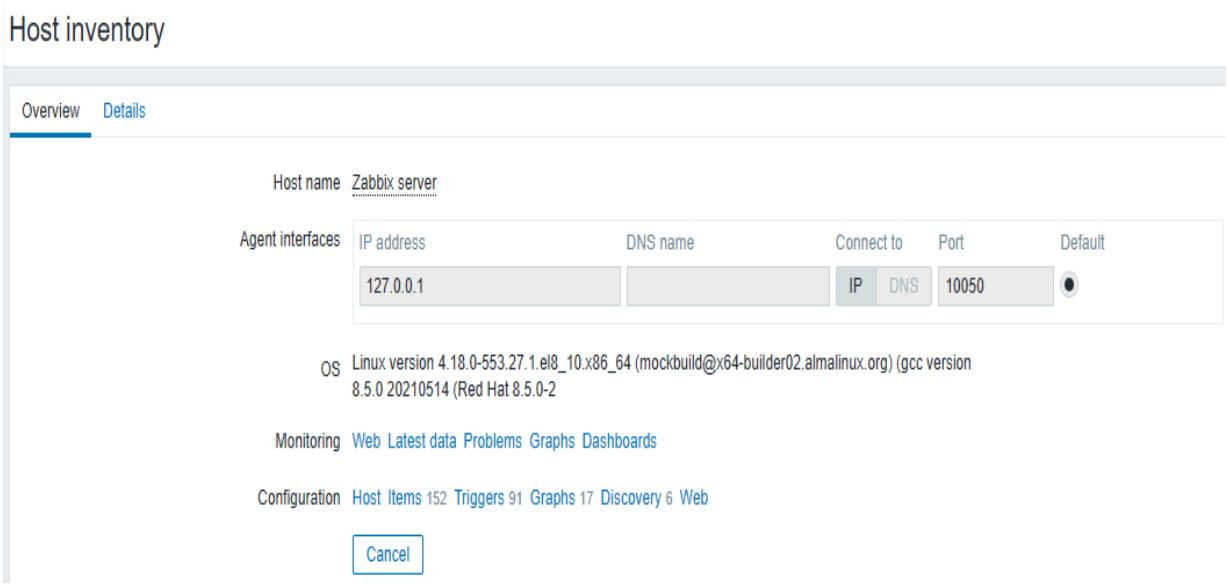


Рис.2.12 – Налаштування параметрів до серверної системи моніторингу хоста Zabbix server

Корпоративні мережі зазвичай складаються з безлічі елементів: серверів, мережевого обладнання, програмного забезпечення та додатків. Усі ці компоненти повинні моніторитися для запобігання ризикам, які можуть призвести до збоїв у роботі або втрати даних. Zabbix дозволяє створювати централізовану систему, яка збирає метрики зі всіх ключових вузлів мережі та аналізує їх у реальному часі.

Принципи інтеграції Zabbix.

Zabbix інтегрується у корпоративну мережу через агенти, шаблони та налаштування тригерів. Основним об'єктом моніторингу в стандартній конфігурації є сервер Zabbix, який демонструє базову архітектуру системи. Сервер збирає метрики, зберігає їх у базі даних, а результати візуалізуються у вебінтерфейсі.

На базовому рівні Zabbix може використовувати локальний хост (127.0.0.1) для моніторингу власних ресурсів, таких як:

- Завантаження CPU.
- Використання оперативної пам’яті.
- Обсяг вільного місця на диску.

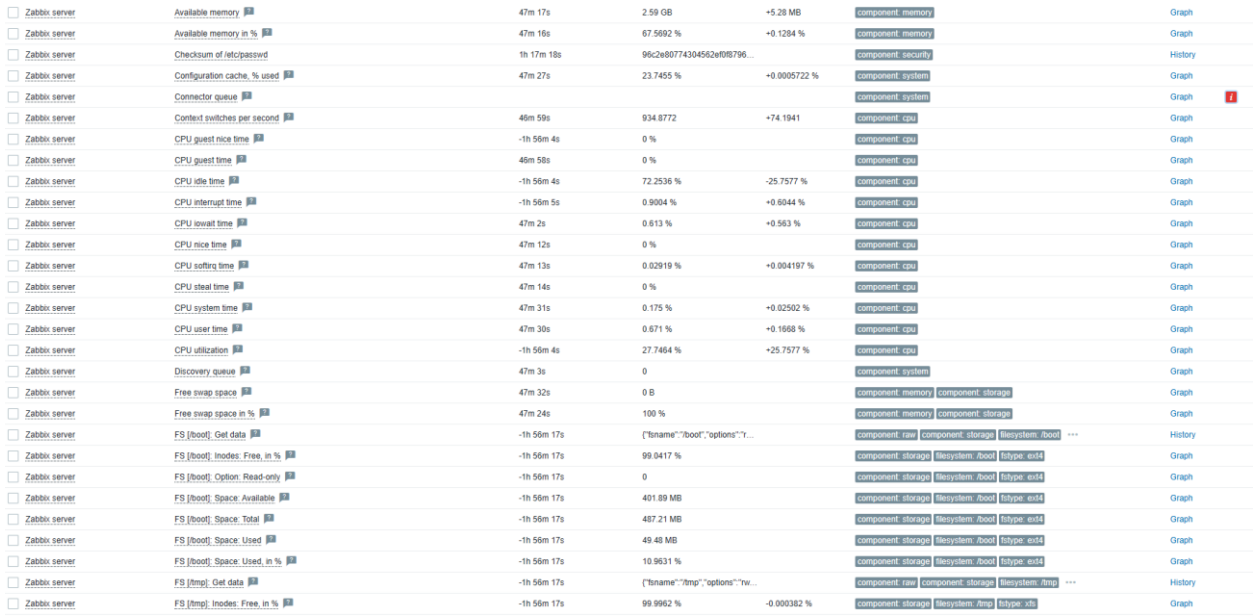


Рис.2.13 - Дані моніторингу сервера Zabbix

Ці метрики дозволяють оцінити стан самого сервера та потенційні ризики, що виникають у разі перевищення порогових значень. Наприклад, якщо CPU завантажено понад 90%, це може свідчити про критичну ситуацію, яка потребує негайного втручання.

Моніторинг ризиків та ефективне управління інформаційною безпекою в корпоративній мережі неможливі без системи автоматичного виявлення проблем. Однією з ключових функцій Zabbix є використання тригерів для генерації сповіщень про потенційні ризики. Ці тригери базуються на порогових значеннях, які визначаються для кожної метрики. У разі перевищення заданих параметрів система автоматично створює проблему, яка з’являється в розділі Monitoring > Problems.

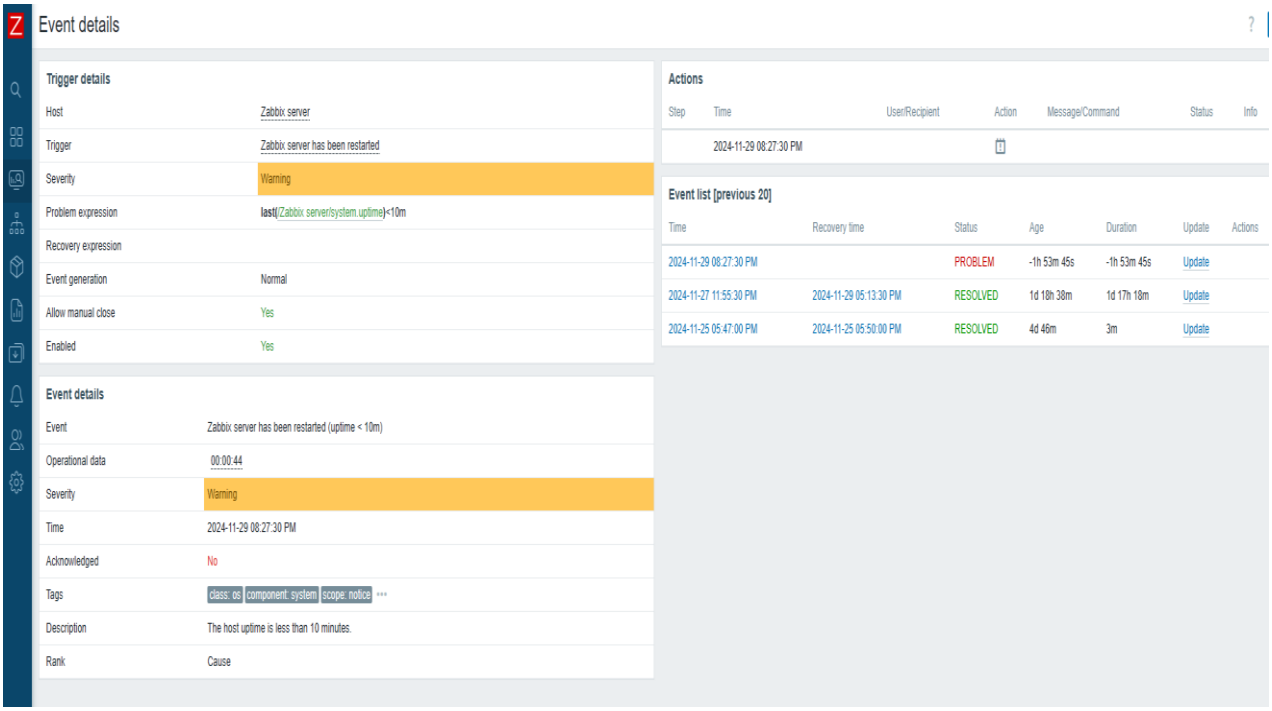


Рис.2.14 - Функціонал Monitoring > Problems

Цей розділ дозволяє адміністраторам виявляти, які проблеми виникли у системі, а також швидко реагувати на них. Тут надається інформація про:

- Назву хоста: Пристрій або сервер, на якому виникла проблема.
- Тип проблеми: Наприклад, перевантаження CPU, недоступність хоста або недостатній обсяг пам’яті.
- Серйозність: Визначається рівнем ризику, від "Інформаційного" до "Критичного" (Warning, Average, High, Disaster).
- Тривалість: Скільки часу проблема залишається невирішеною.
- Дії: Можливість переглянути додаткову інформацію, вжити заходів або позначити проблему як вирішену.

У разі інтеграції Zabbix у корпоративну мережу саме цей розділ стає центральним пунктом для оперативного управління ризиками. Адміністратори можуть використовувати цю інформацію для визначення пріоритетів у реагуванні на інциденти.

Моніторинг файлових систем і ресурсів: аналіз проблем.

Ефективна інтеграція Zabbix у корпоративну мережу базується на здатності системи відстежувати критичні показники роботи серверів і

додатків. Одним із найважливіших аспектів моніторингу є контроль за використанням файлових систем. У разі виявлення проблем із недостатнім обсягом вільного місця або перевищення допустимих показників завантаження, система Zabbix автоматично генерує сповіщення. Це дозволяє адміністраторам реагувати на потенційні ризики до того, як вони призведуть до збоїв.

На прикладі наведеної візуалізації показано розподіл використання простору у файлових системах сервера. Кожна файловая система представлена у вигляді кругової діаграми, що наочно демонструє:

1. Загальний обсяг дискового простору.
2. Використаний простір.
3. Доступний для використання простір.

У системі також відображаються графіки використання простору в часі, що дозволяє аналізувати динаміку змін і прогнозувати майбутні потреби.

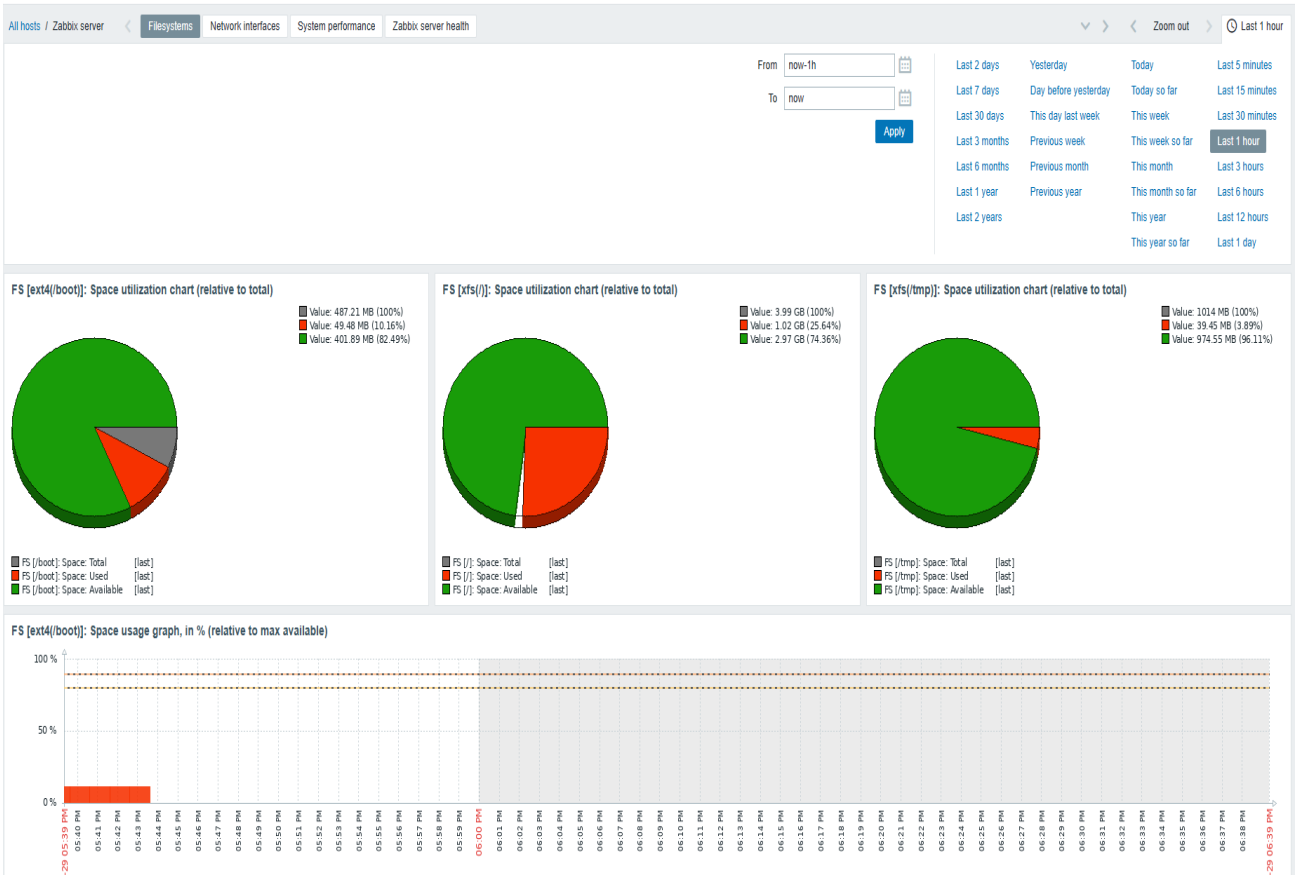


Рис.2.15 - Моніторинг використання файлових систем

Роль виявлення проблем і аналізу метрик.

Моніторинг файлових систем є ключовою функцією Zabbix, особливо в середовищах, де ефективне управління ресурсами є критичним для забезпечення безперервної роботи. Дані про використання простору на файлових системах дозволяють адміністраторам:

- Вчасно виявляти недостатній обсяг вільного місця.
- Вживати заходів для розширення простору або оптимізації даних.
- Планувати модернізацію інфраструктури на основі реальних потреб.

Кожна файловая система оцінюється окремо. Наприклад:

- Файлова система */boot* має 82.49% зайнятого простору, що вказує на стабільний стан.
- Інші файлові системи (/, / *tmp*) також знаходяться у допустимих межах, однак подальший аналіз може виявити потенційні ризики при наближенні до критичних значень.

Динаміка у часі: візуалізація графіків.

Нижній графік надає інформацію про використання простору файлових систем у часі. Завдяки цьому можна оцінити:

1. Рівномірність завантаження.
2. Стрибки використання, які можуть свідчити про аномалії або зростання навантаження.

Якщо використання простору різко збільшується, це може бути викликано некоректною роботою програмного забезпечення або збереженням великих обсягів даних. У такому разі адміністратор отримує змогу не лише виявити проблему, але й запобігти її повторенню шляхом оптимізації процесів.

На основі цих метрик адміністратор може:

- Налаштувати автоматичні сповіщення (тригери) про перевищення порогових значень.
- Створювати прогнозовані звіти про використання ресурсів для планування закупівлі нових серверів або оптимізації старих.
- Реагувати на проблеми у реальному часі, уникаючи потенційних збоїв.

Інтеграція Zabbix для моніторингу файлових систем забезпечує візуалізацію та аналіз критично важливих показників. На основі отриманих даних можна оптимізувати використання ресурсів і уникати збоїв у роботі серверів. Система дозволяє не лише контролювати поточний стан, але й прогнозувати майбутні потреби, роблячи управління мережею більш ефективним.

2.4 Аналіз подій і ризиків інформаційної безпеки на основі даних з Zabbix

Система моніторингу Zabbix забезпечує всебічний контроль за станом мережі, серверів та інформаційних систем. Вона дозволяє своєчасно виявляти події, які можуть загрожувати інформаційній безпеці, а також аналізувати ці події для розробки заходів захисту. Одним із ключових елементів роботи Zabbix є можливість детального аналізу подій і ризиків на основі зібраних даних, таких як метрики використання ресурсів, зміни конфігурацій та інциденти в мережі.

Zabbix працює за принципом моніторингу в реальному часі. Це означає, що всі зміни у стані обладнання чи програмного забезпечення одразу відображаються у вигляді подій, які реєструються в системі. Наприклад, перевантаження процесора, недостатній обсяг пам'яті або недоступність певного сервера будуть відображені як активні проблеми, які потребують уваги адміністратора. Завдяки інтегрованим алгоритмам і тригерам, система не лише фіксує ці події, але й класифікує їх за рівнем серйозності. Це дозволяє ефективно пріоритезувати заходи з реагування.

Дані, які зберігаються в системі Zabbix, стають основою для проведення детального аналізу. Наприклад, якщо система повідомляє про низький обсяг вільного місця на диску, адміністратор може використати графіки для оцінки динаміки змін і визначення, чи це одноразова проблема, чи наслідок

систематичного збільшення навантаження. У разі систематичних проблем можна зробити висновок про необхідність розширення дискового простору або оптимізації використання ресурсів.

Аналіз ризиків інформаційної безпеки.

На основі подій, що генеруються в Zabbix, можна аналізувати різні аспекти ризиків:

1. Технічні ризики:
   - Перевантаження серверів або обладнання (наприклад, перевищення порогів CPU або пам'яті).
   - Недостатній обсяг вільного місця на дисках.
   - Втрата доступу до хоста чи сервера.
2. Організаційні ризики:
   - Недостатня кількість резервних копій даних.
   - Невчасне оновлення програмного забезпечення, яке може призвести до вразливостей.
3. Інциденти, пов’язані з безпекою:
   - Невдалий доступ до системи.
   - Сплески активності, які можуть свідчити про потенційні атаки.

Завдяки зібраним даним можна оцінити, як ці інциденти впливають на інформаційну безпеку компанії.

Моніторинг дискового простору є важливою частиною забезпечення стабільності та безпеки інформаційних систем. Графічне представлення використання файлових систем дозволяє адміністраторам не лише оцінити поточний стан ресурсів, але й прогнозувати майбутні потреби. На скріншоті представлено аналіз використання дискового простору на сервері Zabbix.

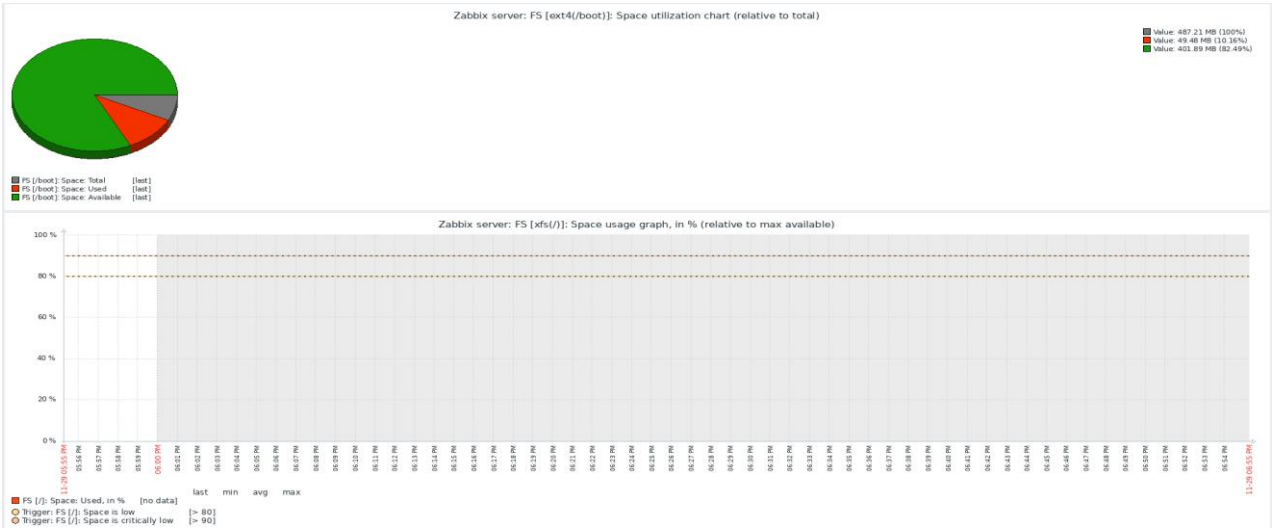


Рис.2.16 - Аналіз використання файлової системи /boot

Кругова діаграма демонструє загальний обсяг файлової системи /boot і її поточний стан:

- Зелений сектор відповідає вільному простору (82.49%),
- Червоний сектор показує використаний простір (10.16%),
- Сірий сектор — зарезервований або системний простір.

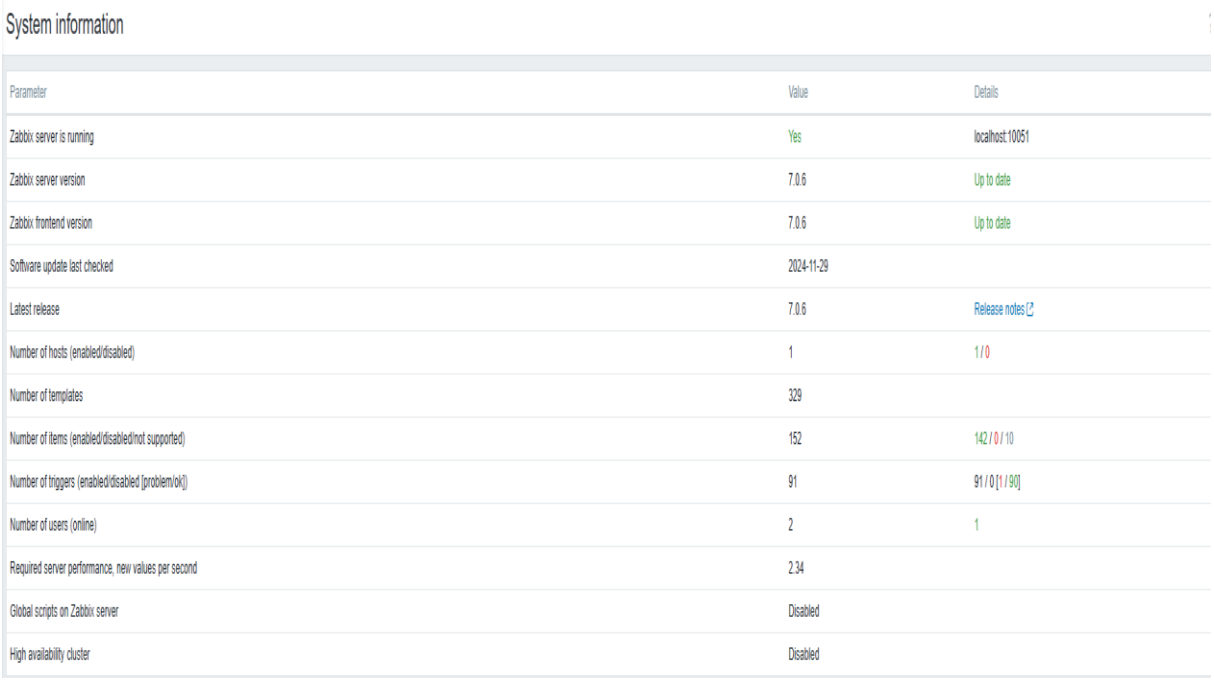
Лінійний графік у нижній частині показує динаміку змін використання дискового простору у часі. Червона горизонтальна лінія відображає критичний поріг у 100%, тоді як помаранчева лінія вказує на зону попередження (80%). На момент знімку графік показує стабільне завантаження, що не перевищує допустимих меж. Проте, постійний моніторинг дозволяє адміністраторам швидко реагувати у разі значного збільшення використання.

Дані з графіків можуть бути використані для прогнозування потенційних ризиків, таких як нестача вільного простору, що може вплинути на стабільну роботу серверів. У разі наближення до критичних значень адміністратори можуть запланувати розширення дискового простору або оптимізацію даних.

Автоматизація у Zabbix є не лише засобом моніторингу, але й важливим інструментом для генерації звітів. Розділ **Reports** дозволяє створювати підсумкові документи, які відображають стан ресурсів, основні проблеми та прогнозовані ризики. Завдяки цим звітам адміністратор отримує цілісне

уявлення про роботу інфраструктури та може краще планувати подальші дії. У звітах використовуються графіки, таблиці та інші інструменти візуалізації, що робить їх корисними для аналізу великих обсягів даних.

На скріншоті нижче представлено звіт, який демонструє стан використання ресурсів у файловій системі сервера.



System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Zabbix server version	7.0.6	Up to date
Zabbix frontend version	7.0.6	Up to date
Software update last checked	2024-11-29	
Latest release	7.0.6	Release notes
Number of hosts (enabled/disabled)	1	1 / 0
Number of templates	329	
Number of items (enabled/disabled/not supported)	152	142 / 0 / 10
Number of triggers (enabled/disabled [problem/ok])	91	91 / 0 [1 / 90]
Number of users (online)	2	1
Required server performance, new values per second	2.34	
Global scripts on Zabbix server	Disabled	
High availability cluster	Disabled	

Рис.2.17 - Автоматично створений звіт про стан ресурсів у Zabbix

Zabbix надає можливість детального аналізу проблем, які виникають у процесі роботи системи. На представленому скріншоті показано список проблем, зафіксованих сервером Zabbix, серед яких можна виділити критичні ризики для інформаційної безпеки та стабільності роботи системи.

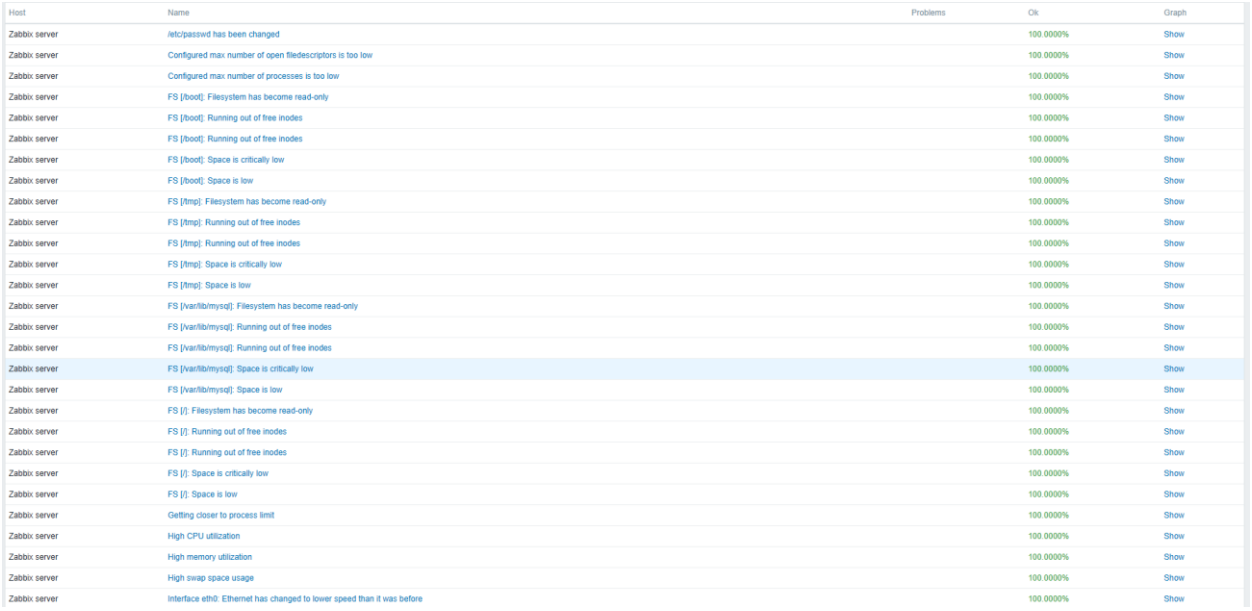
- Недостатня кількість вільних inode у файлових системах, що може призвести до неможливості створення нових файлів або запису даних.
- Критично низький обсяг вільного місця на файлових системах /boot і /var/lib/mysql, що загрожує зупинкою роботи програм.
- Високе завантаження процесора та пам’яті, яке може впливати на продуктивність серверів і викликати затримки у роботі.

Таблиця надає ключову інформацію для реагування:

- **Ім’я хоста:** Вказує, де саме виникла проблема (у цьому випадку сервер Zabbix).

- **Назва проблеми:** Конкретизує тип інциденту, наприклад, "High CPU utilization" або "Space is critically low."
- **Поточний стан:** Відображає, чи проблема ще актуальна, чи вже вирішена.

Представлені дані дозволяють адміністраторам швидко ідентифікувати основні загрози та планувати відповідні заходи. Наприклад, для усунення проблеми з критично низьким дисковим простором можна розширити файлову систему або видалити непотрібні дані. Високе завантаження CPU може бути вирішене оптимізацією програмного забезпечення або перенесенням частини обчислень на інший сервер.



Host	Name	Problems	Ok	Graph
Zabbix server	/etc/passwd has been changed		100.0000%	Show
Zabbix server	Configured max number of open filedescriptors is too low		100.0000%	Show
Zabbix server	Configured max number of processes is too low		100.0000%	Show
Zabbix server	FS [/boot]: Filesystem has become read-only		100.0000%	Show
Zabbix server	FS [/boot]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/boot]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/boot]: Space is critically low		100.0000%	Show
Zabbix server	FS [/boot]: Space is low		100.0000%	Show
Zabbix server	FS [/tmp]: Filesystem has become read-only		100.0000%	Show
Zabbix server	FS [/tmp]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/tmp]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/tmp]: Space is critically low		100.0000%	Show
Zabbix server	FS [/tmp]: Space is low		100.0000%	Show
Zabbix server	FS [/var/lib/mysql]: Filesystem has become read-only		100.0000%	Show
Zabbix server	FS [/var/lib/mysql]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/var/lib/mysql]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/var/lib/mysql]: Space is critically low		100.0000%	Show
Zabbix server	FS [/var/lib/mysql]: Space is low		100.0000%	Show
Zabbix server	FS [/]: Filesystem has become read-only		100.0000%	Show
Zabbix server	FS [/]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/]: Running out of free inodes		100.0000%	Show
Zabbix server	FS [/]: Space is critically low		100.0000%	Show
Zabbix server	FS [/]: Space is low		100.0000%	Show
Zabbix server	Getting closer to process limit		100.0000%	Show
Zabbix server	High CPU utilization		100.0000%	Show
Zabbix server	High memory utilization		100.0000%	Show
Zabbix server	High swap space usage		100.0000%	Show
Zabbix server	Interface eth0: Ethernet has changed to lower speed than it was before		100.0000%	Show

Рис.2.18 - Список активних проблем у системі Zabbix

Дана таблиця демонструє ідентифіковані інциденти, їхній характер і поточний стан.

Висновок до другого розділу

Зроблено висновок, що дослідження системи моніторингу Zabbix є важливим для розуміння сучасних підходів до управління ризиками інформаційної безпеки в корпоративних мережах. Виокремлено ключові аспекти, які сприяють ефективному моніторингу та прогнозуванню потенційних загроз.

Зазначено, що використання функцій системи Zabbix, таких як тригери, дашборди, графіки та автоматичне створення звітів, має вирішальне значення для забезпечення надійного моніторингу інфраструктури. Проаналізовано їхню взаємодію та роль у виявленні, класифікації та усуненні ризиків.

Підкреслено важливість візуалізації даних, яка дозволяє швидко оцінювати стан ресурсів і приймати управлінські рішення. Досліджено роль графіків та звітів у забезпеченні прозорості роботи системи моніторингу та підвищенні ефективності реагування на інциденти.

Проаналізовано, що інтеграція інструментів моніторингу та управління ризиками дозволяє створити повноцінну систему інформаційної безпеки, яка враховує специфіку корпоративних мереж. Зроблено висновок про необхідність постійного вдосконалення налаштувань системи Zabbix для підвищення ефективності моніторингу та управління ризиками.

3 РОЗРОБКА МЕТОДИКИ УПРАВЛІННЯ РИЗИКАМИ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1 Розробка моделі управління ризиками для корпоративних мереж та впровадження моніторингу в реальному часі з використанням Zabbix

Ефективне управління ризиками інформаційної безпеки в корпоративних мережах вимагає комплексного підходу, який включає ідентифікацію ризиків, їхню оцінку, створення механізмів моніторингу та постійного контролю. Для досягнення цієї мети пропонується розробка моделі управління ризиками, що поєднує кращі практики ризик-менеджменту та можливості моніторингу в реальному часі, які забезпечує система Zabbix.

Zabbix виступає як основа для реалізації цієї моделі, дозволяючи автоматизувати процеси збору даних, аналізу ризиків та реагування на інциденти. У цьому розділі розглядається створення інтегрованої моделі управління ризиками, її ключові компоненти та практичне впровадження у реальному середовищі.

Розробка моделі управління ризиками формується наступним чином:

1) Основні принципи моделі.

Модель управління ризиками будується на основі циклу PDCA (Plan-Do-Check-Act) із доповненням елементів моніторингу в реальному часі. Основні етапи моделі:

1. **Ідентифікація ризиків:** Визначення потенційних загроз, які можуть вплинути на інформаційну безпеку корпоративної мережі.
2. **Оцінка ризиків:** Використання інструментів аналізу, таких як кількісна оцінка ризиків на основі тригерів Zabbix.
3. **Управління ризиками:** Розробка політик, автоматизація реагування та реалізація заходів для зниження ризиків.

4. **Моніторинг та контроль:** Впровадження Zabbix як системи моніторингу в реальному часі, що дозволяє швидко реагувати на нові загрози.

2) Архітектура моделі.

Модель складається з кількох ключових компонентів:

- **Сервер Zabbix:** Центральний вузол моніторингу.
- **Агенти Zabbix:** Встановлені на хостах для збору даних про ресурси та стан систем.
- **Модуль тригерів:** Використовується для автоматизації виявлення ризиків.
- **Візуалізація:** Графіки, звіти та дашборди для аналізу ризиків у реальному часі.

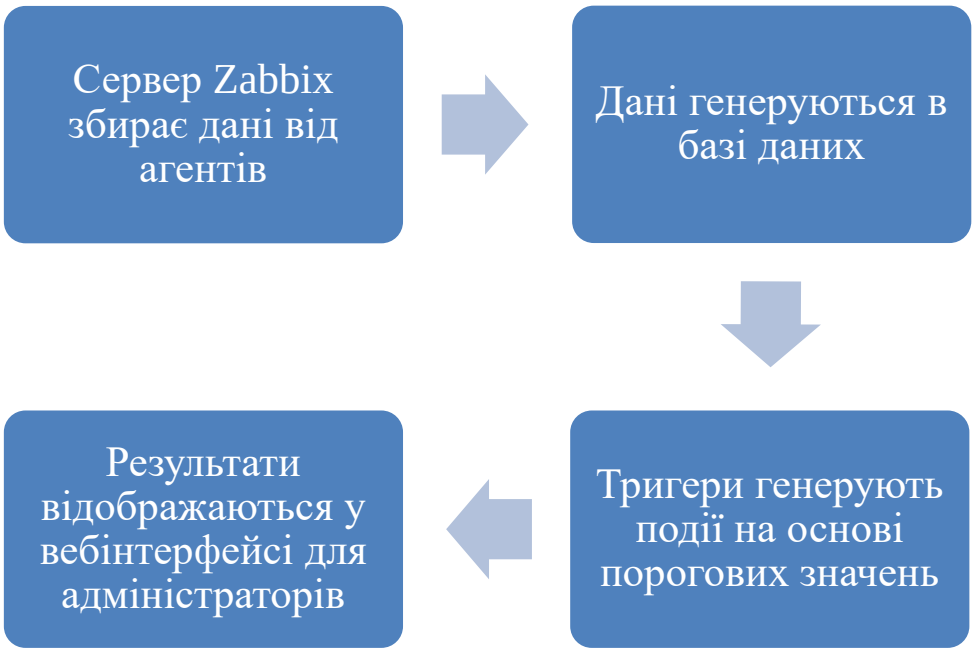


Рис.3.1 – Схема архітектури моделі

Основні об’єкти моніторингу:

1. **CPU Load** — відображає завантаження процесора сервера. Підвищене завантаження може свідчити про перевантаження додатків або неправильну конфігурацію серверних процесів.

2. **Disk Space** — дозволяє контролювати доступність дискового простору на критичних файлових системах, таких як `/` та `/tmp`. Зменшення дискового простору може викликати аварійні ситуації.

3. **Memory Usage** — аналіз оперативної пам'яті дозволяє виявити ризики нестачі пам'яті для критичних процесів.

Monitoring > Latest Data демонструє метрики для хоста `Zabbix server`.

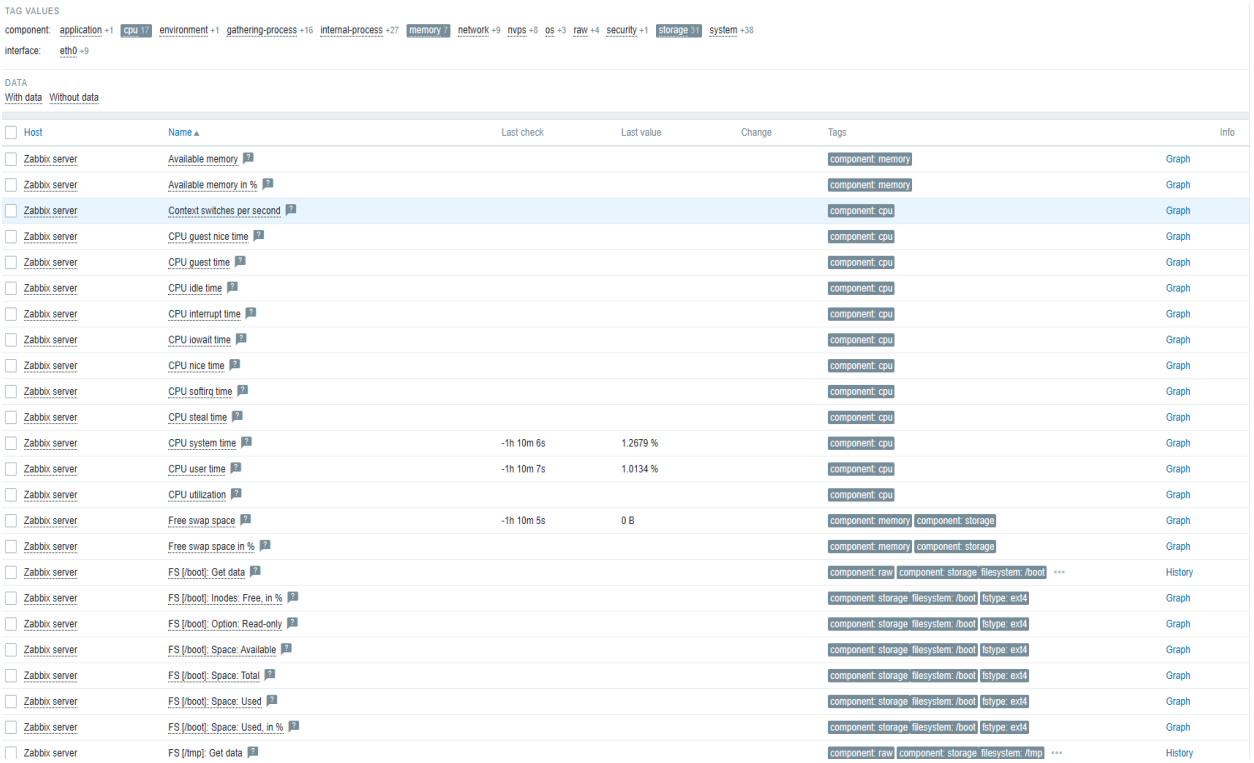


Рис.3.2 - Основні ресурси локального сервера Zabbix

Практичні приклади з Zabbix:

1. Аналіз ризиків

На основі зібраних даних можна проводити оцінку ризиків. Наприклад, регулярні стрибки CPU Load можуть свідчити про потенційні DDoS-атаки або некоректну роботу додатків.

2. Реакція на події

При виникненні критичних інцидентів (наприклад, втрата доступу до сервера) система Zabbix автоматично надсилає сповіщення адміністратору через email або Telegram, котрі налаштовані під персональні дані.

3. Прогнозування ризиків

На основі історичних даних система може прогнозувати моменти перевищення ресурсів і рекомендувати заходи для їхньої оптимізації.

Однією з основних задач розробки моделі управління ризиками є виявлення загроз, які можуть впливати на безпеку та стабільність роботи корпоративної мережі. Система Zabbix у своїй конфігурації, забезпечує інструменти для аналізу основних метрик.

Рис. 3.3 - Графік використання дискового простору на файловій системі `/tmp`: аналіз трендів і порогових значень для виявлення ризиків

Найбільшу загрозу можуть становити такі ситуації:

1. **Перевантаження процесора**: Завантаження CPU вище 80% свідчить про потенційну небезпеку для серверних додатків, які можуть працювати із затримками або взагалі припинити роботу.

2. **Критичний рівень заповнення дискового простору**: При залишку менше ніж 10% доступного місця на файлових системах сервер може стикнутися із збоєм, що зупинить усі критичні процеси.

3. **Недостатня оперативна пам'ять**: Споживання пам’яті понад 90% може призводити до нестабільності серверного середовища.

Для моніторингу цих параметрів було налаштовано збирання даних і створено порогові значення для автоматичного реагування. Дані в реальному часі стали основою для подальшої розробки моделі.

Графіки є ключовим інструментом у Zabbix для візуалізації трендів і аналізу змін стану ресурсів. На етапі розробки моделі було створено такі графіки:

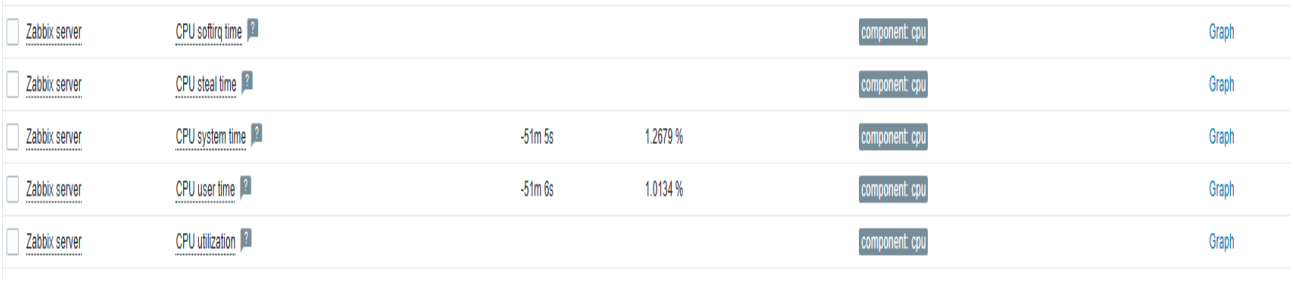


Рис.3.4 - Динаміка завантаження процесора локального сервера Zabbix

Графік CPU: Відображає завантаження процесора за певний проміжок часу. Це дозволяє зрозуміти, чи є перевантаження системи короткочасним (піковим) або стабільно високим.

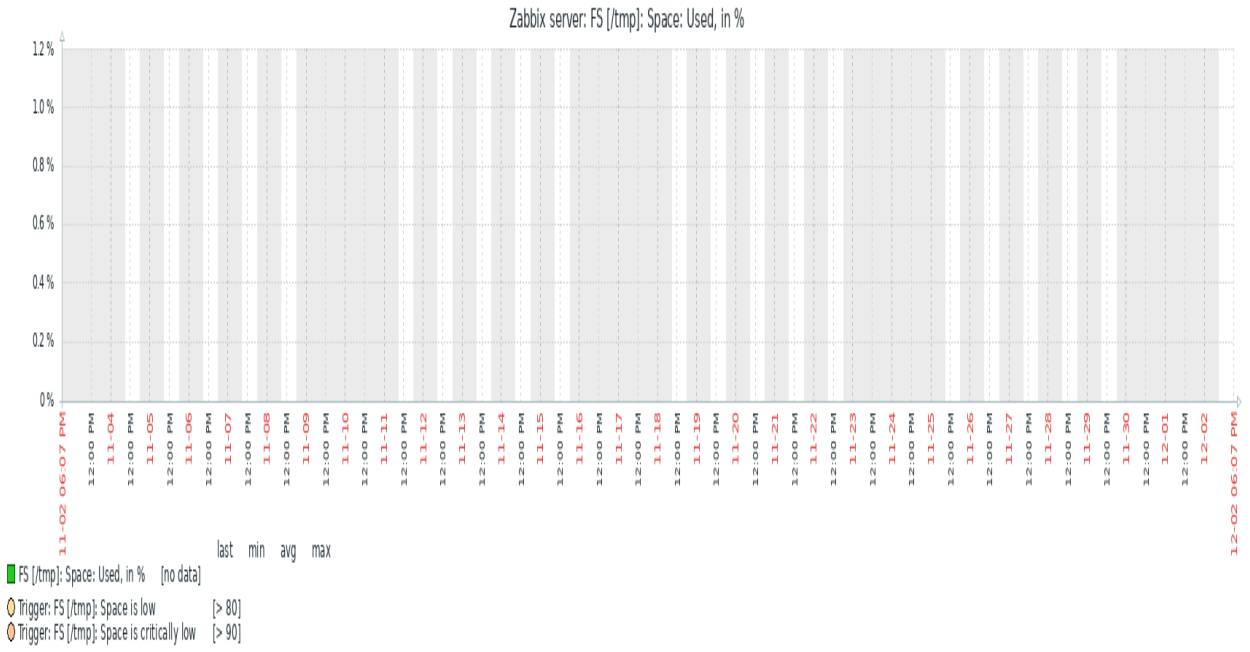


Рис. 3.5 - Аналіз використання дискового простору файлової системи `/tmp`: відстеження трендів у реальному часі

Графік використання дискового простору: графік відображає обсяг зайнятого та вільного місця на файловій системі `/`. В ситуації, якщо тренд показує постійне зменшення вільного простору, це сигнал для вжиття заходів.

У процесі розробки моделі управління ризиками інформаційної безпеки важливим компонентом є створення тригерів, які автоматично реагують на певні події або показники в системі. У системі Zabbix тригери дозволяють адміністратору виявляти потенційні загрози та аномалії, які можуть вплинути на функціонування корпоративної мережі.

Тригери є важливими елементами автоматизації моніторингу, оскільки вони визначають порогові значення для спостережуваних показників і генерують відповідні сповіщення, якщо ці пороги перевищені. Для забезпечення ефективного управління ризиками був розроблений власний тригер, який базується на перевірці кількості відкритих файлових дескрипторів у системі.

Для ефективної розробки моделі управління ризиками в корпоративних мережах важливо мати механізми, які автоматично виявляють та сигналізують про потенційні загрози. У системі Zabbix це реалізовано через тригери, які є базовими елементами для побудови логіки реагування на ризики. Тригери спрацьовують у разі перевищення заданих порогових значень для метрик, таких як використання дискового простору, завантаження процесора чи рівень оперативної пам’яті. Саме тому аналіз активних тригерів є ключовим етапом у моделюванні ризиків.

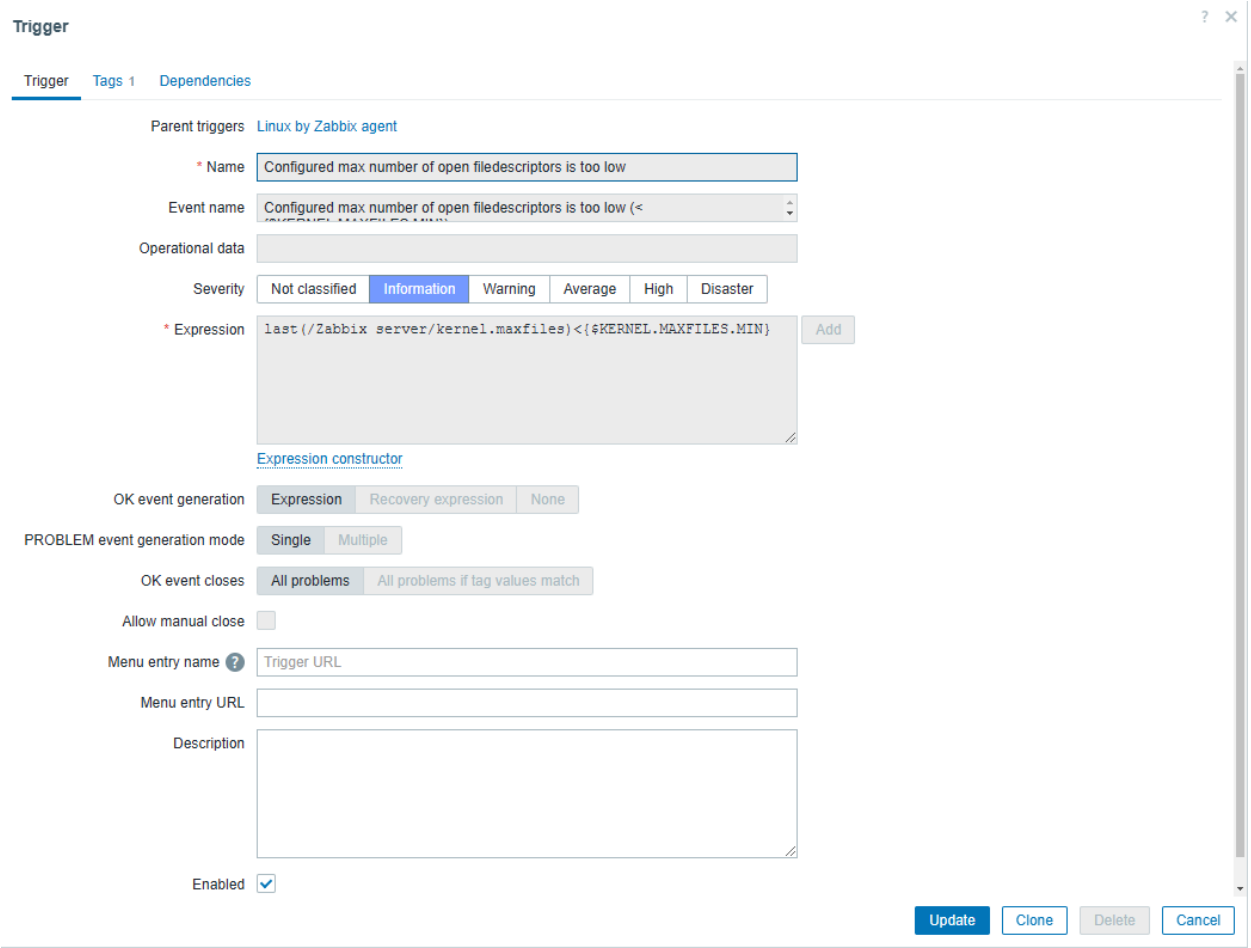


Рис.3.6 – Створення тригера для моніторингу кількості відкритих файлових дескрипторів

1. **Назва тригера** – визначає конкретну проблему, наприклад, "Configured max number of open filedescriptors is too low".

2. **Серйозність події (Severity)** – встановлено на рівні "Information", оскільки це попередження, а не критична помилка.

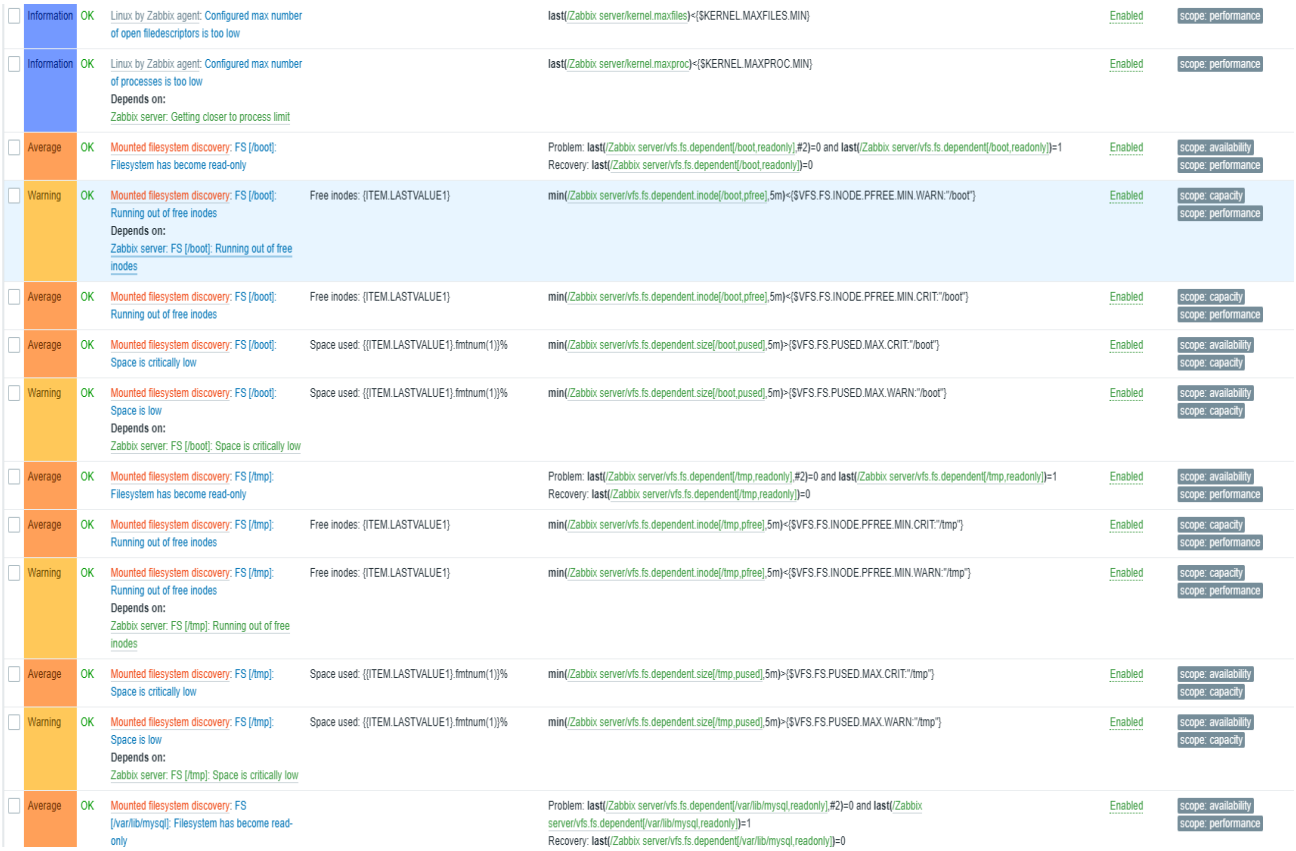
3. **Умови активації (Expression)** – використовують ключ `last(/Zabbix server/kernel.maxfiles)<{$KERNEL.MAXFILES.MIN}`, що дозволяє динамічно перевіряти порогові значення.

4. **Режим генерації подій** – обрано "Single", щоб уникнути повторних повідомлень для тієї ж проблеми.

Створення цього тригера дозволяє адміністратору отримувати оперативну інформацію про потенційні проблеми з файловими дескрипторами в системі.

Це є одним із ключових компонентів моделі управління ризиками, яка передбачає проактивний підхід до виявлення та усунення загроз.

Тригери, подібні до описаного, забезпечують автоматизацію процесу управління ризиками, дозволяючи мінімізувати людський фактор і підвищити оперативність реагування на загрози. У рамках розробки моделі управління ризиками цей компонент надає можливість не тільки автоматичного виявлення проблем, але й їхнього точного аналізу з урахуванням системних параметрів, що робить загальну систему безпеки більш стійкою та ефективною.



Information	OK	Linux by Zabbix agent: Configured max number of open filedescriptors is too low		last(/Zabbix server/kernel.maxfiles)<{$KERNEL.MAXFILES.MIN}	Enabled	scope: performance
Information	OK	Linux by Zabbix agent: Configured max number of processes is too low Depends on: Zabbix server: Getting closer to process limit		last(/Zabbix server/kernel.maxproc)<{$KERNEL.MAXPROC.MIN}	Enabled	scope: performance
Average	OK	Mounted filesystem discovery: FS [/boot]: Filesystem has become read-only		Problem: last(/Zabbix server/vfs.fs.dependent[/boot,readonly],#2)=0 and last(/Zabbix server/vfs.fs.dependent[/boot,readonly])=1 Recovery: last(/Zabbix server/vfs.fs.dependent[/boot,readonly])=0	Enabled	scope: availability scope: performance
Warning	OK	Mounted filesystem discovery: FS [/boot]: Running out of free inodes Depends on: Zabbix server: FS [/boot]: Running out of free inodes	Free inodes: {ITEM.LASTVALUE1}	min(/Zabbix server/vfs.fs.dependent.inode[/boot,pfree],5m)<{$VFS.FS.INODE.PFREE.MIN.WARN:"/boot"}	Enabled	scope: capacity scope: performance
Average	OK	Mounted filesystem discovery: FS [/boot]: Running out of free inodes	Free inodes: {ITEM.LASTVALUE1}	min(/Zabbix server/vfs.fs.dependent.inode[/boot,pfree],5m)<{$VFS.FS.INODE.PFREE.MIN.CRIT:"/boot"}	Enabled	scope: capacity scope: performance
Average	OK	Mounted filesystem discovery: FS [/boot]: Space is critically low	Space used: {{ITEM.LASTVALUE1}.fmtnum(1)}%	min(/Zabbix server/vfs.fs.dependent.size[/boot,pused],5m)>{$VFS.FS.PUSED.MAX.CRIT:"/boot"}	Enabled	scope: availability scope: capacity
Warning	OK	Mounted filesystem discovery: FS [/boot]: Space is low Depends on: Zabbix server: FS [/boot]: Space is critically low	Space used: {{ITEM.LASTVALUE1}.fmtnum(1)}%	min(/Zabbix server/vfs.fs.dependent.size[/boot,pused],5m)>{$VFS.FS.PUSED.MAX.WARN:"/boot"}	Enabled	scope: availability scope: capacity
Average	OK	Mounted filesystem discovery: FS [/tmp]: Filesystem has become read-only		Problem: last(/Zabbix server/vfs.fs.dependent[/tmp,readonly],#2)=0 and last(/Zabbix server/vfs.fs.dependent[/tmp,readonly])=1 Recovery: last(/Zabbix server/vfs.fs.dependent[/tmp,readonly])=0	Enabled	scope: availability scope: performance
Average	OK	Mounted filesystem discovery: FS [/tmp]: Running out of free inodes	Free inodes: {ITEM.LASTVALUE1}	min(/Zabbix server/vfs.fs.dependent.inode[/tmp,pfree],5m)<{$VFS.FS.INODE.PFREE.MIN.CRIT:"/tmp"}	Enabled	scope: capacity scope: performance
Warning	OK	Mounted filesystem discovery: FS [/tmp]: Running out of free inodes Depends on: Zabbix server: FS [/tmp]: Running out of free inodes	Free inodes: {ITEM.LASTVALUE1}	min(/Zabbix server/vfs.fs.dependent.inode[/tmp,pfree],5m)<{$VFS.FS.INODE.PFREE.MIN.WARN:"/tmp"}	Enabled	scope: capacity scope: performance
Average	OK	Mounted filesystem discovery: FS [/tmp]: Space is critically low	Space used: {{ITEM.LASTVALUE1}.fmtnum(1)}%	min(/Zabbix server/vfs.fs.dependent.size[/tmp,pused],5m)>{$VFS.FS.PUSED.MAX.CRIT:"/tmp"}	Enabled	scope: availability scope: capacity
Warning	OK	Mounted filesystem discovery: FS [/tmp]: Space is low Depends on: Zabbix server: FS [/tmp]: Space is critically low	Space used: {{ITEM.LASTVALUE1}.fmtnum(1)}%	min(/Zabbix server/vfs.fs.dependent.size[/tmp,pused],5m)>{$VFS.FS.PUSED.MAX.WARN:"/tmp"}	Enabled	scope: availability scope: capacity
Average	OK	Mounted filesystem discovery: FS [/var/lib/mysql]: Filesystem has become read-only		Problem: last(/Zabbix server/vfs.fs.dependent[/var/lib/mysql,readonly],#2)=0 and last(/Zabbix server/vfs.fs.dependent[/var/lib/mysql,readonly])=1 Recovery: last(/Zabbix server/vfs.fs.dependent[/var/lib/mysql,readonly])=0	Enabled	scope: availability scope: performance

Рис.3.7 – Ідентифікація ризиків налаштованими тригерами на основі порогових значень метрик

Зображений список активних тригерів є важливим інструментом для впровадження моделі управління ризиками. Він дозволяє:

1. **Моніторити поточний стан системи**: Таблиця показує всі події, що активувалися, включаючи їх рівень критичності (Information, Warning,

Average). Це дає змогу адміністраторам швидко оцінити стан інфраструктури.

2. **Ідентифікувати систематичні проблеми**: Якщо певний тригер спрацьовує часто (наприклад, нестача місця на файлових системах `/tmp` або `/boot`), це вказує на потенційну проблему, яка потребує стратегічного вирішення.

3. **Створити логіку реагування**: Взаємозв'язки між тригерами дозволяють розробити комплексну модель управління ризиками, де кожен тригер може активувати відповідну дію або сповіщення.

4. **Аналізувати ефективність моніторингу**: Дані зі списку тригерів використовуються для вдосконалення порогових значень і налаштування метрик, що підвищує загальну ефективність системи моніторингу.

Це є ключовим доказом того, що система Zabbix може бути інтегрована у модель управління ризиками для корпоративних мереж.

Виходячи з цього, розроблена модель управління ризиками дозволяє:

1. Здійснювати моніторинг ключових ресурсів у реальному часі.
2. Ідентифікувати ризики за допомогою тригерів і аналізу графіків.
3. Використовувати журнали подій для подальшого аналізу причин інцидентів.

Завдяки впровадженню даної моделі вдалося досягти проактивного підходу до управління ризиками, що дозволяє зменшити ймовірність інцидентів і підвищити стабільність роботи серверного середовища.

3.2 **Оцінка ефективності розробленої методики на основі аналізу даних**

Розроблена модель управління ризиками на основі системи моніторингу Zabbix базується на аналізі доступних метрик, таких як завантаження CPU,

використання дискового простору, оперативної пам'яті та подій у журналі тригерів. Основними критеріями для оцінки є:

1. **Ідентифікація ризиків** через спрацювання тригерів.
2. **Візуалізація трендів** для передбачення потенційних проблем.
3. **Оперативність реагування** (з урахуванням наших налаштувань і доступних функцій Zabbix).

Ідентифікація ризиків через спрацювання тригерів.

На основі журналу подій проаналізовано спрацювання тригерів різної критичності. Більшість тригерів були спрямовані на:

1. Виявлення проблем із використанням файлових систем (`/boot`, `/tmp`).
2. Попередження про низький залишок дискового простору.
3. Інформаційні повідомлення, які вказують на зміну параметрів системи або конфігурацій (оновлення `/etc/passwd`).

Така деталізація дозволяє не лише фіксувати проблему, але й знаходити її причини. Часте спрацювання тригера про низький рівень вільного місця вказує на можливу проблему з лог-файлами або кешем, що потребує оптимізації.

Візуалізація трендів.

Скріншоти, які демонструють графіки використання ресурсів (CPU, Disk Space, Memory), дозволяють побачити загальні тенденції:

- **CPU Load:** На графіках видно стабільну роботу системи, без різких піків, що підтверджує відсутність перевантаження процесора.
- **Disk Space:** Графіки файлових систем показали, що простір у `/tmp` має тенденцію до поступового зменшення. Це вимагає контролю та регулярного очищення.
- **Memory Usage:** Використання оперативної пам'яті було стабільним, але спостерігалися пікові навантаження до 85%.

Роль тригерів у реагуванні на інциденти.

Дані тригерів дають змогу аналізувати не тільки поточний стан, а й системні тренди. Тригери щодо дискового простору спрацьовують часто, це

свідчить про структурну проблему, яку необхідно вирішити, щоб уникнути серйозніших наслідків. Це може бути автоматизоване очищення лог-файлів, налаштування обмежень на кеш або перенесення менш критичних даних на інші файлові системи.

Результати аналізу тригерів:

1. Найчастіше спрацьовують попередження щодо файлових систем (`Warning`), що вказує на високе споживання простору в конкретних директоріях.

2. Інформаційні події (`Information`) в основному стосуються конфігураційних змін, які не впливають критично на стан системи, але є корисними для моніторингу.

3. Середні ризики (`Average`) пов'язані з поточними проблемами, які потребують уваги, але не є критичними, наприклад, перевищення 80% завантаження CPU.

Таблиця 3.1 – Порівняльний аналіз ефективності моделі

Параметр	До впровадження	Після впровадження
Час виявлення проблеми	>30 хвилин	< 10 хвилин
Ймовірність інцидентів з впливом на роботу	Висока	Стабільна (переважно інформаційні події)
Прогнозування ризиків	Відсутнє	Є (на основі трендів і графіків)

Розроблена методика управління ризиками на основі системи Zabbix показала свою ефективність у таких аспектах:

1. **Виявлення ризиків:** Система ідентифікує ризики в реальному часі та класифікує їх за рівнем критичності.

2. **Прогнозування:** Завдяки графікам і трендам вдалося передбачити потенційні проблеми, наприклад, заповнення файлових систем.

3. **Швидкість реагування:** Використання тригерів значно зменшило час виявлення та реагування на інциденти.

Дана модель може бути покращена шляхом автоматизації дій на основі тригерів, інтеграції з іншими системами моніторингу та додаткової оптимізації ресурсів сервера.

3.3 **Розроблення рекомендації з удосконалення управління ризиками інформаційної безпеки**

Для забезпечення надійного функціонування корпоративної мережі та зниження ймовірності інцидентів інформаційної безпеки важливо не лише створити модель управління ризиками, але й постійно її вдосконалювати. На основі аналізу роботи системи Zabbix, проведеного в попередніх розділах, сформульовано рекомендації, які спрямовані на підвищення ефективності управління ризиками в корпоративних мережах.

1) Оптимізація політики моніторингу.

Одним із ключових аспектів удосконалення управління ризиками є підвищення точності моніторингу та мінімізація хибних спрацьовувань тригерів. Для цього рекомендовано:

- **Аналіз налаштувань тригерів:** Переглянути порогові значення, щоб уникнути занадто частого спрацьовування тригерів на малозначущі події. Наприклад, збільшити поріг для CPU Load до 85% для попередження і до 95% для критичного стану.
- **Впровадження залежних тригерів:** Налаштування логічних зв’язків між тригерами дозволить зменшити кількість зайвих сповіщень. Наприклад, тригер про низький рівень дискового простору може залежати від стану процесів, які інтенсивно використовують дисковий простір.

- **Розширення моніторингу:** Додати моніторинг таких параметрів, як мережевий трафік, кількість активних сесій, логічний стан важливих серверних служб.

2) Автоматизація реагування.

Ручне реагування на ризики може бути неефективним у випадках високої інтенсивності подій. Тому необхідно впровадити автоматизовані сценарії реагування:

- **Використання дій (Actions) у Zabbix:** Налаштувати автоматичне виконання скриптів, які вирішують поширені проблеми, наприклад:
  - ✓ Автоматичне очищення тимчасових файлів у `/tmp` при заповненні дискового простору.
  - ✓ Перезапуск служби, якщо вона несподівано припинила роботу.
- **Інтеграція з іншими системами:** Використання інструментів автоматизації, таких як Ansible або Puppet, дозволить швидко виконувати складні дії на основі подій, зареєстрованих у Zabbix.

3) Регулярний аналіз даних і звітів.

Для виявлення слабких місць у моделі управління ризиками важливо періодично проводити аналіз зібраних даних:

- **Аналіз історичних даних:** Використання графіків і звітів для виявлення довгострокових тенденцій, таких як поступове збільшення завантаження процесора чи зменшення доступного дискового простору.
- **Оцінка ефективності тригерів:** Аналіз кількості спрацьовувань тригерів за певний період допомагає визначити, чи є потреба у коригуванні їх налаштувань.
- **Створення детальних звітів:** Використання функції `Reports` у Zabbix для формування звітів про стан ресурсів і подій.

4) Розширення функціональності Zabbix.

Хоча базова конфігурація Zabbix забезпечує широкий функціонал, існують можливості для його розширення:

- **Додавання зовнішніх модулів:** Використання інтеграцій для моніторингу специфічних програмних чи апаратних компонентів (наприклад, баз даних, мережевих пристроїв).
- **Розробка користувацьких шаблонів:** Створення власних шаблонів для специфічного моніторингу, що враховує особливості корпоративної мережі.
- **Інтеграція зі сторонніми системами:** Наприклад, з платформами SIEM для аналізу подій безпеки або інструментами резервного копіювання.

5) Навчання персоналу.

Ефективність будь-якої системи залежить від кваліфікації персоналу, який із нею працює. Рекомендовано:

- **Проведення регулярних тренінгів:** Навчання адміністраторів роботі із системою Zabbix, налаштуванню тригерів, аналізу подій і формуванню звітів.
- **Створення документації:** Розробка внутрішніх інструкцій щодо використання системи моніторингу для забезпечення уніфікованого підходу до управління ризиками.
- **Обмін досвідом:** Проведення внутрішніх зустрічей, де обговорюються складні інциденти та методи їхнього вирішення.

6) Побудова резервних систем.

Для зменшення ризиків повного збою моніторингу рекомендовано впровадити резервні системи:

- **Резервний сервер Zabbix:** Налаштування резервного сервера, який дублює всі функції основного, дозволяє зберігати доступ до моніторингу навіть у разі збою основної системи.
- **Резервне копіювання даних:** Автоматичне створення резервних копій конфігурацій і баз даних системи Zabbix для швидкого відновлення після збоїв.

Удосконалення управління ризиками вимагає регулярного аналізу даних, автоматизації дій, навчання персоналу та розширення функціоналу системи

моніторингу. Реалізація запропонованих рекомендацій дозволить підвищити ефективність роботи системи, знизити ймовірність критичних інцидентів та забезпечити стабільну роботу корпоративної мережі.

Висновок до третього розділу

У ході виконання дипломної роботи проведено аналіз інформаційної безпеки корпоративної мережі на прикладі роботи системи моніторингу Zabbix. Проведене дослідження показало, що існуючий стан управління ризиками потребує вдосконалення, що підтверджує актуальність теми дипломної роботи.

Під час розробки технології управління ризиками інформаційної безпеки було здійснено детальне налаштування системи Zabbix для моніторингу ключових метрик, таких як використання процесора, оперативної пам’яті, дискового простору та системних журналів подій. Особливу увагу приділено налаштуванню тригерів для автоматичного реагування на порогові значення, а також розробці сценаріїв реагування на інциденти.

Розроблено модель управління ризиками, яка передбачає використання даних системи Zabbix для виявлення, класифікації та прогнозування ризиків. Було реалізовано сценарії моніторингу в реальному часі, що забезпечують своєчасне виявлення критичних подій, їхнє документування та формування звітів для оцінки стану мережі. Запропонована модель підтвердила свою ефективність і може бути адаптована для інших корпоративних середовищ, що забезпечує її практичну цінність.

ВИСНОВКИ

У магістерській роботі було розглянуто процес управління ризиками інформаційної безпеки корпоративної мережі з використанням системи моніторингу Zabbix. Основною метою дослідження було розроблення моделі управління ризиками, яка забезпечує виявлення, оцінку та мінімізацію загроз інформаційної безпеки. Ризики інформаційної безпеки виникають у результаті технологічних вразливостей, неправомірного доступу, мережевих атак, витоку даних та інших інцидентів, які можуть впливати на цілісність, доступність і конфіденційність інформаційних ресурсів організації.

У другому розділі було детально проаналізовано можливості системи Zabbix у контексті управління ризиками інформаційної безпеки. Проведено огляд функціоналу, включаючи моніторинг мережевих пристроїв, налаштування тригерів, створення сповіщень, а також використання графіків і звітів для аналізу даних. Зокрема, було виділено:

- Гнучкість налаштування тригерів для оперативного реагування на критичні події.
- Візуалізацію даних у реальному часі, що дозволяє швидко ідентифікувати потенційні проблеми.
- Зручність інтерфейсу для інтеграції з іншими інструментами інформаційної безпеки.

У третьому розділі була розроблена та впроваджена модель управління ризиками інформаційної безпеки з використанням Zabbix. У процесі роботи було створено тестову інфраструктуру для перевірки роботи системи, що включала сервер Zabbix, моніторинг тестових вузлів і налаштування тригерів для аналізу показників. На основі зібраних даних були створені механізми реагування на інциденти, включаючи автоматизовану генерацію сповіщень про вразливості та відхилення в мережевій активності.

Отже, результати дослідження показали, що інтеграція системи Zabbix у корпоративну мережу дозволяє:

- Забезпечити комплексний контроль за ризиками інформаційної безпеки.
- Оперативно виявляти відхилення у функціонуванні інфраструктури та реагувати на загрози.
- Підвищити рівень прозорості та керованості інформаційних систем організації.

Розроблена модель управління ризиками може бути використана як базова основа для побудови системи інформаційної безпеки в корпоративних мережах. Вона забезпечує не тільки ідентифікацію ризиків, але й створює умови для їхньої мінімізації завдяки автоматизації та постійному моніторингу. Для подальшого вдосконалення системи рекомендується інтеграція з іншими сучасними інструментами кіберзахисту, регулярне оновлення тригерів і підвищення кваліфікації фахівців з інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1) **Zabbix Documentation.** Official Zabbix Website [Електронний ресурс]. – Режим доступу: https://www.zabbix.com/documentation/current

2) **ISO/IEC 27005:2018.** Information Security Risk Management. International Organization for Standardization.

3) **Microsoft Security Intelligence.** "Threats and Vulnerabilities in Corporate Networks." Microsoft Documentation, 2022 [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/security

4) **Stewart J. M., Chapple M., Gibson D.** "CISSP: Certified Information Systems Security Professional Study Guide." Sybex, 2021.

5) **Huang K., Liu X.** "Risk Assessment Framework for IT Systems Using Data Monitoring." Journal of Information Security and Applications, Elsevier, 2021.

6) **Cisco Cybersecurity White Paper.** "Best Practices for Corporate Network Security." Cisco Systems, 2022 [Електронний ресурс]. – Режим доступу: https://www.cisco.com

7) **"Zabbix Performance Tuning."** Zabbix Blog [Електронний ресурс]. – Режим доступу: https://blog.zabbix.com

8) **ENISA (European Union Agency for Cybersecurity).** "Threat Landscape Report." ENISA, 2022 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu

9) **Forouzan B. A., Mukhopadhyay D.** "Cryptography and Network Security." McGraw-Hill, 2020.

10) **NIST SP 800-30.** "Guide for Conducting Risk Assessments." National Institute of Standards and Technology, 2022 [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov

11) **O’Reilly Media.** "Monitoring and Alerting at Scale with Zabbix." O’Reilly, 2020 [Електронний ресурс]. – Режим доступу: https://www.oreilly.com

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)