МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «РОЗРОБКА СИСТЕМИ РЕАЛІЗАЦІЇ БЕЗПЕРЕРВНОГО МОНІТОРИНГУ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

на здобуття освітнього ступеня бакалавр
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Микола МОКОВОЗЮК
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи УБЗ-51
МОКОВОЗЮК Микола
(прізвище, ім'я)

Керівник ПОРОХНИЦЬКИЙ Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньої програми Управління інформаційною та кібернетичною безпекою.

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“___” _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Моковозюк Микола Олександрович
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури»
керівник кваліфікаційної роботи Порохницький Олександр
(прізвище, ім’я, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологій від “27“ лютого 2024 р. № 36.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 20.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи: аудит управління, доступу та цілістності системи;
рішення безперебійного моніторингу на базі Zabbix;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки:
1. Аналіз методів та засобів забезпечення безперервного моніторингу.
2. Аудит управління, доступу та цілістності.
3. Розроблення системи реалізації безперервного моніторингу за допомогою Zabbix.

5. Перелік графічного матеріалу: Презентація PowerPoint

6. Дата видачі завдання 11.03.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми.	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	20.04.2024 р.	
3.	Аналіз методів та засобів забезпечення безперервного моніторингу.	25.04.2024 р.	
4.	Аудит управління, доступу та цілісності системи .	10.05.2024 р.	
5.	Розроблення системи реалізації безперервного моніторингу за допомогою ZABBIX.	15.05.2024 р.	
6.	Оформлення результатів дослідження.	20.04.2024 р.	
7.	Підготовка доповіді до захисту.	25.05.2024 р.	
8.	Оформлення презентації.	03.06.2024 р.	
9.	Отримання рецензії на роботу.	03.06.2024 р.	
10.	Захист в ДЕК.	__.06.2024 р.	

Здобувач вищої освіти _____ Микола МОКОВОЗЮК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) *(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Моковозюк М.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач МОКОВОЗЮК Микола обрав тему роботи, метою якої було розробка і впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури з метою підвищення рівня безпеки та стійкості цих об'єктів до кібератак. Результати дослідження даної теми та використані джерела свідчать про відповідальний підхід до виконання поставленого завдання перед здобувачем, також слід зазначити що він продемонстрував вміння самостійно працювати з науковими матеріалами.

Під час виконання кваліфікаційної роботи МОКОВОЗЮК Микола показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та дотримувався розкладу за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача МОКОВОЗЮКА Миколи на оцінку **«добре»** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач МОКОВОЗЮК Микола допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
Управління інформаційною
та кібернетичною безпекою

_____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача Моковозюк Микола
на тему: «Розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури».

Актуальність:

У сучасному світі кібербезпека стала однією з найбільш актуальних проблем, особливо коли йдеться про критичну інфраструктуру. Кібератаки на об'єкти критичної інфраструктури можуть мати серйозні наслідки, такі як переривання роботи систем життєзабезпечення, знищення даних або навіть загроза життю людей.

Однією з основних стратегій захисту критичної інфраструктури є безперервний моніторинг загроз кібербезпеки. Цей підхід передбачає постійне виявлення, аналіз та реагування на потенційні загрози з метою запобігання або мінімізації їх впливу на інфраструктуру.

У даній дипломній роботі розглядається розробка системи реалізації безперервного моніторингу загроз кібербезпеки для критичної інфраструктури на базі Zabbix. Основними завданнями роботи є аналіз існуючих підходів до моніторингу кібербезпеки, тестування системи на реальних даних.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми моніторингу загроз кібербезпеці для критичної інфраструктури. Проаналізовано існуючі технології контролю доступу до мережі організації.
2. Проаналізовано методи та засоби забезпечення безперервного моніторингу.
3. Запропоновано розроблення системи реалізації безперервного моніторингу за допомогою Zabbix.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. Потрібно більше деталей щодо практичної реалізації системи та її впливу на реальний захист критичної інфраструктури
2. Деякі аспекти безперервного моніторингу можуть бути недостатньо розглянуті або вимагають додаткового вдосконалення для забезпечення повноцінного функціонування системи

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **Моковозюк Микола -** присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ _____

підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 57 сторінок, 25 рисунків, 23 джерел.

У сучасному світі кібербезпека стала однією з найбільш актуальних проблем, особливо коли йдеться про критичну інфраструктуру. Кібератаки на об'єкти критичної інфраструктури можуть мати серйозні наслідки, такі як переривання роботи систем життєзабезпечення, знищення даних або навіть загроза життю людей.

Однією з основних стратегій захисту критичної інфраструктури є безперервний моніторинг загроз кібербезпеки. Цей підхід передбачає постійне виявлення, аналіз та реагування на потенційні загрози з метою запобігання або мінімізації їх впливу на інфраструктуру.

У даній дипломній роботі розглядається розробка системи реалізації безперервного моніторингу загроз кібербезпеки для критичної інфраструктури на базі Zabbix. Основними завданнями роботи є аналіз існуючих підходів до моніторингу кібербезпеки, тестування системи на реальних даних.

Метою дослідження є розробка і впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури з метою підвищення рівня безпеки та стійкості цих об'єктів до кібератак.

Об’єкт дослідження є процес розробки та впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури.

Предмет дослідження є розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури.

КЛЮЧОВІ СЛОВА: ZABBIX, АУДИТ, МОНІТОРИНГ КРИТИЧНА ІНФРАСТРУКТУРА

ABSTRACT

The text part of the qualification work: 57 pages, 25 figures, 23 sources.

In the modern world, cybersecurity has become one of the most pressing issues in the modern world, especially when it comes to critical infrastructure.

Cyberattacks on critical infrastructure can have serious consequences, such as interruption of life support systems, data destruction, or even threatening human life.

One of the main strategies to protect critical infrastructure is to continuously monitor infrastructure is to continuously monitor cybersecurity threats. This approach involves the constant identification, analysis and response to potential threats in order to in order to prevent or minimize their impact on the infrastructure.

This thesis deals with the development of a system for for the implementation of continuous monitoring of cybersecurity threats for critical infrastructure based on Zabbix. The main objectives of the work are to analyze existing approachesto cybersecurity monitoring, testing the system on real data.

The aim of the study is to develop and implement a system for monitoring cybersecurity threats for critical infrastructure facilities in order to increase the level of security and resilience of these facilities to cyberattacks.

The object of research is the process of development and implementation of a cybersecurity threat monitoring system for critical infrastructure facilities.

The subject of the study is the development of a system for the implementation of continuous monitoring of cybersecurity threats to critical infrastructure.

KEYWORDS: ZABBIX, AUDIT, CRITICAL INFRASTRUCTURE MONITORING

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасному світі кібербезпека стала однією з найбільш актуальних проблем, особливо коли йдеться про критичну інфраструктуру. Кібератаки на об'єкти критичної інфраструктури можуть мати серйозні наслідки, такі як переривання роботи систем життєзабезпечення, знищення даних або навіть загроза життю людей.

Однією з основних стратегій захисту критичної інфраструктури є безперервний моніторинг загроз кібербезпеки. Цей підхід передбачає постійне виявлення, аналіз та реагування на потенційні загрози з метою запобігання або мінімізації їх впливу на інфраструктуру.

У даній дипломній роботі розглядається розробка системи реалізації безперервного моніторингу загроз кібербезпеки для критичної інфраструктури на базі Zabbix. Основними завданнями роботи є аналіз існуючих підходів до моніторингу кібербезпеки, тестування системи на реальних даних.

Ця робота має велике значення для підвищення рівня кібербезпеки критичної інфраструктури та забезпечення безперервності її роботи в умовах постійно зростаючих загроз кібернетичної безпеки.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становить розробка системи безперервного моніторингу загроз.

Об’єкт дослідження – процес розробки та впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури.

Предмет дослідження – розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури.

Мета роботи розробка і впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури з метою підвищення рівня безпеки та стійкості цих об'єктів до кібератак.

Наукові завдання:

– Провести огляд понять та термінів в галузі кібербезпеки.

– Визначити основні загрози та ризики для критичної інфраструктури.

– Розглянути процес аудиту інформаційної безпеки.

– Налаштувати політику аудиту системи.

– Проаналізувати існуючі системи безперервного моніторингу загроз.

– Впровадити систему моніторингу Zabbix для аналізу управління обліковими записами, доступу до об'єктів файлової системи та цілісності системи.

– Налаштувати систему моніторингу для ефективного виявлення та реагування на загрози кібербезпеки.

– Провести аналіз ефективності розробленої системи та зробити висновки щодо її використання для захисту критичної інфраструктури.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації.

Розділ 1 ТЕОРЕТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В сучасному світі кібербезпека стає все більш важливою складовою для забезпечення безпеки критичної інфраструктури. Високотехнологічні атаки та кіберзлочинність можуть миттєво викликати серйозні загрози для функціонування критичних систем, таких як електроенергетика, транспорт, комунікації та інші. У зв'язку з цим важливо розглядати теоретичні аспекти моніторингу кібербезпеки для критичної інфраструктури, щоб розробляти ефективні заходи захисту та реагування на потенційні загрози.

1.1 Огляд поняття моніторингу та термінів в галузі кібербезпеки

Моніторинг мережі - це система, яка вказує на уповільнення роботи мережі або непрацездатність мережевих пристроїв. Моніторинг базується на аналізі пропускної здатності, частоти помилок, втрат і затримок пакетів, доступності маршрутизаторів і комутаторів, а також часу відгуку. У разі збою мережеві адміністратори отримують повідомлення про збій за допомогою попереджувальних банерів, електронних листів, телефонних дзвінків та інших сповіщень [1].

Моніторинг мережі також є стратегічним інструментом у сучасному бізнесі. Він допомагає оптимізувати потік даних і виявити ненадійне обладнання. Він також перевіряє пропускну здатність і стан обладнання, включаючи температуру і доступність. В результаті моніторинг мережі максимізує її продуктивність і знижує ймовірність перебоїв у роботі. Основними перевагами оптимізованої мережі для компаній є зниження витрат на інфраструктуру, підвищення ефективності роботи співробітників, збільшення продуктивності та швидкі, надійні потоки даних.

Існує хибна думка, що моніторинг мережі також виконує функцію контролю безпеки і запобігає несанкціонованому доступу до мережі. Для цього типу моніторингу безпеки використовуються системи запобігання вторгнень (IPS) і

системи виявлення вторгнень (IDS). Моніторинг мережі використовується лише для моніторингу використання та надійності мережі. Мережевий моніторинг охоплює широкий спектр пристроїв, включаючи сервери, маршрутизатори, комутатори і навіть кінцеві точки. Його також можна використовувати в будь-якій мережі, включаючи бездротові локальні мережі, локальні мережі, VPN і глобальні мережі [1].

Цей інструмент мережевого моніторингу дозволяє здійснювати комплексне сканування та аналіз різних типів пристроїв і сервісів. Це досягається за рахунок використання різних типів протоколів, що працюють на різних рівнях OSI.

Моніторинг мережі використовується для вимірювання продуктивності всієї мережі. Це вимірюється шляхом порівняння кількості відправлених і отриманих пакетів. В процесі вимірюється кількість переходів (кількість проміжних пристроїв перед досягненням місця призначення). Також вимірюється поширення маршруту та затримка мережевих пристроїв. Таким чином, можна оцінити втрати пакетів, пропускну здатність і затримку. В результаті покращується якість мережевих послуг.

Ще одна важлива частина моніторингу - аналіз маршрутів. Це набір інструментів, методів і алгоритмів, які контролюють маршрутизацію в мережі. Він працює на рівні мережі. Аналіз маршрутів пасивно взаємодіє з протоколами маршрутизації OSPF, IS-IS, EIGRP і BGP і контролює їх. Як результат, він отримує всі повідомлення про оновлення так само, як і інші маршрутизатори. Він також використовує алгоритм Дейкстри для обчислення повної карти топології мережі, включаючи всі шляхи. Крім того, записується повна історія подій маршрутизації, яка може бути використана для усунення несправностей. В цілому, аналіз маршрутів покращує швидкість і ефективність роботи мережі, знижуючи витрати і підвищуючи продуктивність співробітників [2].

Website Motoring забезпечує моніторинг стану сервера. Він вимірює доступність сервера, продуктивність, підключення, час безвідмовної роботи, записи DNS, пропускну здатність і навіть апаратні ресурси. Існує два типи моніторингу веб-сайтів: внутрішній і зовнішній. Внутрішній моніторинг (всередині

корпоративного брандмауера) слугує для виявлення проблем внутрішньої інфраструктури та розробки додатків. Зовнішній моніторинг (поза корпоративним брандмауером) відповідає за наскрізний моніторинг. Моніторинг веб-сайтів відповідає за такі інтернет-протоколи: http, https, ftp, snmp, stpm, ssh, telnet, pop3, dns, ssl, tcp, udp.

Моніторинг з точки зору кінцевого користувача означає, що робот регулярно імітує поведінку користувача. Він виконує користувацькі скрипти так, ніби користувач здійснює навігацію та натискає на меню. Якщо робот не може виконати дію, то і кінцевий користувач не зможе. Нещодавно було додано відстеження на рівні коду. Це особливо актуально для J2EE та .NET додатків. Такі модулі можуть виявляти затримки системних викликів, витоки пам'яті та затримки виконання SQL-запитів [2].

Наразі на ринку існує два типи програмного забезпечення для моніторингу: Перший - це інструменти моніторингу з відкритим вихідним кодом. Зазвичай такі системи випускаються під ліцензією GPLv2. Таким чином, стороннім розробникам дозволяється вносити зміни на рівні коду. Ліцензія обмежує зміни на рівні коду.

Я вважаю, що мережевий моніторинг з відкритим вихідним кодом має багато переваг над пропрієтарними системами. Я думаю, що кінцеві користувачі отримують вигоду від багатьох функцій, які пропонують системи з відкритим вихідним кодом.

Провайдери мережевого моніторингу намагаються включити найкращі функції для моніторингу, але практично неможливо створити єдине рішення, яке б підходило для всіх мереж. Різні мережі мають різні потреби. Саме тут можуть допомогти інструменти моніторингу з відкритим вихідним кодом. Якщо функції моніторингу мережі не включені в готові продукти, вони можуть бути створені мережевими адміністраторами з достатніми навичками і знаннями або завантажені зі спільноти.

Компанії, які пропонують свої продукти з відкритим вихідним кодом, також можуть отримати вигоду від цього, оскільки вони можуть відчути ефект краудсорсингу.

Якщо незалежні розробники створюють доповнення або додаткові функції, найпопулярніші з них можуть бути додані до наступної версії продукту. Це забезпечує додаткову гнучкість і дозволяє компаніям йти в ногу з тенденціями моніторингу мереж. Загалом, інструменти мережевого моніторингу з відкритим вихідним кодом приносять значні переваги моніторингу мережі і допомагають розширити деякі функції, які не пропонуються постачальником [3].

Моніторинг на основі агентів складається з програмного забезпечення, яке називається агентами. Агенти - це програми, які встановлюються локально на сервери та інші мережеві пристрої. Їхнє призначення - відстежувати продуктивність мережі. Якщо виникає помилка, генерується попереджувальне повідомлення. Крім того, агент може також виправляти деякі помилки.

Агенти - це легкі програми. Однак деякі з них споживають багато мережевих ресурсів. В результаті використання мережевого моніторингу втрачає свою важливість. З цієї причини все більшої популярності набувають легкі агенти, так звані "невидимі" агенти. Їх головна перевага перед традиційними агентами полягає в тому, що вони не мають жодного з недоліків моніторингу продуктивності і не залишають слідів роботи мережі.

Основна перевага моніторингу на основі агентів полягає в тому, що він забезпечує більш глибокий аналіз мережі. Крім того, інструменти моніторингу на основі агентів можуть також діагностувати продуктивність обладнання. Вони також надають функції попередження та звітності. Деякі помилки вирішуються автоматично.

Основним недоліком є те, що налаштування такої системи займає багато часу і потрібно враховувати багато мережевих деталей. Крім того, агенти потребують оновлення. Традиційні рішення на основі агентів можуть впливати на продуктивність мережі. Слід також зазначити, що ліцензійні платежі на агентські інструменти моніторингу досить дорогі.

Безагентні рішення не вимагають встановлення окремого агента. Аналіз мережі базується на прямому відстеженні пакетів. Він використовується для

моніторингу доступності та продуктивності мережі. Однак він не надає детальної інформації про збої.

Моніторинг без агентів зазвичай базується на SNMP (Simple Network Monitoring Protocol) або WMI (Windows Management Instrumentation). Він покладається на центральну станцію управління, яка контролює всі інші мережеві пристрої. Однак рішення на основі агентів забезпечують більш детальні вимірювання.

Основна перевага безагентного моніторингу полягає в тому, що агенти не потрібні. Це не впливає на продуктивність мережі. Процес розгортання також простіший. Крім того, агенти не потребують регулярного оновлення. Основним недоліком безагентного моніторингу є відсутність детальних метрик. Крім того, безагентний режим не надає можливостей звітування та аналізу [3].

Агентний моніторинг рекомендується для великих мереж зі складною інфраструктурою. У разі збою інструменти агентного моніторингу сповіщають вас про збій. Вони також намагаються вирішити проблему автоматично. Якщо несправність не є тривіальною, адміністратор мережі повинен втрутитися. Інструменти моніторингу на основі агентів надають детальну інформацію про те, де і як виникла проблема. Це скорочує час, витрачений на усунення несправностей.

Моніторинг без агентів підходить для невеликих мереж з невеликою кількістю мережевих пристроїв. Все, що потрібно - це доступність і продуктивність мережі. Такі мережі не потребують метрик або детальної інформації про мережеві пристрої.

Рекомендується використовувати як агентний, так і безагентний моніторинг мережі. В даний час такі постачальники, як Nagios і Zabbix, пропонують як агентські, так і безагентські можливості в своїх рішеннях. Моніторинг на основі агентів можна використовувати в основних частинах мережі, де доступність і продуктивність є пріоритетами. Режим без агентів більше підходить для менш критичних частин мережі.

1.2 Основні загрози та ризики для критичної інфраструктури

Основні загрози та ризики для критичної інфраструктури можуть бути дуже різноманітними та включати такі аспекти, як кібератаки, техногенні аварії, природні катастрофи та інші небезпеки. Важливість безперервного моніторингу загроз полягає в здатності оперативно виявляти, аналізувати та реагувати на потенційні небезпеки, що можуть негативно вплинути на роботу критичної інфраструктури.

Кібератаки можуть включати в себе різноманітні методи, такі як DDoS-атаки, введення зловмисного коду, фішинг та інші, спрямовані на відключення або порушення роботи систем. Техногенні аварії, такі як витоки газу, аварії на транспорті чи вибухи, можуть призвести до фізичного пошкодження інфраструктури та інших серйозних наслідків.

DDoS-атака (розподілений збій обслуговування) - це вид кібератаки, призначений для перекриття доступу до онлайн-сервісу, мережі або веб-сайту, шляхом перевантаження їх серверів або мережевих ресурсів великою кількістю запитів. Ось декілька ключових характеристик DDoS-атак:

1. Розподіленість на відміну від звичайних DoS-атак, де один зловмисник відправляє запити з одного джерела, DDoS-атака використовує розподілену мережу комп'ютерів або ботнет, що робить атаку складніше виявити та протистояти.
2. Великий обсяг трафіку, атака спрямована на перевантаження мережі або сервера шляхом надмірної кількості запитів. Це може бути UDP, TCP або HTTP-трафік, залежно від типу атаки.
3. Масштабність, DDoS-атаки можуть мати величезний масштаб із використанням тисяч або навіть мільйонів ботнет-пристроїв, що робить їх надзвичайно ефективними та складними для захисту.
4. Замаскованість, зловмисники можуть приховати свою ідентичність та місцезнаходження, використовуючи анонімні або скомпрометовані пристрої для запуску атаки, що робить їх важкими для виявлення та припинення.

5. Закритість ресурсів, одним з основних наслідків DDoS-атак є перекриття доступу до веб-сайту або онлайн-сервісу для законних користувачів, що може призвести до втрати бізнесу, репутаційних збитків та фінансових втрат [4].

Кібератака введення зловмисного коду (віруси, черв'яки, троянські коні, шкідливі програми) - це процес введення в широке використання шкідливих програм чи коду з метою нанесення шкоди комп'ютерним системам, мережам чи даним. Ось декілька основних характеристик цієї категорії кібератак:

1. Розповсюдження через вразливості, шкідливий код може використовувати вразливості в програмному забезпеченні або операційних системах для введення у систему.

2. Саморозповсюдження, деякі види шкідливого коду, такі як черв'яки, можуть самостійно розповсюджуватися по мережі, використовуючи вразливості у системах для введення свого копіюючогося коду.

3. Руйнівні наслідки, введення зловмисного коду може мати різні наслідки, включаючи втрату даних, пошкодження програмного забезпечення, викрадення конфіденційної інформації, а також заморожування або блокування роботи системи.

4. Крадіжка ідентифікаційних даних, деякі види шкідливого коду, такі як троянські коні, спрямовані на крадіжку ідентифікаційних даних, таких як паролі, логіни, номери кредитних карток тощо.

5. Крипто-шахрайство, останнім часом, шкідливий код також використовується для криптографічного шахрайства, коли він захоплює ресурси комп'ютера, щоб видобувати криптовалюту, таку як Bitcoin [4].

Фішингові атаки - це вид кібератак, які спрямовані на використання соціальної інженерії для шахрайського отримання конфіденційної інформації, такої як паролі, ідентифікаційні дані, номери кредитних карток тощо. Ось деякі характеристики фішингових атак:

1. Соціальна інженерія, фішингові атаки зазвичай використовують техніки соціальної інженерії, щоб обманом викликати у потенційної жертви довіру

або підставити її для отримання конфіденційної інформації.

2. Використання підроблених повідомлень, атаки можуть включати відправку підроблених електронних листів, повідомлень в мережах соціальних медіа або SMS-повідомлень, що пропонують ланцюжок дій, які зазвичай включають переход на підроблений веб-сайт або введення конфіденційної інформації.

3. Шахрайські веб-сайти, шахраї створюють підроблені веб-сайти, що імітують легітимні веб-сайти, такі як банки, платіжні системи або соціальні мережі, для того щоб викликати у жертв довіру та отримати їхні ідентифікаційні дані.

4. Спам, фішингові атаки також можуть включати відправку масових спам-повідомлень з ланцюжками фішингових веб-сайтів або прямих запитів на введення конфіденційної інформації.

5. Подвоєння ідентичності, деякі атаки можуть включати використання викрадених ідентифікаційних даних для отримання несанкціонованого доступу до різних сервісів або для вчинення злочинних дій в ім'я жертви.

Для захисту від фішингових атак важливо навчити користувачів розпізнавати підозрілі повідомлення та веб-сайти, використовувати механізми двофакторної аутентифікації та обережно поводитися з конфіденційною інформацією в інтернеті. Також ефективним заходом захисту є використання антивірусного програмного забезпечення, яке може розпізнавати та блокувати шкідливі веб-сайти та файли [5].

Безперервний моніторинг загроз дозволяє вчасно виявляти вразливості та потенційні загрози, здійснювати аналіз їхнього впливу та приймати необхідні заходи для захисту критичної інфраструктури. Такий моніторинг дозволяє забезпечити неперервну та надійну роботу систем, запобігаючи можливим негативним наслідкам для безпеки та ефективності інфраструктури.

1. Система моніторингу Zabbix може допомогти виявляти та реагувати на кібератаки різних типів, включаючи фішинг, введення зловмисного коду та DDoS-атаки, за допомогою наступних функцій:

2. Моніторинг системи та мережі, Zabbix надає можливість моніторингу різних параметрів системи та мережі, таких як використання ресурсів, пропускна

здатність мережі, активність користувачів тощо. За допомогою цих функцій можна виявити аномальну активність, яка може бути ознакою кібератак.

3. Сповіщення про відхилення, Zabbix може налаштовувати сповіщення про відхилення від нормального стану системи або мережі. Наприклад, при підозрілій активності або перевищенні допустимих значень, система може автоматично сповістити адміністратора про потенційну кібератаку.

4. Моніторинг безпеки, Zabbix може інтегруватися з системами безпеки та іншими інструментами моніторингу безпеки для виявлення підозрілої активності, такої як атаки фішингу, спроби введення зловмисного коду або DDoS-атаки. Це дозволяє оперативно реагувати на потенційні загрози та вживати відповідних заходів захисту.

5. Аналіз логів, Zabbix може збирати, аналізувати та відстежувати логи подій системи та мережі. Це дозволяє виявляти незвичайну активність, а також аналізувати попередні атаки та прийоми, щоб уникнути їх у майбутньому.

Швидка реакція Zabbix дозволяє автоматизувати реакцію на кібератаки шляхом виконання попередньо налаштованих дій при виявленні певних умов або подій. Наприклад, при виявленні DDoS-атаки система може автоматично активувати захисні фільтри або сповістити відповідні служби безпеки.

1.3 Аудит інформаційної безпеки

Аудит інформаційної безпеки - це систематичний процес перевірки та оцінки заходів безпеки, що застосовуються в інформаційних системах та інфраструктурі організації. Його основна мета полягає в ідентифікації потенційних загроз, вразливостей та ризиків для безпеки інформації, а також у визначенні ефективності та відповідності заходів безпеки стандартам та вимогам.

Під час аудиту інформаційної безпеки проводяться такі дії:

1. Аналіз систем безпеки, оцінка технічних та організаційних заходів безпеки, таких як захист мережі, доступ до даних, управління правами доступу, політики безпеки тощо.

2. Перевірка відповідності стандартам, перевірка того, чи відповідають заходи безпеки вимогам і стандартам, таким як ISO 27001, HIPAA, GDPR тощо.

3. Ідентифікація ризиків, визначення потенційних загроз безпеці та визначення рівня ризику для організації.

4. Розробка рекомендацій, висунення рекомендацій щодо вдосконалення систем безпеки та зменшення виявлених ризиків.

5. Проведення тестування, виконання тестування на проникнення та інших видів тестування безпеки для перевірки вразливостей систем [6].

Аудит інформаційної безпеки є важливою складовою для забезпечення надійності, цілісності та конфіденційності інформації, що зберігається та обробляється в організації.

Дані аудиту - це всі інформаційні дані, які збираються, аналізуються та використовуються під час проведення аудиторської перевірки інформаційної безпеки організації. Ці дані включають в себе різноманітну інформацію про стан безпеки, відомості про системи, процедури та практики безпеки, а також результати аналізу та оцінки безпеки інформаційних систем.

Мета проведення аудиту інформаційної безпеки полягає у забезпеченні надійності, цілісності та конфіденційності інформації та інформаційних систем в організації. Основні цілі аудиту включають:

1. Виявлення потенційних загроз та вразливостей, аудиторська перевірка допомагає ідентифікувати ризики безпеки, такі як вразливості програмного забезпечення, недостатні контрольні механізми доступу та потенційні точки вторгнення, які можуть бути використані зловмисниками.

2. Оцінка ефективності заходів безпеки, аудит дозволяє оцінити, наскільки ефективні та відповідні заходи безпеки, які застосовуються в організації, і визначити, чи вони відповідають стандартам безпеки та вимогам законодавства.

3. Забезпечення відповідності, аудит допомагає перевірити, чи відповідають дії та процеси організації вимогам внутрішніх політик безпеки, міжнародних стандартів (наприклад, ISO 27001) та регуляторних вимог (наприклад, GDPR, HIPAA).

4. Виявлення слабких місць, аудиторська перевірка допомагає виявити слабкі місця в інформаційних системах та процесах безпеки, що може допомогти організації підвищити свій рівень захисту та підготуватися до можливих загроз.

5. Надання рекомендацій, на основі результатів аудиту можуть бути надані рекомендації щодо покращення систем безпеки та запобігання можливим інцидентам безпеки [7].

Види аудиту інформаційної безпеки:

1. Експертні аудити безпеки: проводяться експертами, призначеними для оцінки та виявлення недоліків у системі безпеки.

2. Активні аудити: оперативні аудити, основною метою яких є виявлення підозрілої поведінки та автоматичне вжиття заходів. Підозріла поведінка включає в себе порушення користувачами політик інформаційної безпеки, нетипову поведінку по відношенню до системи та підозрілу поведінку.

3. Аудит ІБ - перевіряє відповідність міжнародним стандартам;

4. Комплексний аудит - охоплює всі перераховані вище варіанти діагностики.

Таким чином, організації, яким необхідно забезпечити інформаційну безпеку своїх інформаційних систем, повинні вирішити питання оповіщення, виявлення та реєстрації системних подій. Це необхідно як для забезпечення можливості проведення аудиту ІБ, так і для швидкого реагування на інциденти інформаційної безпеки.

Для обробки системних подій в IT-інфраструктурах часто використовують системи моніторингу, які відстежують події для критично важливих компонентів. Які саме події слід відстежувати, має бути формалізовано в політиці інформаційної безпеки організації, залежно від особливостей IT-інфраструктури та бізнес-процесів організації [7].

Розділ 2 ОГЛЯД ПОНЯТЬ ТА ТЕРМІНІВ В ГАЛУЗІ КІБЕРБЕЗПЕКИ

2.1 Налаштування політики аудиту

Аудит безпеки Windows - це процес систематичної перевірки та аналізу конфігурації, активності та подій, що відбуваються в операційній системі Windows, з метою виявлення потенційних загроз безпеці та вразливостей. Основні аспекти аудиту безпеки Windows включають:

1. Моніторинг подій, системи Windows зберігають велику кількість подій, пов'язаних з безпекою, такі як входи в систему, спроби доступу до файлів, запуск програм тощо. Аудитори аналізують ці події для виявлення незвичайних або підозрілих дій, які можуть свідчити про атаки або порушення безпеки.

2. Перевірка конфігурації, аудитори перевіряють налаштування системи Windows, такі як політики безпеки, права доступу, файли журналів подій, файли реєстру тощо, для виявлення вразливостей та можливих шляхів атаки.

3. Аналіз доступу, аудитори перевіряють права доступу до файлів, ресурсів та мережевих служб, щоб впевнитися, що доступ до конфіденційної інформації обмежений лише авторизованим користувачам.

4. Виявлення зловмисного програмного забезпечення, шляхом аналізу активності процесів та виявлення підозрілих файлів, аудитори намагаються виявити наявність шкідливого програмного забезпечення, такого як віруси, троянські програми або шпигунське ПЗ.

5. Рекомендації щодо покращення безпеки на основі результатів аудиту безпеки Windows аудитори надають рекомендації щодо усунення виявлених вразливостей та покращення безпеки системи.

Аудит безпеки Windows відіграє ключову роль у забезпеченні безпеки та захисту інформаційних систем на базі операційної системи Windows.

Контроль безпеки - один з найпотужніших інструментів Windows для захисту цілісності системи Контроль безпеки Windows можна ввімкнути за допомогою групової політики (середовище Active Directory) або локальної політики безпеки

(окремі комп'ютери). Відкрийте Панель керування Windows, натисніть Керування і виберіть Локальна політика безпеки. Перейдіть на вкладку Локальні політики і натисніть Політики аудиту. У правій частині вікна Локальна політика безпеки з'явиться список політик аудиту (рис. 2.1).

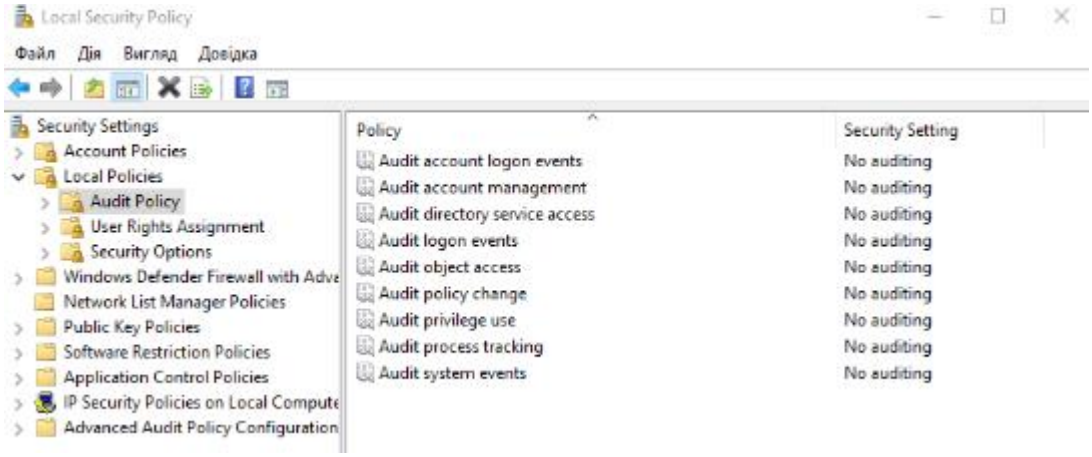


Рис. 2.1 – Налаштування політики аудиту

Політика аудиту повинна розглядатися як частина загальної стратегії безпеки, а рівень аудиту повинен визначатися для кожного середовища окремо. Аудит повинен виявляти атаки (успішні або неуспішні), які становлять загрозу для IT-інфраструктури, а також атаки на ресурси, визначені як цінні під час оцінки ризиків [8].

Налаштування політики аудиту визначають, які події слід реєструвати. У цьому розділі описано розширені параметри політики аудиту безпеки, доступні для Windows Server 2008 R2, Windows 7 і пізніших версій операційних систем Windows, а також показано, як вони працюють.

Загалом 53 параметри політики аудиту безпеки дають змогу гарантувати, що ваша організація дотримується критично важливих для бізнесу та безпеки політик, виконуючи точно визначені дії.

Адміністратори групи змінили налаштування сервера або дані.

Певна група співробітників отримала доступ до критично важливих файлів.

Застосування точних списків контролю доступу до системи (SACL) до всіх файлів, папок і ключів реєстру на комп'ютері забезпечує надійний захист від несанкціонованого доступу.

Крім того, політики аудиту безпеки Windows 7 і Windows Server 2008 R2 можна застосовувати за допомогою доменних і групових політик, що дозволяє відносно легко змінювати, тестувати і розгортати параметри політики аудиту для вибраних користувачів і груп [9].

2.2 Основні переваги, функції та архітектура Zabbix

Zabbix - це інструмент моніторингу мережі, який централізовано контролює доступність і продуктивність мереж і мережевих пристроїв. У разі збою мережеві адміністратори отримують сповіщення по телефону або електронною поштою. Zabbix - це абсолютно безкоштовний інструмент моніторингу мережі, випущений під ліцензією GPLv2. Кількість функцій або пристроїв, що підлягають моніторингу, не обмежена. Зміни на рівні вихідного коду також офіційно дозволені. Крім того, Zabbix підтримує розгортання всіх розмірів, від невеликих мереж до архітектур корпоративного рівня, а команда Zabbix регулярно випускає поліпшення і оновлення [10].

Zabbix була заснована в 1998 році і була корпоративним проектом Олексія Владишева. На той час він працював системним адміністратором у банку. Він відповідав за адміністрування баз даних. Для автоматизації рутинних завдань Владишев створив перший прототип Zabbix на основі скриптів на мові Perl.

У той час на ринку було лише два гравці: HP Open View та IBM BMC, але ці рішення були дуже дорогими і складними в обслуговуванні та налаштуванні. Nagios, перший загальнодоступний інструмент моніторингу мережі з відкритим вихідним кодом, був випущений в 1999 році.

Знадобилося три роки, щоб випустити першу публічну версію Zabbix. Це була Zabbix v1.0 Alpha 1, випущена під Загальною публічною ліцензією (GPL) у

2001 році; у 2004 році Zabbix v1 була випущена як перша версія з довгостроковою підтримкою (LTS).

Zabbix підтримує моніторинг мережевих пристроїв, таких як маршрутизатори, комутатори та сервери, як на основі агентів, так і без них. Мережеве обладнання повинно підтримувати SNMP; Zabbix може контролювати доступність і продуктивність обладнання. Крім того, Zabbix підтримує моніторинг VMware. Це використовується для моніторингу статистики віртуальних машин. Низькорівневі правила виявлення використовуються для виявлення віртуальних машин і гіпервізорів. Крім того, Zabbix може моніторити бази даних і веб-сервіси [11].

Якщо мережа або пристрій виходить з ладу, Zabbix повинен повідомити про це системного адміністратора; Zabbix підтримує низькорівневе виявлення мережевих пристроїв і дозволяє їх логічно групувати. Однак, Zabbix не має функції відстеження тенденцій. Тому Zabbix не може забезпечити завчасне попередження про можливі збої. Однак команда Zabbix оголосила, що в даний час вони працюють над інтеграцією прогнозування тенденцій в архітектуру Zabbix.

Zabbix складається з наступних компонентів: Zabbix Server, Zabbix Proxy, Zabbix Agent та веб-інтерфейс. Кожен з них відіграє певну роль у моніторингу. У цьому розділі описано ці компоненти. На рисунку 2.2 показано огляд архітектури Zabbix, включаючи всі компоненти.

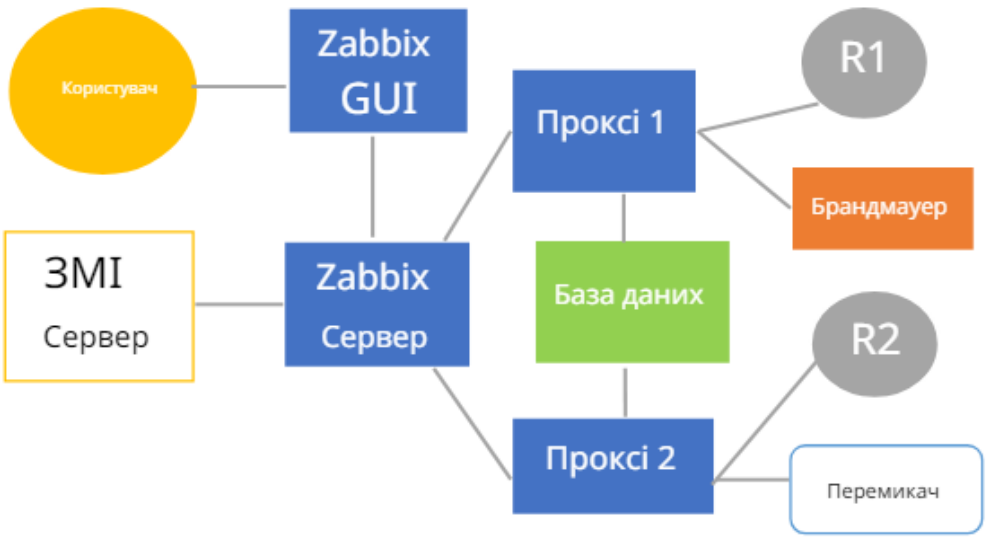


Рис. 2.2 – Компоненти Zabbix

Сервер Zabbix є ядром Zabbix і його основним призначенням є віддалений моніторинг самої мережі та її компонентів. Він також зберігає конфігураційні, історичні та операційні дані. У разі виникнення помилок, Zabbix Server повідомляє про це адміністратора мережі.

Zabbix Proxy збирає дані про продуктивність від імені Zabbix Server. На локальному рівні всі дані збираються в буфер, який перенаправляється на Zabbix Server. Проксі - це рішення для централізованого віддаленого моніторингу мережі. Також проксі розподіляє навантаження на сервер Zabbix. В результаті, це зменшує обчислювальну потужність, процесор і пам'ять вводу/виводу сервера Zabbix.

Zabbix Agent виконує локальний моніторинг мережевих пристроїв; Zabbix Agent відстежує такі ресурси, як жорсткий диск, пам'ять і статистику процесора. Для моніторингу ресурсів Zabbix Agent необхідно встановити локально на кожному пристрої, що дуже ефективно, оскільки Zabbix Agent виконує власні системні виклики. Zabbix Agent призначений для збору статистичних даних.

Веб-інтерфейс є частиною Zabbix Server. Веб-інтерфейс зазвичай працює на тому ж фізичному сервері, що і сервер Zabbix; веб-інтерфейс не є традиційним користувацьким інтерфейсом. Всі операції читання/запису оминають сервер Zabbix і надсилаються до бази даних. Це значно підвищує продуктивність Zabbix. З іншого боку, Zabbix Server не може працювати без веб-інтерфейсу [12].

На рисунку 2.2 показано два додаткові компоненти, які не входять до складу Zabbix. Однак вони відіграють важливу роль у моніторингу мережі. Це медіа-сервер і база даних. Медіа-сервер відповідає за надсилання сповіщень електронною поштою та SMS, а база даних використовується для зберігання конфігурації та історичних даних.

Загалом, поєднання цих компонентів дозволяє Zabbix підтримувати три типи моніторингу: Простий контроль, Zabbix Agent та Зовнішній контроль. Прості засоби контролю перевіряють доступність різних сервісів, таких як SMTP і HTTP, без додаткового встановлення на хост, Агенти Zabbix контролюють використання обладнання локально, а Зовнішні засоби контролю перевіряють доступність сервісів, таких як IPMI, SSH і HTTP, без додаткового встановлення на хост, HTTP

та інших сервісів без додаткового встановлення на хост. Зовнішній контроль забезпечує віддалений моніторинг за допомогою SNMP, TCP і ICMP через IPMI, SSH і Telnet.

Також можливий моніторинг хостів без проксі-сервера. В цьому випадку всі дані моніторингу з хоста збираються безпосередньо сервером Zabbix. Крім того, на одній машині можна встановити графічний інтерфейс Zabbix, Zabbix-сервер, медіа-сервер і базу даних. Цей спосіб необхідний для малих і середніх мереж.

Zabbix відповідає вимогам надійного інструменту моніторингу мережі. Він забезпечує як агентний, так і безагентний моніторинг. Доступні такі функції, як рівні виявлення, автоматичне виявлення і логічне групування. Всі перераховані вище функції роблять Zabbix надійним інструментом моніторингу мережі, який повністю відповідає вимогам мереж будь-якого розміру. Однак, Zabbix не підтримує прогнозування тенденцій. Ця функція не була включена командою розробників Zabbix, оскільки вона погіршує загальну продуктивність [13].

Zabbix - це надійний і прогностичний інструмент моніторингу мережі: Якщо Zabbix повідомляє користувача про збій, користувач може бути на 100% впевнений, що проблема існує. Ті ж принципи надійності застосовуються до відновлення та візуалізації. Крім того, однією з головних переваг Zabbix є його масштабованість, яка може бути застосована до середовищ будь-якого розміру. Принцип масштабованості поширюється на продуктивність і простоту використання.

Однак можливості Zabbix не обмежуються IT. Як інструмент моніторингу мережі, Zabbix можна порівняти з мозком: Zabbix отримує вхідні дані з датчиків, цілочисельні значення, файли потоку нахилу та іншу необхідну інформацію. Тригери аналізують всі ці дані. Коли тригер генерує вихідний сигнал, результати можуть змінюватися. Це може бути сповіщення або команда, яка запускає мак-адресу пристрою, температуру процесора або сценарій руху транспортного засобу [14].

2.3 Аналіз існуючих систем аналогів безперервного моніторингу загроз

Nagios (рис. 2.3) - це відкрите програмне забезпечення для моніторингу комп'ютерних систем, мережевих ресурсів та інфраструктури. В основі Nagios лежить ідея постійного моніторингу різних аспектів системи та автоматизованого сповіщення про виникнення проблем [15].

Рис. 2.3 – Офіційне лого компанії

Основні функції Nagios включають:

1. Моніторинг ресурсів, Nagios дозволяє налаштовувати моніторинг різних аспектів системи та мережі. Це включає в себе перевірку доступності серверів і сервісів, використання ресурсів (таких як процесор, оперативна пам'ять, дисковий простір), а також інші параметри, що визначають стан системи. Nagios може періодично запускати тести і перевіряти, чи відповідають значення цих параметрів заданим умовам.

2. Сповіщення про проблеми, у разі виявлення проблеми або перевищення заданих меж, Nagios автоматично відправляє сповіщення адміністраторам. Це може бути електронна пошта, SMS-повідомлення або повідомлення через месенджери. Це дозволяє адміністраторам оперативно реагувати на проблеми і приймати відповідні заходи.

3. Автоматизована реакція, на основі правил та налаштувань, Nagios може автоматично виконувати певні дії для відновлення працездатності системи або

сервісу. Наприклад, при виявленні відмови сервісу, Nagios може спробувати перезапустити його автоматично або запустити скрипт для відновлення роботи [16].

4. Графічний інтерфейс користувача, Nagios надає зручний веб-інтерфейс для відображення статусу моніторингу, роботи сервісів та системи в цілому. Користувачі можуть легко переглядати дані моніторингу, налаштовувати сповіщення та встановлювати правила для автоматизованої реакції на проблеми. Графіки та звіти допомагають адміністраторам аналізувати стан системи та приймати ефективні рішення для її підтримки.Nagios є потужним інструментом для забезпечення стабільності і безпеки комп'ютерних систем і мереж, а також для швидкого реагування на виникнення проблем.

ELK Stack - це платформа для збору, аналізу та візуалізації великих обсягів даних з різних джерел. ELK - це абревіатура, яка складається з трьох основних компонентів:

1. Elasticsearch:

– Elasticsearch - це розподілена система для зберігання, пошуку та аналізу даних в реальному часі. Вона базується на технології Apache Lucene і забезпечує швидкий та масштабований пошук великих обсягів структурованих та неструктурованих даних.

– Elasticsearch дозволяє зберігати дані у вигляді документів JSON і проводити складні пошукові операції, включаючи повнотекстовий пошук, географічний пошук, агрегації та фільтрації.

– Він підтримує розподілену архітектуру, що дозволяє масштабувати його горизонтально для обробки великих обсягів даних та забезпечення високої доступності.

2. Logstash:

– Logstash - це інструмент для обробки, нормалізації та індексації різноманітних джерел даних перед їхнім збереженням в Elasticsearch. Він дозволяє збирати дані з різних джерел, таких як журнальні файли, бази даних, мережеві протоколи тощо, та структурувати їх для подальшого аналізу.

– Logstash використовує конфігураційні файли для налаштування різних входів, фільтрів та виходів для обробки даних. Він може перетворювати дані у формат JSON, розбивати їх на окремі поля, видаляти непотрібну інформацію та багато іншого

3. Kibana:

– Kibana - це інтерактивний веб-інтерфейс для візуалізації та аналізу даних, що зберігаються в Elasticsearch. Він дозволяє користувачам створювати різноманітні графіки, діаграми, таблиці та інші візуалізації для аналізу даних в реальному часі.

– Крім того, Kibana надає можливість створювати і відслідковувати розширені запити, створювати та виконувати звіти, налаштовувати сповіщення та алерти для моніторингу даних. Він також має інтуїтивно зрозумілий інтерфейс для управління та налаштування всіх компонентів ELK Stack [17].

ELK Stack використовується для моніторингу, аналізу логів, відстеження метрик продуктивності, виявлення аномалій та багатьох інших сценаріїв аналізу даних. Він широко використовується в області моніторингу систем, аналізу безпеки, моніторингу додатків та інших галузях для відстеження та аналізу подій та великих обсягів даних. На рисунку 2.4 показана стекова архітектура ELK Stack [18].

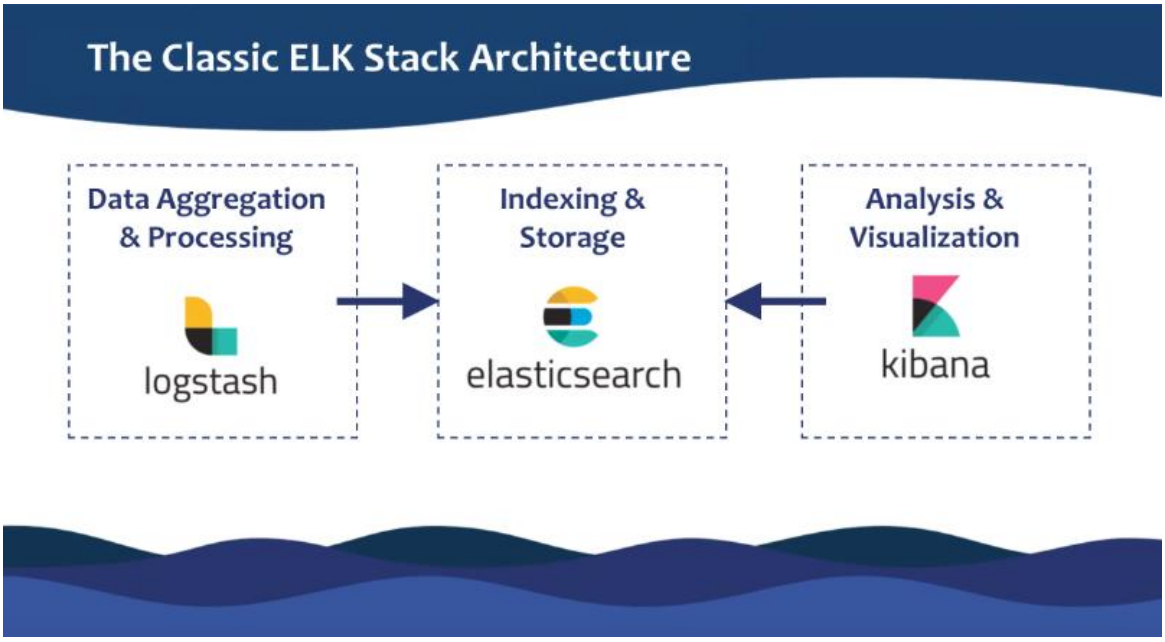


Рис. 2.4 – Стекова архітектура ELK

Graylog (рис. 2.5)- це відкрите програмне забезпечення для збору, аналізу та візуалізації журнальних даних. Він дозволяє організаціям ефективно моніторити та аналізувати великі обсяги журнальних даних з різних джерел у реальному часі.

Рис. 2.5 – Офіційне лого компанії Graylog

Основні компоненти Graylog включають в себе:

1. Система збору даних (Input):

– Graylog надає різноманітні інтерфейси для збору журнальних даних з різних джерел. Це може бути логи систем, мережеві пристрої, додатки, веб-сервери, додатки в хмарних сервісах тощо.

– Він підтримує стандартні протоколи збору даних, такі як syslog, а також дозволяє налаштовувати власні протоколи інтеграції.

2. Система обробки (Processing):

– Після збору даних Graylog дозволяє застосовувати різні фільтри та правила обробки для нормалізації та структурування даних. Це може включати видалення непотрібної інформації, розподіл даних на поля, конвертацію форматів даних тощо.

– Фільтри дозволяють вам фокусуватися на конкретних типах подій або виключати непотрібні дані перед їхнім збереженням.

3. Система збереження (Storage):

– Дані, оброблені та відфільтровані Graylog, зберігаються у високоефективному сховищі даних на основі Elasticsearch. Це дозволяє швидко та ефективно виконувати пошук та аналіз великих обсягів журнальних даних.

– Elasticsearch використовується для забезпечення швидкого та ефективного пошуку, а також для відображення даних у реальному часі.

4. Інтерфейс користувача (User Interface):

– Graylog має зручний веб-інтерфейс, який надає користувачам доступ до всіх функцій та можливостей платформи. Цей інтерфейс дозволяє аналізувати дані, створювати візуалізації, налаштовувати моніторинг і сповіщення та багато іншого.

– Інтерфейс має інтуїтивно зрозумілий дизайн і дозволяє легко навігувати між різними сторінками та функціями [19].

5. Моніторинг та сповіщення (Monitoring & Alerts):

– Graylog дозволяє налаштовувати моніторинг різних параметрів системи та налаштовувати сповіщення в разі виявлення проблем або важливих подій.

– Користувачі можуть налаштовувати різноманітні типи сповіщень, включаючи електронні листи, повідомлення через Slack або інші канали зв'язку.

Розділ 3 РОЗРОБЛЕННЯ СИСТЕМИ РЕАЛІЗАЦІЇ МОНІТОРИНГУ НА БАЗІ ZABBIX

Після аналізу вимог до реєстрації подій на об'єктах критичної інфраструктури, встановлених у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури", було сформовано список аудитів подій. Ці аудити мають бути проведені системою моніторингу незалежно від архітектури IT-інфраструктури та політики безпеки організації. Їх завдання полягає у виявленні потенційних загроз безпеці, а також незвичайної чи підозрілої активності в інформаційних системах критичних об'єктів. Такий підхід допомагає запобігти можливим інцидентам та забезпечити надійний захист критичних інфраструктурних об'єктів [20].

– Аудит управління обліковими записами – означає відстеження усіх дій, пов'язаних з обліковими записами користувачів в системі. Це включає створення, редагування, видалення облікових записів, а також надання або скасування прав доступу.

– Аудит доступу до об’єктів файлової системи – полягає в моніторингу всіх спроб доступу до файлів та папок в системі. Він відстежує, хто намагається отримати доступ, які файли вони намагаються відкрити або змінити, і чи успішно вони це роблять.

– Аудит цілісності системи –перевірка цілісності всіх компонентів системи, щоб виявити будь-які зміни або втручання, які можуть вказувати на потенційні атаки або інші проблеми безпеки. Це може включати перевірку хеш-сум файлів, контроль цілісності конфігураційних файлів тощо.

Загалом, ці аудити допомагають організаціям виявляти та реагувати на потенційні загрози та порушення безпеки в їх інформаційних системах, що є критичним для забезпечення безпеки об'єктів критичної інфраструктури.

3.1. Аудит управління обліковими записами

Для того, щоб система Windows фіксувала події входу/виходу користувачів у журналі подій, необхідно увімкнути відповідні параметри аудиту системи (рис. 3.1):

Audit Credential Validation визначає, чи генерує операційна система події аудиту для облікових даних, що передаються при запиті входу до облікового запису користувача. Ці події виникають на комп'ютері, який є авторитетним для облікових даних (для локальних облікових записів локальний комп'ютер є авторитетним). Аудит Credential Validation є важливим засобом контролю за безпекою, оскільки дозволяє виявляти та реагувати на спроби несанкціонованого доступу до облікових даних користувачів. Відстеження цих подій допомагає ідентифікувати можливі загрози та вживати відповідних заходів забезпечення безпеки для запобігання несанкціонованому доступу та витоку конфіденційної інформації [21].

Audit Kerberos Authentication Service визначає, чи потрібно генерувати події автентифікації для запитів щодо надання квитків автентифікації Kerberos (TGT). Якщо ви налаштуєте цей параметр політики, подія аудиту генерується після кожного запиту TGT автентифікації Kerberos (рис. 3.2). Події аудиту дозволяють відстежувати як успішні, так і невдали спроби автентифікації. Аудит успіху реєструється для кожної успішної спроби автентифікації, тоді як аудит невдачі фіксує невдалі спроби. Це допомагає виявляти та реагувати на спроби несанкціонованого доступу через Kerberos, забезпечуючи ефективний контроль за безпекою мережі [22].

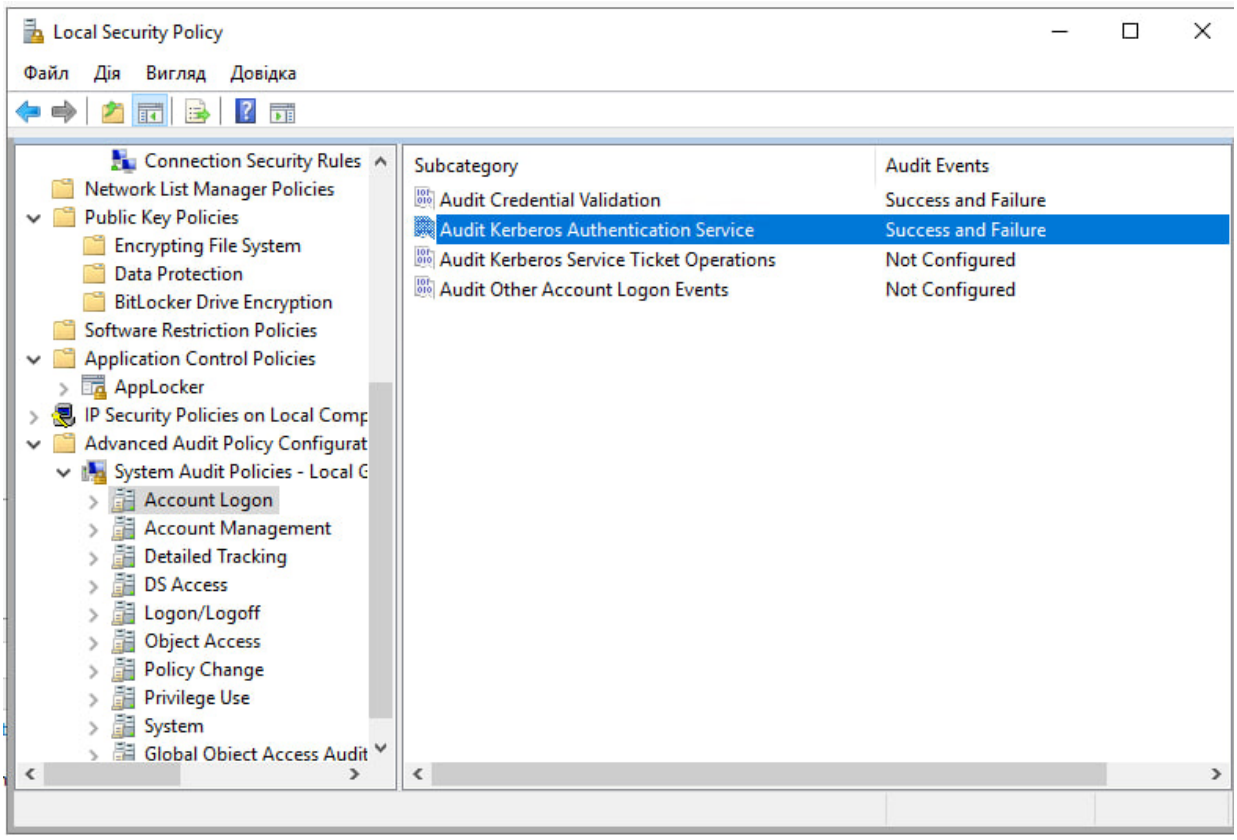


Рис. 3.1 — Політики аудиту для реєстрації подій входу/виходу облікових записів користувачів

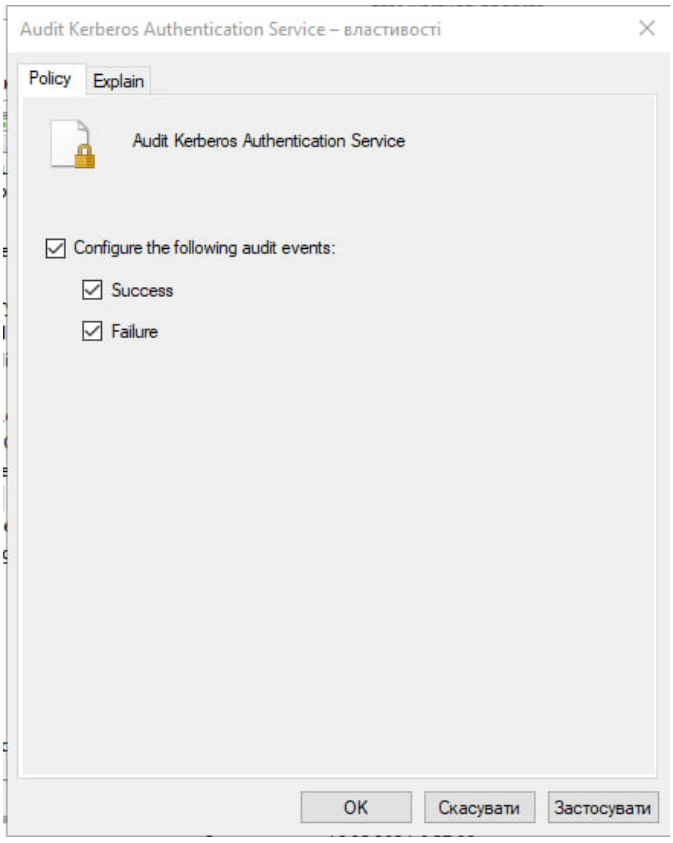


Рис. 3.2 — Конфігурація параметру для реєстрації подій входу/виходу ОЗК

Для належного ведення журналу подій, пов'язаних з видаленням, блокуванням та створенням облікових записів користувачів, важливо активувати дві категорії аудиту: Audit Computer Account Management та Audit User Account Management (як показано на рисунку 3.3). Audit Computer Account Management відповідає за те, щоб операційна система реєструвала події, пов'язані зі створенням, зміною чи видаленням облікового запису комп'ютера. Ця політика аудиту є важливою для відслідковування будь-яких змін, що відбуваються з обліковими записами на комп'ютерах у домені.

Audit User Account Management, з свого боку, надає можливість перевіряти будь-які зміни в облікових записах користувачів. Під цю категорію подій потрапляють такі дії, як створення, зміна або видалення облікового запису користувача. Ця функція аудиту необхідна для забезпечення безпеки та відслідковування будь-яких змін, які можуть відбутися у списку облікових записів користувачів [23].

Активуючи обидві ці категорії аудиту, ви забезпечуєте собі повний контроль над обліковими записами як комп'ютерів, так і користувачів, що в свою чергу підвищує безпеку вашої системи та дає можливість вчасно реагувати на будь-які зміни або потенційні загрози.

Створення, зміна, видалення, перейменування, вимкнення, увімкнення, блокування або розблокування облікового запису користувача;

- Встановлення або зміна пароля облікового запису користувача;
- Додавання ідентифікатора безпеки (SID) до історії SID облікового запису користувача або відсутність такого додавання;
- Налаштування пароля режиму відновлення служб каталогів;
- Зміна дозволів для облікових записів адміністраторів;
- Перерахунок членства користувача в локальній групі;
- Створення або відновлення облікових даних диспетчера облікових даних.

Нижче описані eventID подій які мають реєструватися виконання аудиту облікових записів.

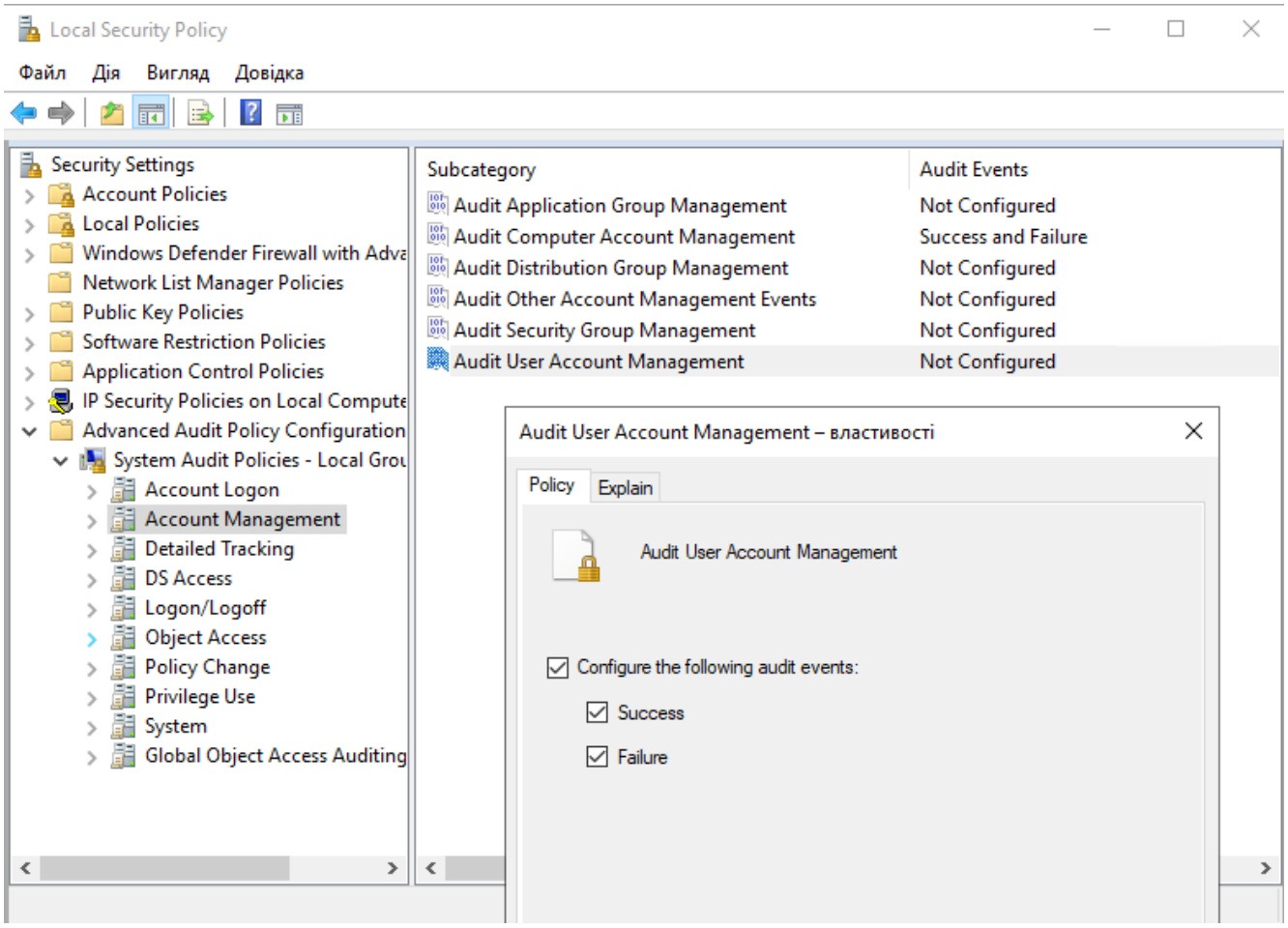


Рис. 3.3 — Політика аудиту для реєстрації подій видалення та створення облікових записів користувачів.

3.2. Аудит доступу до об’єктів файлової системи

Для ефективного контролю за доступом до об'єктів файлової системи необхідно включити аудиторський механізм, який буде реєструвати події, пов'язані з читанням, модифікацією, створенням або видаленням цих об'єктів (див. таблицю 3.1). Для цього активується параметр "Audit File System" (як показано на рисунку 3.4). Після активації цього параметра система аудиту буде генерувати події лише для тих об'єктів файлової системи, які мають налаштовані списки керування доступом до системи (SACL) [24].

Необхідно враховувати, що події аудиту будуть реєструватися тільки у випадку, якщо тип запитуваного доступу (наприклад, запис, читання чи зміна) та обліковий запис, що робить запит, відповідають параметрам, встановленим у

SACL. Це забезпечить деталізований аналіз та контроль за всіма діями, що відбуваються з об'єктами файлової системи, зменшуючи тим самим ризик несанкціонованого доступу та збільшуючи безпеку вашої інформаційної системи.

Список контролю доступу до системи (SACL) представляє собою важливий механізм для делегування подій, що визначає, як система перевіряє доступ до файлів і папок. Він не обмежує сам доступ до цих об'єктів, але використовується для встановлення загальносистемних політик безпеки, таких як ведення журналів або аудит доступу до ресурсів.

SACL закріплюється за системою, каталогом або файлом і визначає, які суб'єкти безпеки (користувачі, групи, комп'ютери) мають бути перевірені під час доступу до цього об'єкта. Крім того, він вказує, які події доступу мають бути зареєстровані для цих суб'єктів, включаючи створення записів про успішний чи неуспішний доступ відповідно до дозволів, встановлених у DACL (списку контролю доступу до файлів) [25].

Зазвичай список керування доступом налаштовується для критичних об'єктів файлової системи. Однак, хоча можна активувати політику аудиту файлової системи для всієї системи, це часто призводить до великої кількості подій, що значно збільшує навантаження на систему збереження та ведення журналів. Важливо уважно налаштувати цей механізм для забезпечення ефективного аудиту без зайвого навантаження.

Таблиця 3.1 Події роботи з файловою системою

ID	Опис події	
4656	Ідентифікує початок роботи з файлом	
4663	Ідентифікує виконану операцію над об’єктом	
4660	Ідентифікує операцію видалення	

Продовження Таблиці 3.1

4658	Ідентифікує кінець роботи з файлом	
4670	Режим контролю доступу було змінено	

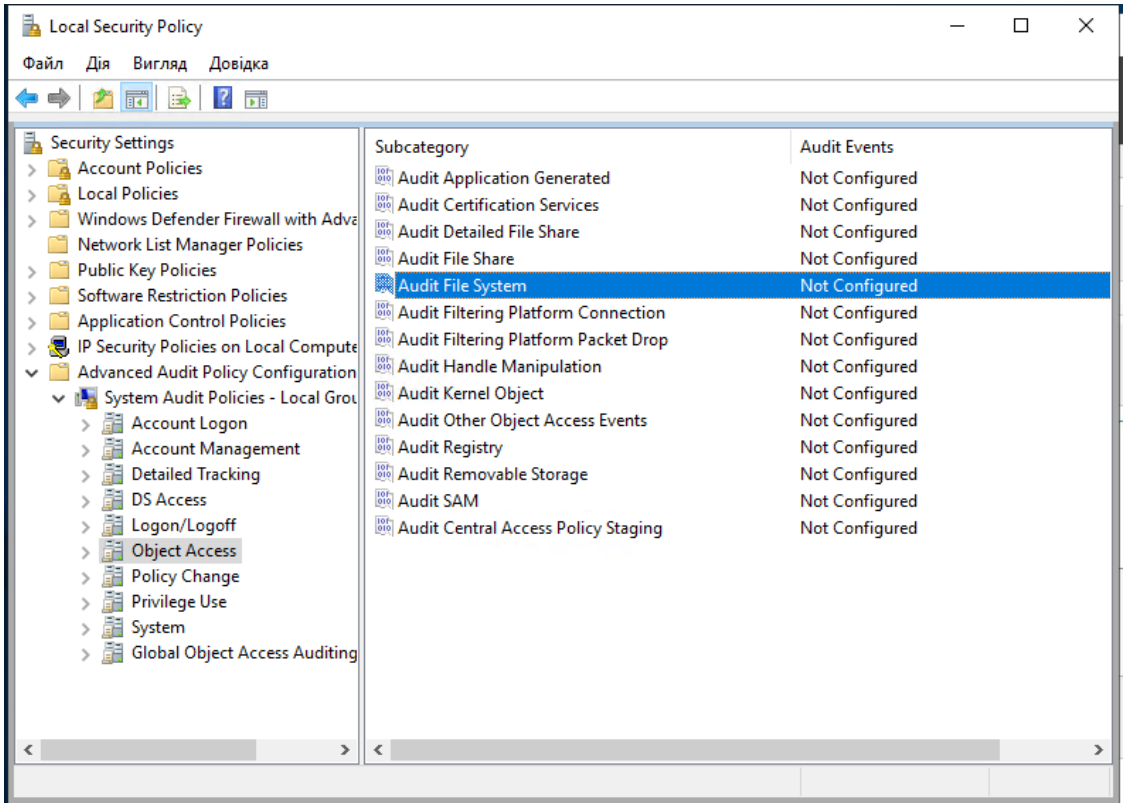


Рис. 3.4 — Політика аудиту для реєстрації подій доступу до об’єктів файлової системи.

3.3. Аудит цілісності системи

Для забезпечення перевірки цілісності даних та програмного забезпечення можна використовувати параметр "Audit System Integrity" (рис. 3.5). "Audit System Integrity" визначає, чи операційна система перевіряє події, які порушують цілісність підсистеми безпеки. Активація параметра "Audit System Integrity" дозволяє системі відслідковувати події, які можуть порушувати цілісність підсистеми безпеки. Це охоплює такі дії, як незаконні зміни в системних файлах, спроби несанкціонованого доступу до ресурсів або втручання в процес

автентифікації користувачів. Активування цього параметра дозволяє вчасно виявляти можливі загрози та реагувати на них, що є важливим елементом заходів безпеки для забезпечення цілісності даних та безпеки системи в цілому [26]. До дій, які порушують цілісність підсистеми безпеки, відносяться (див. таблицю 3.2):

- Події, що перевіряються, втрачаються через збій системи аудиту;
- Процес використовує недійсний порт виклику локальної процедури (LPC) у спробі видати себе за клієнта, відповісти в адресний простір клієнта, прочитати в адресний простір клієнта або записати з клієнтського адресного простору;
- Порушення цілісності виклику віддаленої процедури (RPC);
- Порушення цілісності коду з недійсним хеш-значенням виконуваного файлу;
- Виконання криптографічних операцій.

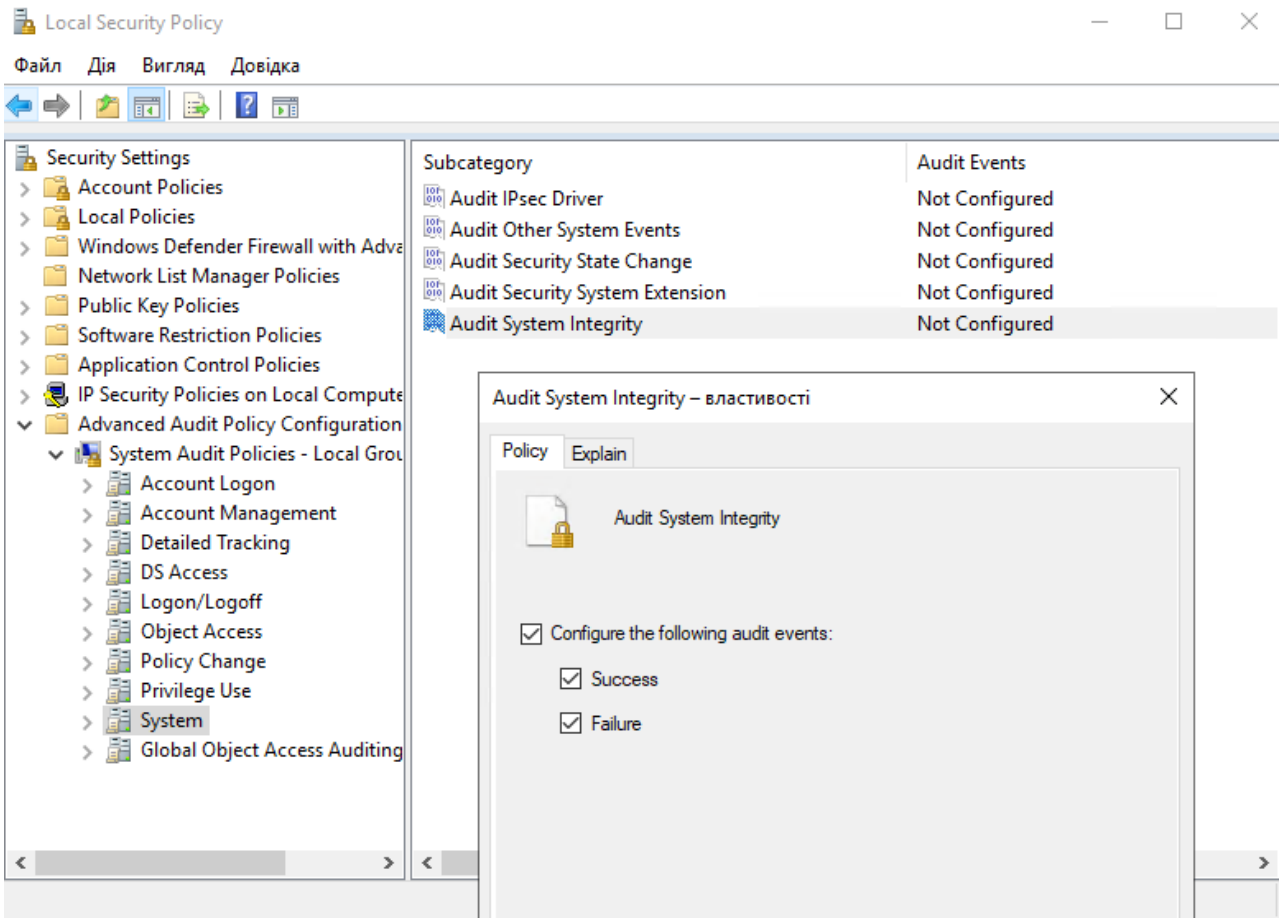


Рис. 3.5 — Політика аудиту для перевірки цілісності системи

Таблиця 3.2 Події що входять до Audit System Integrity

EventID	Опис подій Audit System Integrity
4612	Внутрішні ресурси, виділені для черги аудиторських повідомлень, були вичерпані, що призвело до втрати деяких аудитів.
4615	Недійсне використання порту LPC.
4618	Відбувся відстежений шаблон події безпеки.
4816	RPC виявив порушення цілісності під час дешифрування вхідного повідомлення.
5038	Цілісність коду визначила, що хеш зображення файлу недійсний. Файл може бути пошкоджений через несанкціоновану зміну або недійсний хеш може вказувати на потенційну помилку дискового пристрою.
5056	Проведено криптографічне само тестування.
5057	Не вдалося виконати примітивну операцію криптографії.
5060	Не вдалося перевірити операцію.
5061	Не вдалося перевірити операцію.
6281	Цілісність коду визначила, що Хеші сторінок файлу зображення недійсні. Файл може бути неправильно підписаний без хеш сторінок або пошкоджений через несанкціоновану зміну. Недійсним хеші можуть вказувати на потенційну помилку дискового пристрою.
6410	Цілісність коду визначила, що файл не відповідає вимогам безпеки для завантаження в процес.
5062	Виконано криптографічний само тест у режимі ядра.

3.4. Налаштування системи моніторингу

Zabbix - це рішення для розподіленого моніторингу корпоративного класу з відкритим кодом для моніторингу серверів. Це корисне програмне забезпечення, яке використовується розробниками для моніторингу багатьох параметрів мережі, а також працездатності та цілісності серверів, віртуальних машин, додатків, служб, баз даних, веб-сайтів, хмарних сервісів та іншого. Zabbix використовує гнучкий механізм сповіщень, який повідомляє користувачів про проблеми через різні платформи, такі як електронна пошта, Slack, Jira, Brevis.one та інші. Однією з його основних переваг є те, що це програмне забезпечення має відкритий вихідний код, що означає, що воно є абсолютно безкоштовним і постачається разом із можливістю візуалізації даних [27].

Сервер Zabbix збирає дані від усіх своїх агентів, аналізує та надає належне представлення даних. Крім того, він забезпечує налаштований та простий спосіб інтерпретації веб-інтерфейсу / інформаційної панелі з різноманітними графіками, мережевими картами, слайд-шоу та звітами (рис. 3.6 – рис.3.11).

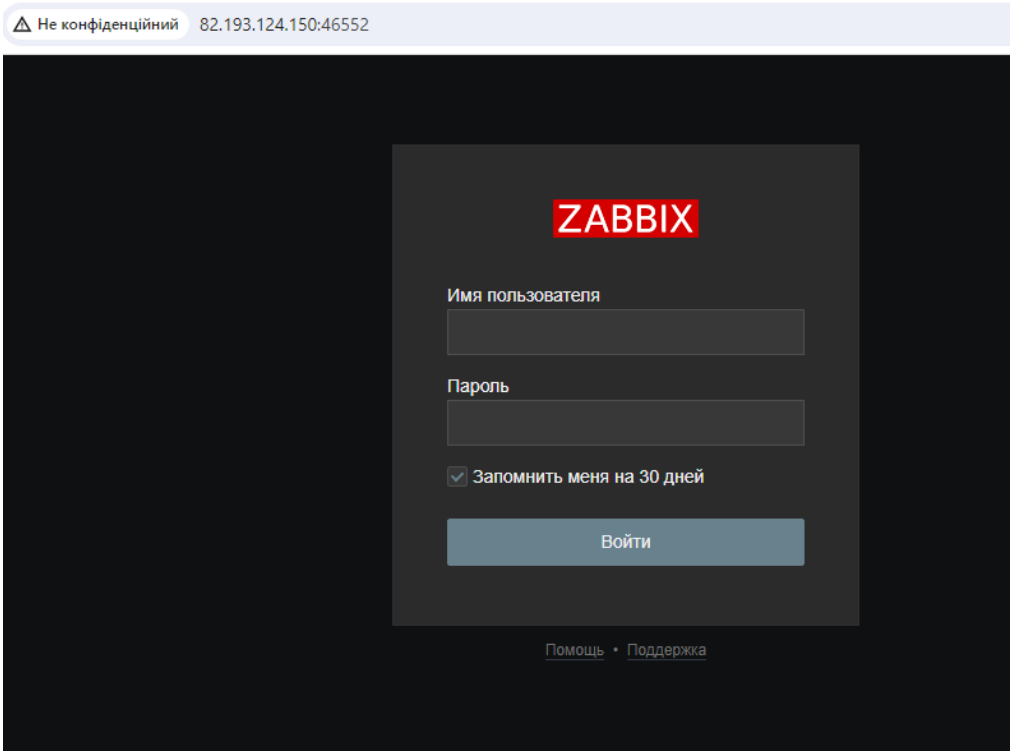


Рис. 3.6 – Головне вікно запуску сервісу

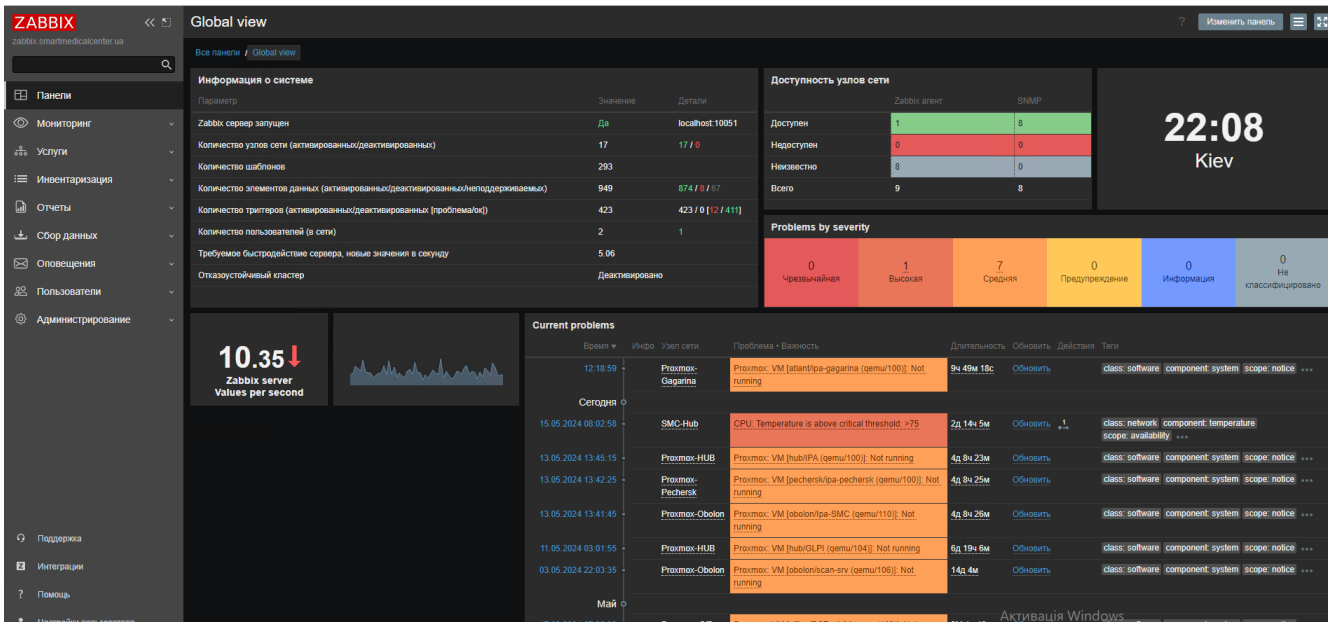


Рис. 3.7 — Web-інтерфейс Zabbix

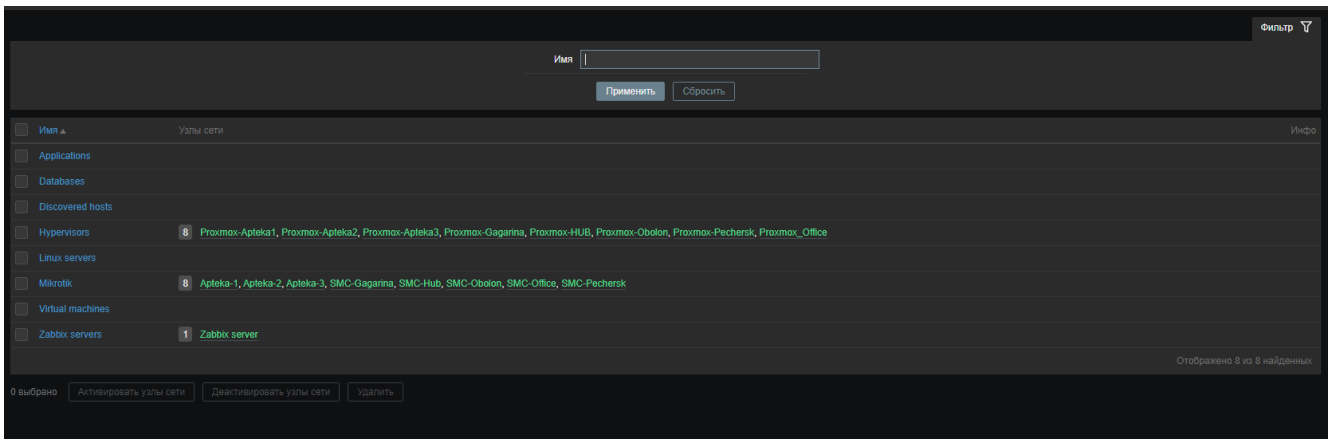


Рис. 3.8 — Група вузлів мережі

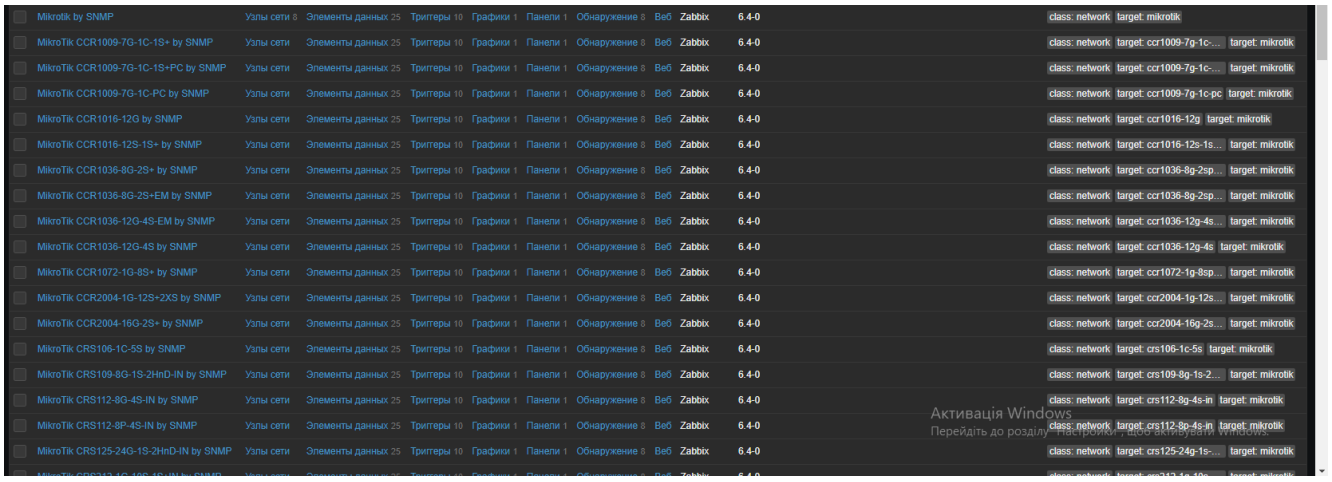


Рис. 3.9 — Група шаблонів (основоположення створення правил аудиту)

1.01.2024 00:00	08.01.2024 00:00	18
8.01.2024 00:00	15.01.2024 00:00	18
5.01.2024 00:00	22.01.2024 00:00	16
2.01.2024 00:00	29.01.2024 00:00	20
9.01.2024 00:00	05.02.2024 00:00	22
5.02.2024 00:00	12.02.2024 00:00	68
2.02.2024 00:00	19.02.2024 00:00	134
9.02.2024 00:00	26.02.2024 00:00	106
6.02.2024 00:00	04.03.2024 00:00	62
4.03.2024 00:00	11.03.2024 00:00	274
1.03.2024 00:00	18.03.2024 00:00	48
8.03.2024 00:00	25.03.2024 00:00	182
5.03.2024 00:00	01.04.2024 00:00	78
1.04.2024 00:00	08.04.2024 00:00	82
8.04.2024 00:00	15.04.2024 00:00	30
5.04.2024 00:00	22.04.2024 00:00	34
2.04.2024 00:00	29.04.2024 00:00	32
9.04.2024 00:00	06.05.2024 00:00	176
6.05.2024 00:00	13.05.2024 00:00	98
3.05.2024 00:00	19.05.2024 13:19	116

Рис. 3.10 — Сповіщення журналу

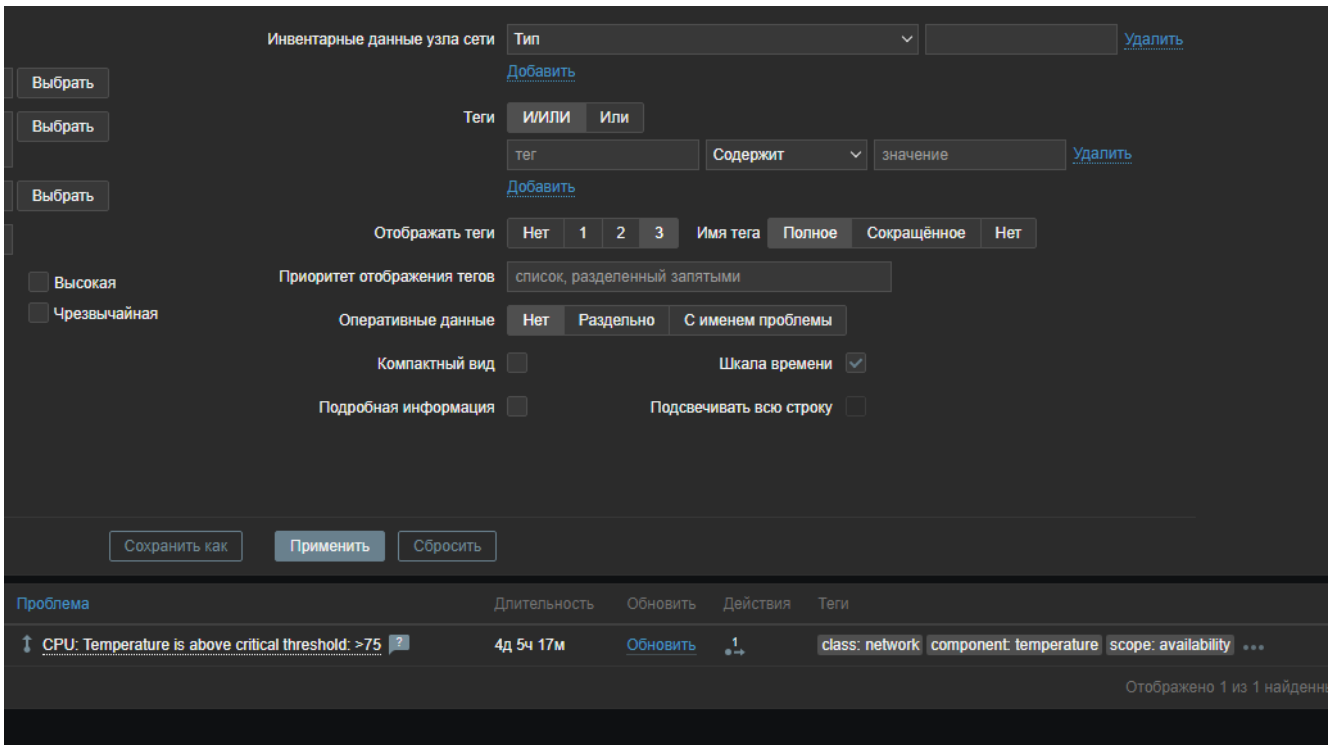


Рис. 3.11 — Проблематика наявних систем

З погляду користувача Zabbix складається з двох основних частин: сервера і агентів. Сервер розміщується на одній системі, де збирає та зберігає статистичні дані, тоді як агенти, розташовані на інших системах, збирають дані для їх подальшої передачі на сервер.

Згідно вимог, викладених у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 "Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури" [27], на сервері Zabbix здійснюється збір даних аудиту з доданих хостів (рис. 3.6).

Записи подій містять інформацію про дату та час реєстрації події, тип і ступінь успішності. Тут подано докладний опис таких деталей, як ім'я користувача, назва системи, ідентифікатор процесу та мережевий об’єкт.

Система моніторингу Zabbix впроваджує систему агрегації, збереження та аналізу журналів подій програмного та апаратного забезпечення вузла IT інфраструктури.

Для зручного відображення адміністратор повинен створити шаблони моніторингу (рис. 3.7, 3.8).

Результати моніторингу об’єктів IT інфраструктури зберігаються у базі даних сервера Zabbix; для архівування даних моніторингу необхідно зробити дамп бази даних на окремий носій інформації.

При наявності елементів, які збирають дані, та тригерів, що переходять у стан "Проблема" при виняткових ситуаціях, корисно мати механізм оповіщення, що повідомлятиме про важливі події у випадках, коли ми не можемо безпосередньо спостерігати через веб-інтерфейс.

Електронна пошта є найпопулярнішим способом надсилання повідомлень. Тому саме її налаштовують. Для цього перейдемо до панелі Administration – Media Types та виберемо Email із списку попередньо встановлених способів повідомлень (рис. 3.9).

На рисунку 3.12 показано запис даних аудиту з хостів Zabbix.

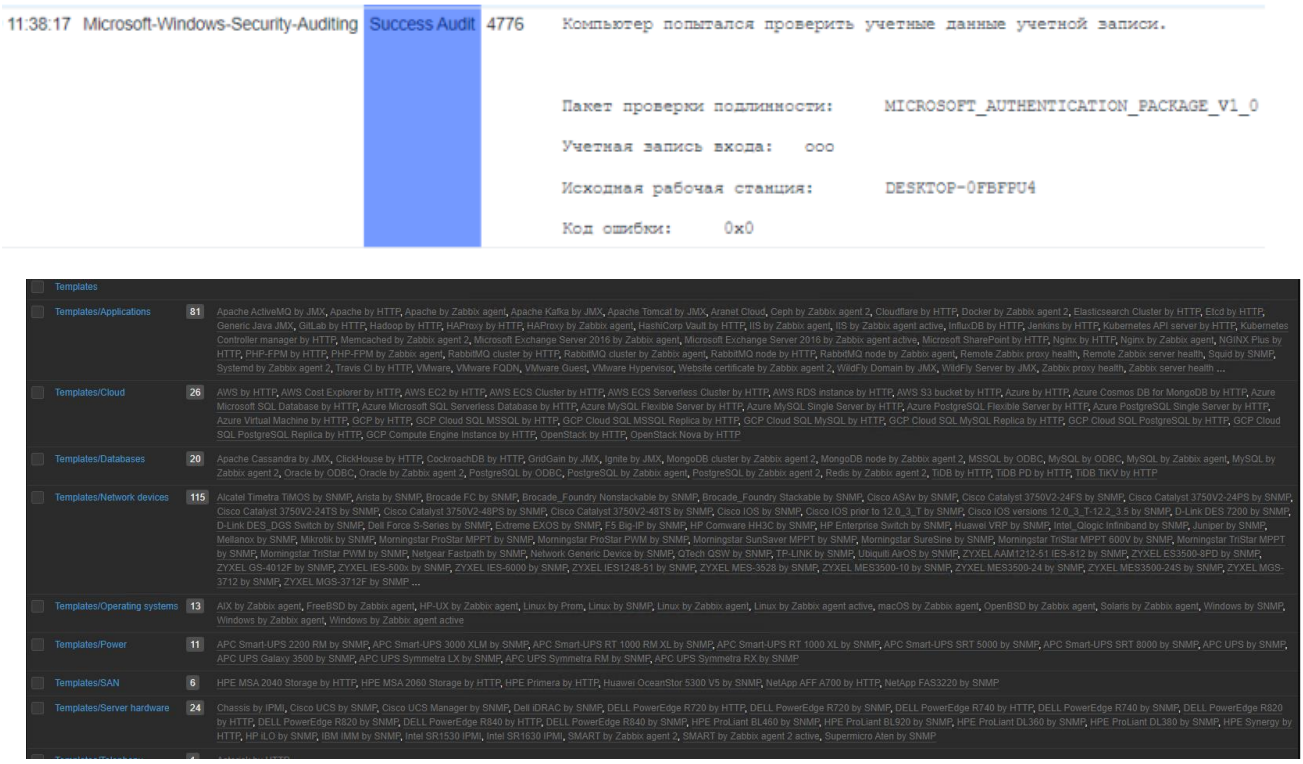


Рис. 3.12 — Запис даних аудиту з хостів Zabbix

На рисунку 3.13 представлено створення шаблону моніторингу. Список існуючих шаблонів наведений на рисунку 3.14.

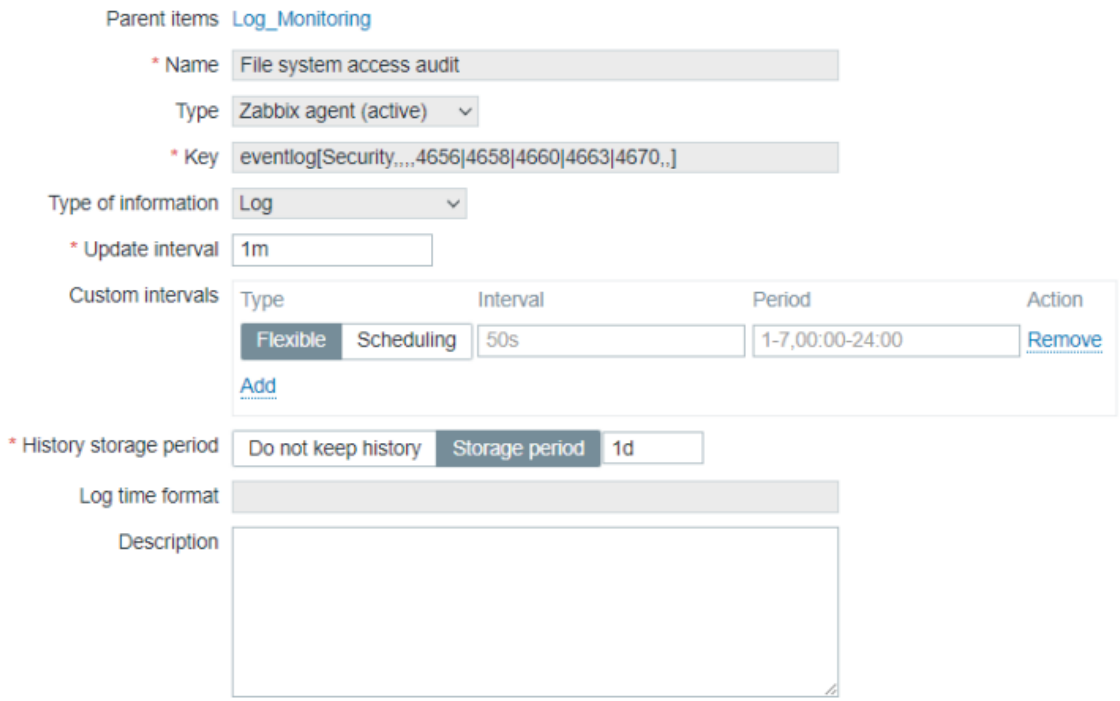
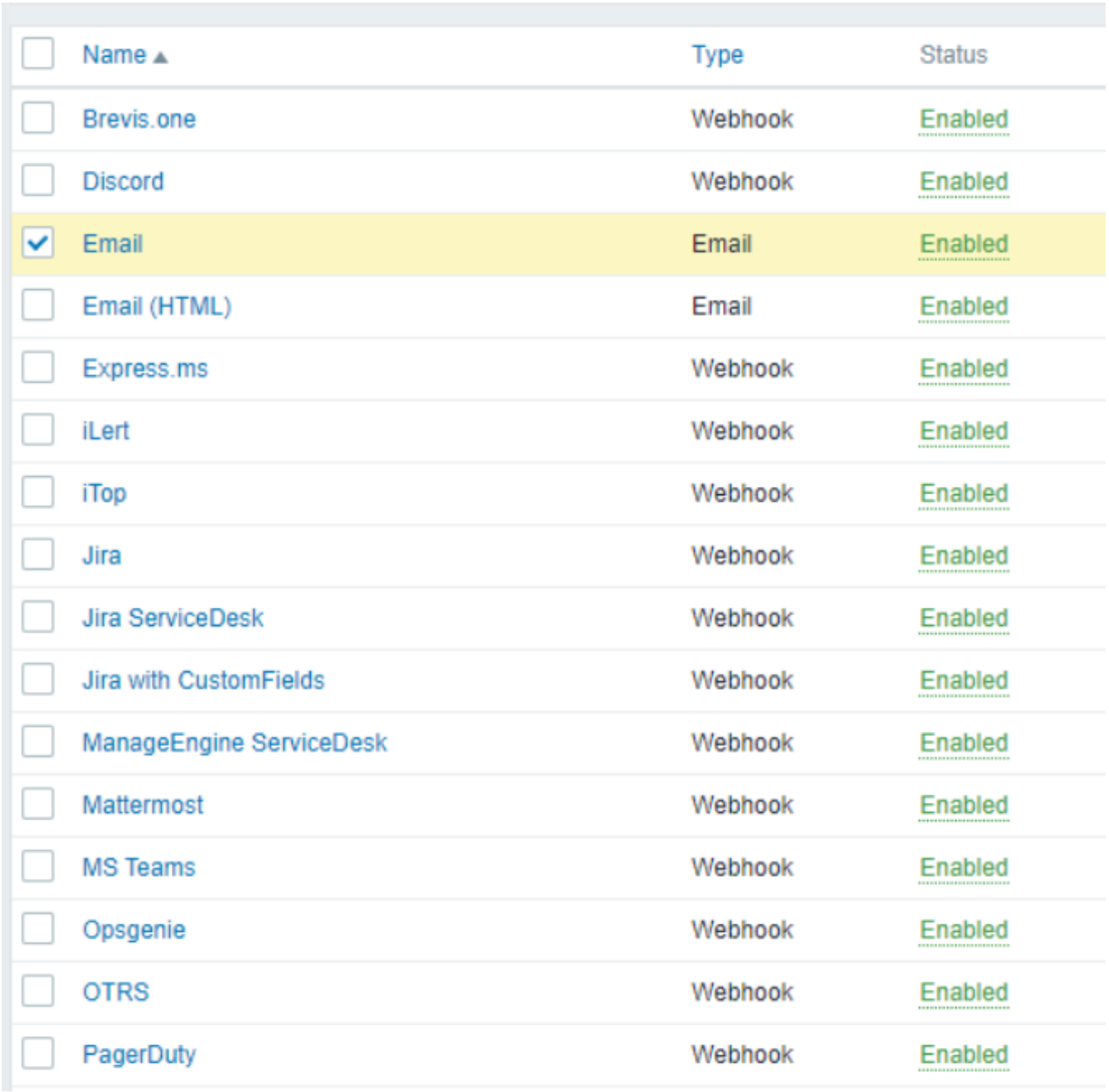


Рис. 3.13 — Створення шаблону моніторингу

Рис. 3.14 — Список шаблонів моніторингу

Zabbix надає можливість вибору більшості активних медіа та соціальних сервісів для надсилання сповіщень, або ж користувач може підключити власний сервіс за допомогою опції "Створити тип медіа". Це дозволяє налаштувати способи сповіщення відповідно до потреб і можливостей інфраструктури.

Список варіантів сповіщення показано на рисунку 3.15 та на рисунку 3.16.



Name ▲	Type	Status
Brevis.one	Webhook	Enabled
Discord	Webhook	Enabled
Email	Email	Enabled
Email (HTML)	Email	Enabled
Express.ms	Webhook	Enabled
iLert	Webhook	Enabled
iTop	Webhook	Enabled
Jira	Webhook	Enabled
Jira ServiceDesk	Webhook	Enabled
Jira with CustomFields	Webhook	Enabled
ManageEngine ServiceDesk	Webhook	Enabled
Mattermost	Webhook	Enabled
MS Teams	Webhook	Enabled
Opsgenie	Webhook	Enabled
OTRS	Webhook	Enabled
PagerDuty	Webhook	Enabled

Рис. 3.15 — Список варіантів сповіщення

Zabbix забезпечує повний цикл робочого процесу сповіщень, включаючи відправлення повідомлень, можливість підтвердження отримання інформації, пересилання повідомлень іншим особам та можливість застосування дій відповідно до сценаріїв автоматизації.

При налаштуванні відправлення електронної пошти, користувач може клацнути на опцію "Ел. пошта", щоб відкрити вікно налаштувань. У полі "SMTP-адреса електронної пошти" вводиться адреса відправника повідомлень, а також

здійснюються налаштування мережевих протоколів для відправлення пошти. Після введення необхідних даних зміни зберігаються для подальшого використання. Збережемо зміни (див. рисунок 3.10).

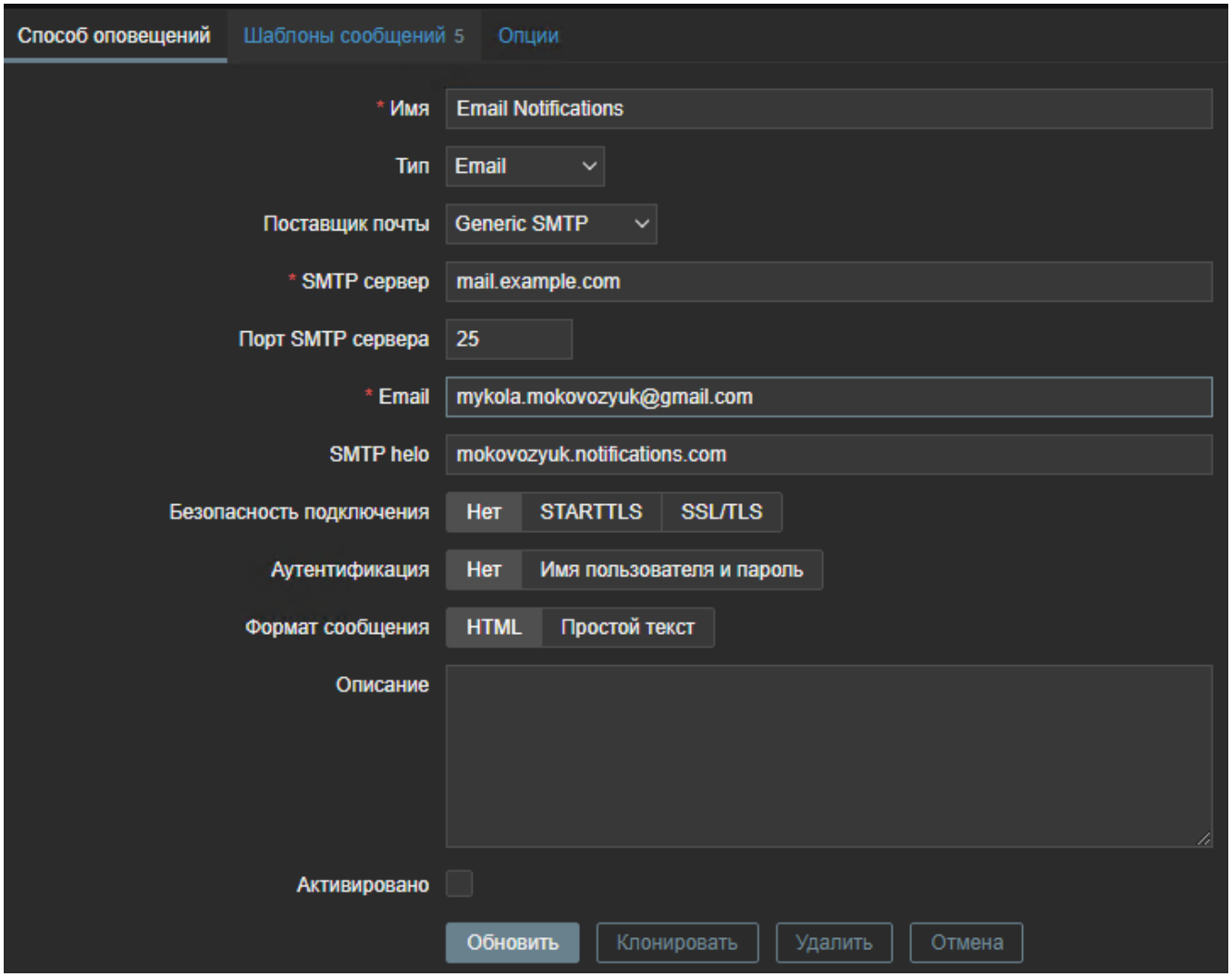


Рисунок 3.16 — Список варіантів сповіщення

Тепер ми можемо застосувати ці зміни для наших тригерів. Перейдемо на панель Actions та створимо дію, яка буде реагувати на події з конкретними унікальними ідентифікаторами, що виникають під час роботи персонального комп'ютера. У рамках даної роботи ми розділили такі події на три логічних блоки: Audit System Integrity з ID 4612, 4615, 4618, 4816, 5038, 5056, 5057, 5060, 5061, 5062, 6281, 6410; (дивитися рисунок 3.11) Audit File System з ID 4656, 4658, 4660, 4663, 4670(дивитися рисунок 3.12); та Audit User Account Management з ID 4624, 4648,

4672, 4625, 4647, 4776, 4771, 4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740, 4767, 4781, 4794, 4741, 4742, 4743.Дуже важливо правильно групувати та обробляти існуючі логи, мати можливість легко розділяти їх на логічні та практичні частини.

На рисунку 3.17 представлений фільтр подій для Audit System Integrity.

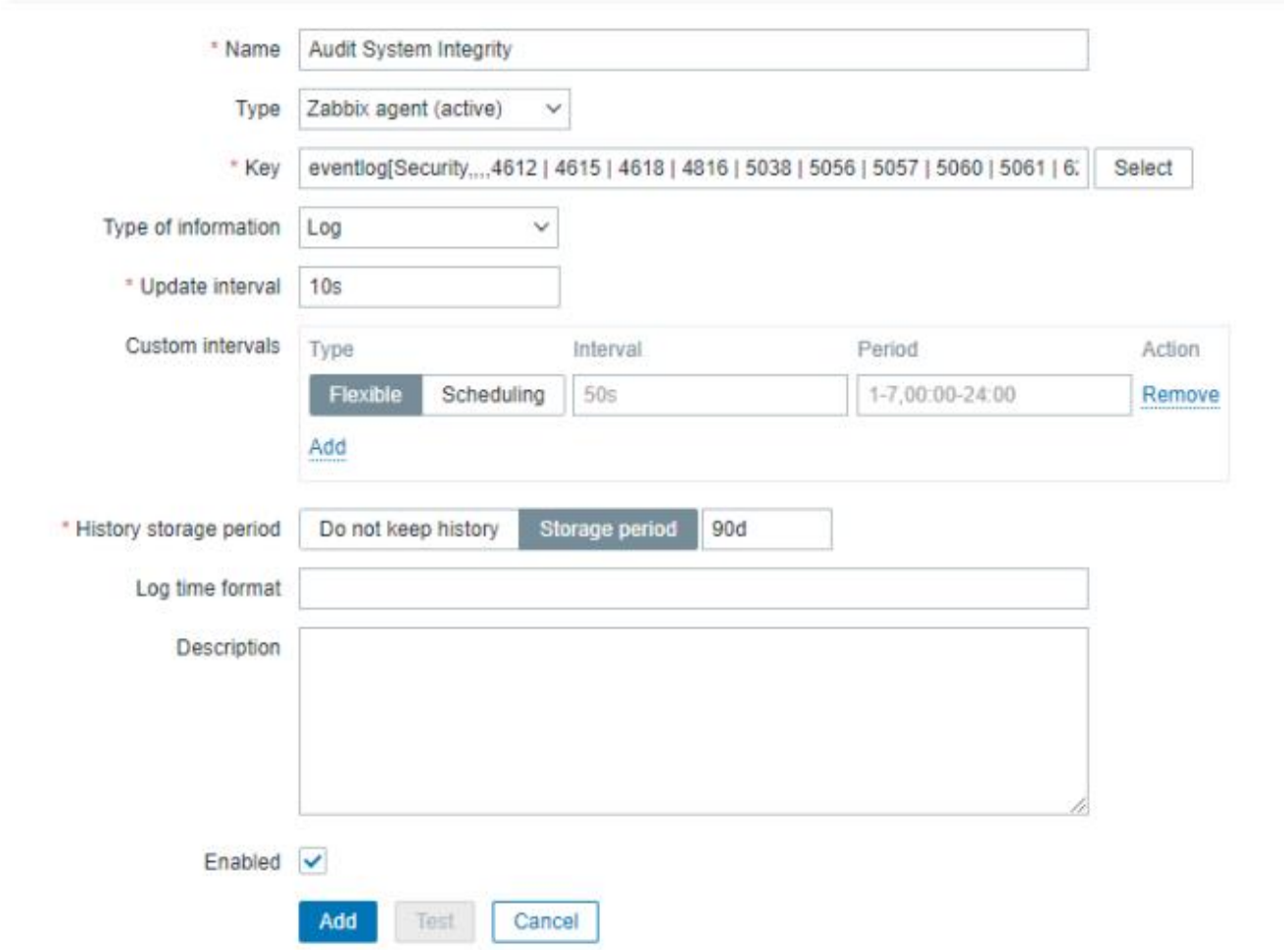


Рис. 3.17 — Фільтр подій для Audit System Integrity

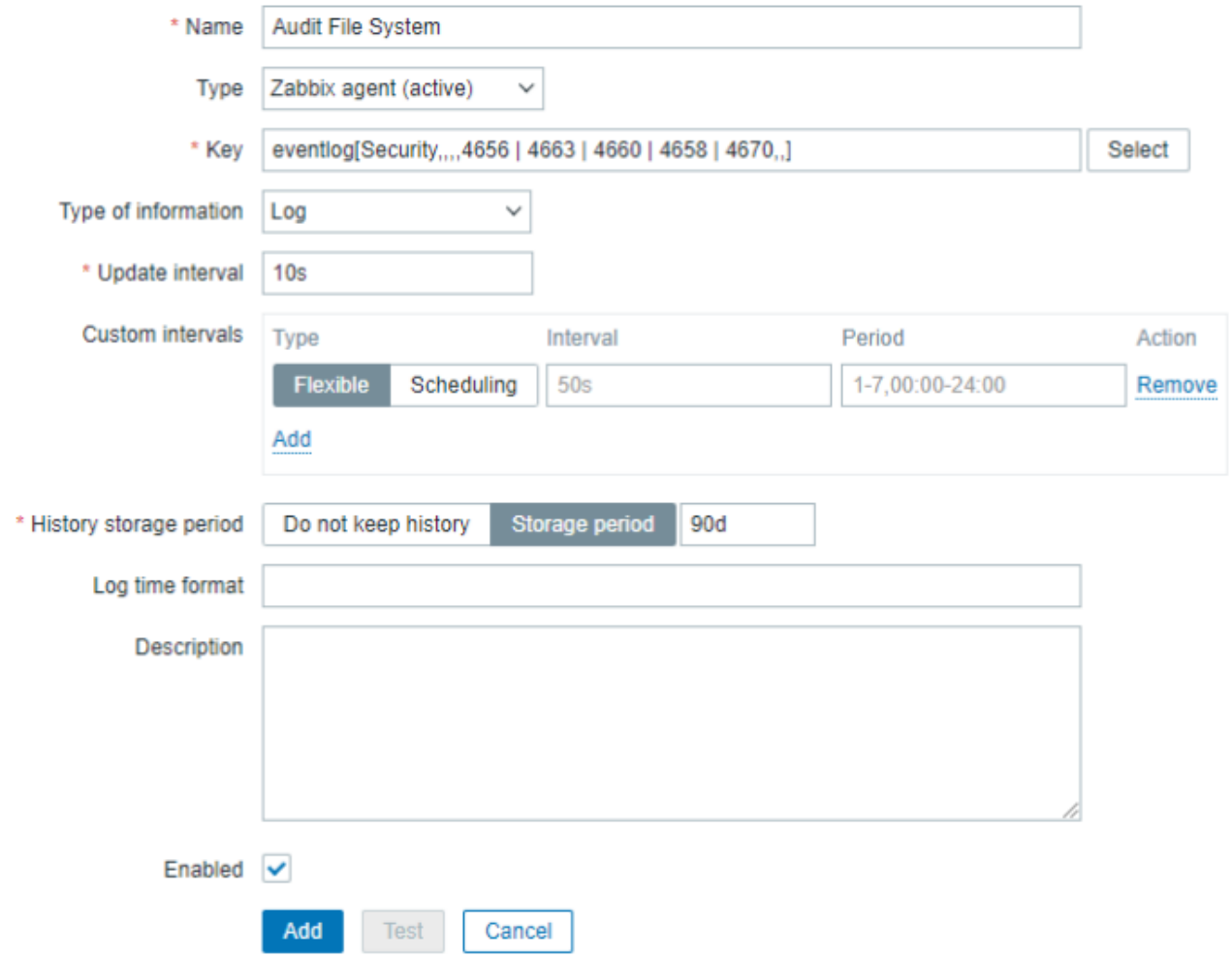


Рис. 3.18 — Фільтр подій для Audit File System

Давайте налаштуємо повідомлення веб-інтерфейсу та рівень логування цієї інформації. Для цього перейдемо на панель Тригери – Створити тригер та додамо умову настання виняткової ситуації (рис. 3.18). Виберемо рівень серйозності цього повідомлення як "Попередження", а умову – одне чи більше спрацювання шуканих ідентифікаторів подій персонального комп'ютера. Подібно повторимо для двох інших груп.

Крім того, у цьому меню ми можемо встановити умову скасування виключної ситуації або створити цілий ланцюг різних умов та перевірок. Розглянемо механізм сповіщень для різних груп користувачів. Для цього необхідно перейти до панелі Конфігурація – Дія – Дія тригера, де ми можемо додати групу (чи декілька) користувачів, що отримають повідомлення про помилку чи попередження.

Для наочності налаштуємо повідомлення про помилки для адміністраторів на електронну пошту. Натиснемо Створити дію, введемо ім'я, умову та додамо групу користувачів, що будуть отримувати сповіщення (дивитися рисунок 3.14).

Створення чи редагування групи користувачів можливе в меню Адміністрування – Групи користувачів/Ролі користувача/Користувачі.

Таким чином, система моніторингу Zabbix реалізує визначений аудит управління обліковими записами, аудит доступу об'єктів до файлової системи та аудит цілісності системи, а також здійснює активний аудит за допомогою тригерів. Ці вимоги можна вважати мінімально необхідними, згідно з постановою Кабінету Міністрів у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 року №518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [5]. Умова активації тригеру представлена на рисунку 3.19.

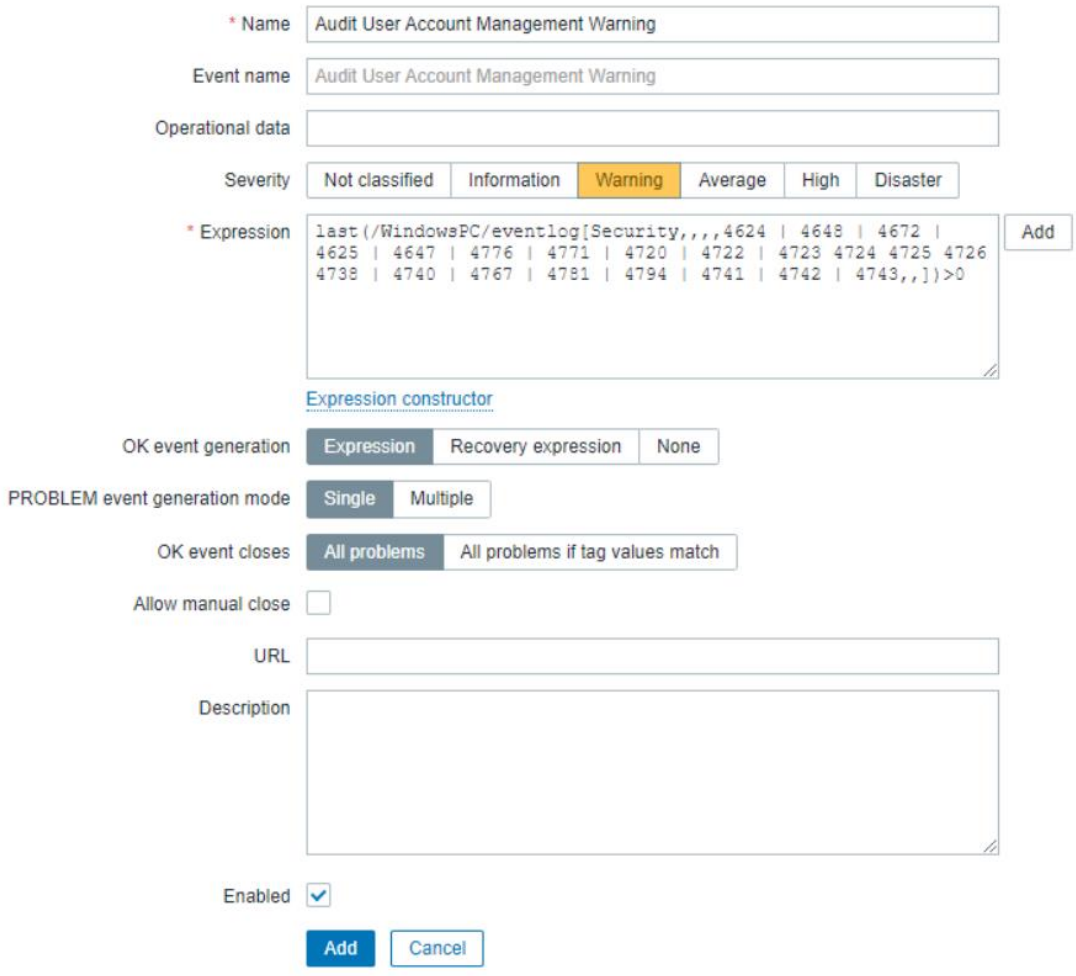


Рис. 3.19 — Умова активації тригеру

Встановлення групи отримувачів email листа показано на рисунку 3.20.

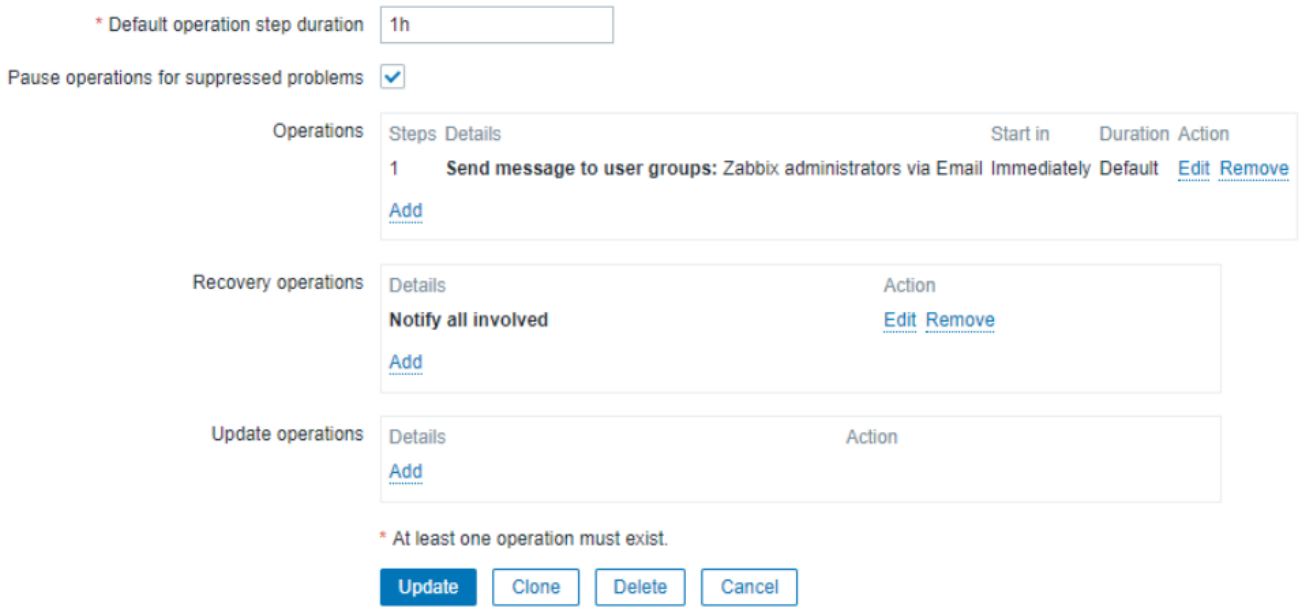


Рис. 3.20 — Встановлення групи отримувачів email листа

ВИСНОВКИ

Досліджено основні терміни і концепції, що стосуються моніторингу в галузі кібербезпеки. Зокрема, розглянуті поняття моніторингу, аналізу, виявлення та реагування на загрози та інциденти в інформаційній безпеці. Було визначено важливість моніторингу для забезпечення безпеки критичної інфраструктури та підтримки безперервності бізнесу. Підкреслено, що ефективний моніторинг є ключовим елементом в управлінні кібербезпекою та дозволяє оперативно виявляти та реагувати на потенційні загрози.

Проаналізовані потенційні атаки, такі як DDoS-атаки, фішинг, введення зловмисного коду та інші, що можуть призвести до порушення нормального функціонування інфраструктури та нанести серйозні збитки. Висвітлено необхідність розробки та впровадження ефективних заходів захисту для запобігання цим загрозам та зменшення ризиків для безпеки критичних інфраструктурних об'єктів.

Розглянуто методи та процеси аудиту для забезпечення безпеки критичної інфраструктури. Було визначено, що аудит є важливим інструментом для оцінки ефективності системи безпеки, виявлення вразливостей та розробки рекомендацій щодо їх виправлення. Підкреслено важливість проведення регулярних аудитів для підтримки високого рівня безпеки критичних інфраструктурних об'єктів і зменшення ризиків

Виявлено, що ця система моніторингу має численні переваги, включаючи простоту встановлення та конфігурації, розширюваність, можливості моніторингу різноманітних ресурсів, а також потужність та гнучкість. За допомогою своєї архітектури, яка базується на розподіленій моделі, Zabbix може ефективно моніторити навіть найбільш складні інфраструктури.

Під час аналізу існуючих систем аналогів безперервного моніторингу загроз було виявлено, що кожна з них має свої переваги та обмеження. Деякі системи спеціалізуються на певних аспектах моніторингу, таких як мережевий трафік або виявлення загроз безпеки, тоді як інші пропонують більш широкий спектр функцій.

Ефективний вибір системи залежить від конкретних потреб та характеристик інфраструктури організації.

У результаті аналізу огляду понять та термінів в галузі кібербезпеки, а також огляду систем моніторингу, стало очевидним, що правильно налаштована політика аудиту, використання потужних та гнучких систем моніторингу, таких як Zabbix, та уважний аналіз існуючих систем аналогів, є важливими складовими ефективного кіберзахисту організації. Тільки за умови вивчення та розуміння цих аспектів організація може ефективно виявляти та запобігати потенційним загрозам та атакам на її інформаційну інфраструктуру.

ПЕРЕЛІК ПОСИЛАНЬ

1. Програмне забезпечення для моніторингу мережі. Spice Works. WWW-публікації. URL: http:// www.spiceworks.com/free-network-monitoring-management-software.

2. Center for Internet Security – Cybersecurity Threats. Center for Internet Security. URL: https://www.cisecurity.org/cybersecuritythreats/

3. О'Доннелл, Гленн 2004. Аналітика маршруту збагачує технологічні відносини. PDF-документ META Group, Inc. URL: http://www.glennodonnell.com/documents/d2751-RouteAnalytics.pdf.

4. Покращення моніторингу мережі за допомогою Route Analytics 2013. Дизайн пакетів. PDF документ. URL: http://www.packetdesign.com/resources/white-papers/ Enhancing%20Network%20Monitoring%20with%20Route%20Analytics.pdf

5. Zabbix True Open Source. Zabbix. URL: http:// www.zabbix.com/true_open_source.php

6. Zabbix. Документація Zabbix 2.4. URL: https://www.zabbix.com/documentation/ 2.4/

7. Analyze Azure network security group flow logs - Graylog. Developer tools, technical documentation and coding examples Microsoft Docs. URL:https://docs.microsoft.com/en-us/azure/network-watcher/network-watcheranalyze-nsg-flow-logs-graylog

8. Eventlog Key – Win32 apps. Developer tools, technical documentation andcoding examples | Microsoft Docs. URL: https://docs.microsoft.com/enus/windows/win32/eventlog/eventlog-key

9. Жайворонок О.І. Вдосконалення механізму протидії інформаційному тероризму в Україні в загальнодержавній системі антикризового реагування/ *Інвестиції: практика та досвід*. 2018. № 17. С. 113-119

10. Комар М. П., Боднар Д. І., Саченко А. О. Інтелектуалізована інформаційна технологія виявлення комп'ютерних атак. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2010. № 2. С. 133- 137.

11. Міночкін А. І., Романюк В. А., Шацило П. В. Виявлення атак в мобільних радіомережах. *Збірник наукових праць* № 1. К.: ВІТІ НТУУ “КПІ”, 2005. С. 102-111.

12. Одарченко Р., Гнатюк В. Концептуальні засади підвищення рівня кібербезпеки сучасних стільникових мереж. Conceptual framework of modern cellular network cybersecurity rising // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 143-149.

13. Тарасюк А.В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. Прикарпатський юридичний вісник. 2020. Вип. 1. С. 133-136

14. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.- практ. посіб. / за заг ред. проф. Я. Ю. Кондратьева. Київ, 2004. 144 с

15. Бакін Д.С. Проблеми захисту інформації в комп’ютерних мережах: матеріали всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С. 79-80. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5101/1/AUConferenceCyberSecurity_November2016_p79.pdf

16. Болехівський Н. Полотай О. Класифікація мережевих атак та методи протидії і ззахисту. URL: https://sci.ldubgd.edu.ua/bitstream/handle/123456789/6737/1.pdf?sequence=1&isAllowed=y

17. Моніторинг та керування мережею. Tibbo Systems. WWW-публікації. URL: http:// aggregate.tibbo.com/solutions/network_management/network_monitoring.html. (дата звернення: 25.04.2024).

18. Функції Zabbix, Zabbix. WWW-публікації. URL: http://www.zabbix.com/features.php.

19. Drogseth, Dennis 2003. HP інвестує в аналітику маршрутів за допомогою Packet Design. Мережевий світ. WWW-публікація. URL: http://www.networkworld.com/article/2338253/infrastructure-management/hpinvests-in-route-analytics-with-packet-design.html.

20. Аксьончиков С.О., Ємельянова І.В., Маркова К.Д., Сватовський І.І. Регресійний аналіз тенденцій розвитку кібератак.. 2017. Випуск 36. С. 5-13. URL: http://nbuv.gov.ua/j-pdf/VKhIMAM_2017_36_3.pdf

21. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. Реєстрація, зберігання і обробка даних. 2015. Т.17. №2. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131565/04-Korpan.pdf?sequence=1

22. Телекомунікаційні та інформаційні мережі.: Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТКнига, 2010. – 708 с.

23. Jozef Janitor, Karol Kniewald. Visual Learning Tools for Teaching / Learning Computer Networks: Sixth International Conference on Networking and Services, 2010. P. 351-355.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО - КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО -НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кваліфікаційна робота на тему:

«Розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури»

Виконав: МоковозюкМикола
Керівник: д.т.н.професор ПорохницькийОлександр

КИЇВ - 2024

Мета роботи – розробка і впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури з метою підвищення рівня безпеки та стійкості цих об'єктів до кібератак.

Об'єкт дослідження – процес розробки та впровадження системи моніторингу загроз кібербезпеці для об'єктів критичної інфраструктури .

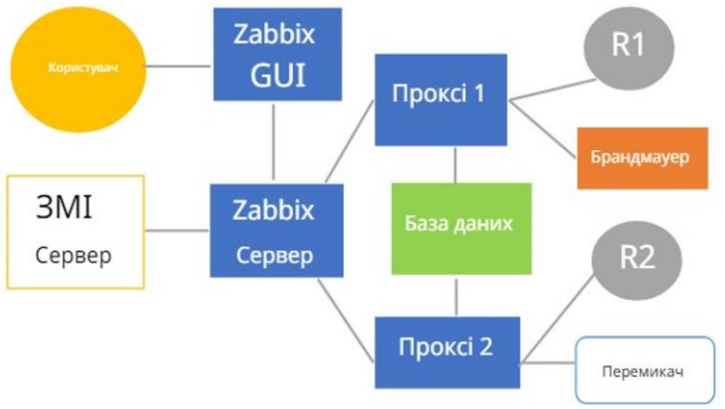
Предмет дослідження – розробка системи реалізації безперервного моніторингу загроз кібербезпеці для критичної інфраструктури .

Наукові завдання:

- Провести огляд понять та термінів в галузі кібербезпеки.
- Визначити основні загрози та ризики для критичної інфраструктури.
- Розглянути процес аудиту інформаційної безпеки.
- Налаштувати політику аудиту системи.
- Проаналізувати існуючі системи безперервного моніторингу загроз.
- Впровадити систему моніторингу Zabbix для аналізу управління обліковими записами, доступу до об'єктів файлової системи та цілісності системи.
- Налаштувати систему моніторингу для ефективного виявлення та реагування на загрози кібербезпеки.
- Провести аналіз ефективності розробленої системи та зробити висновки щодо її використання для захисту критичної інфраструктури.

КомпонентиZabbix

3



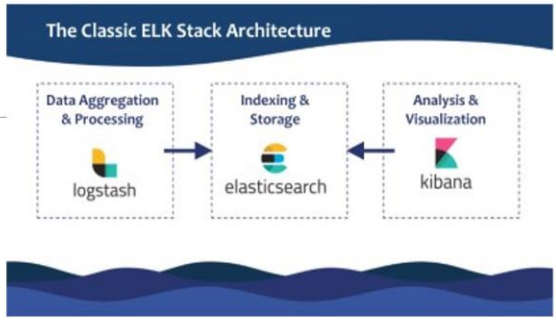
Zabbix складається з наступних компонентів : Zabbix Server, Zabbix Proxy, Zabbix Agent та веб-інтерфейс . Кожен з них відіграє певну роль у моніторингу .

Аналоги безперервного моніторингу

4

Nagios®

Nagios - це система моніторингу комп'ютерних систем та мереж, яка виявляє і відслідковує проблеми в інфраструктурі інформаційних технологій, надсилаючи сповіщення про них для швидкого реагування.



ELK Stack - це популярна відкрита платформа для збору, аналізу та візуалізації логів та інших даних для моніторингу та аналізу систем.

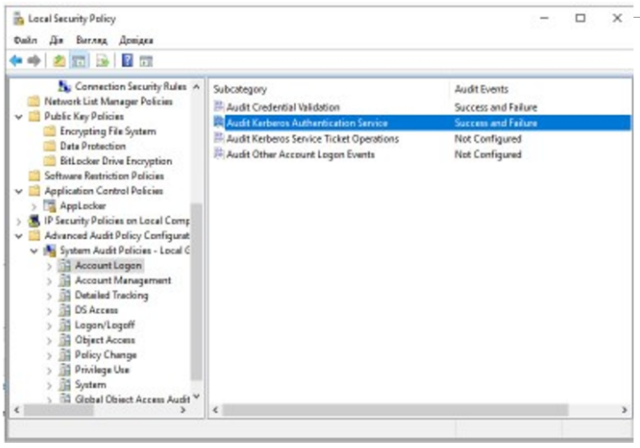
graylog

Graylog - це відкрите програмне забезпечення для централізованого збору, управління та аналізу журналів подій та даних великих обсягів з різних джерел для підвищення безпеки та ефективності мережі.

Управління обліковими записами

5

Для того, щоб система Windows фіксувала події входу/виходу користувачів у журналі подій, необхідно увімкнути відповідні параметри аудиту системи



Політики аудиту для реєстрації подій входу/виходу облікових записів користувачів

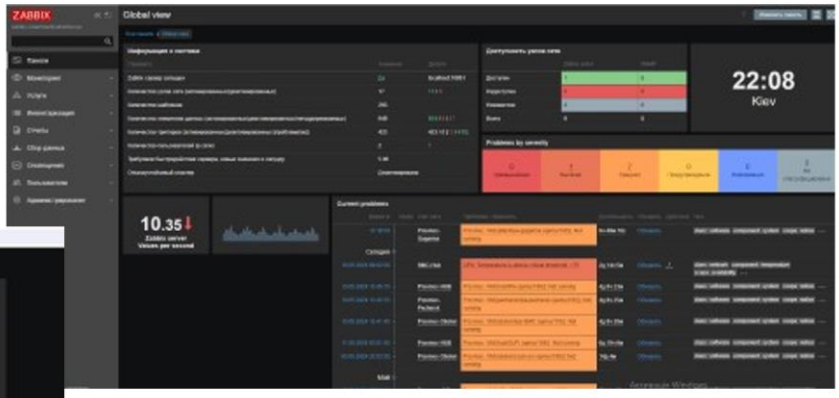
Операції з управління обліковими записами користувачів та безпекою

- Встановлення або зміна пароля облікового запису користувача;
- Додавання ідентифікатора безпеки (SID) до історії SID облікового запису користувача або відсутність такого додавання;
- Налаштування пароля режиму відновлення служб каталогів;
- Зміна дозволів для облікових записів адміністраторів;
- Перерахунок членства користувача в локальній групі.

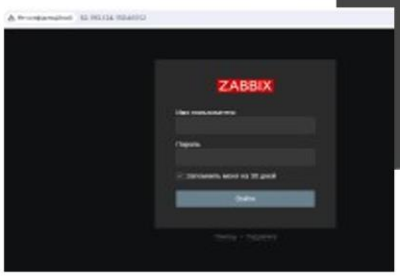
Налаштування системимоніторингу

6

Zabbix - це вільне програмне забезпечення для моніторингу мережі та систем, яке надає можливості моніторингу різних параметрів системи, таких як ресурси комп'ютера, мережеві пристрої, сервери програмного забезпечення та інші пристрої та послуги.



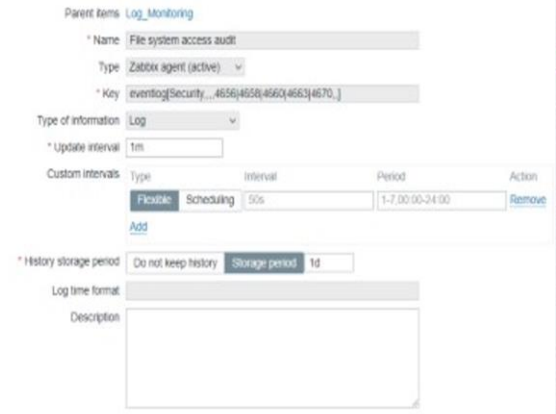
Web-інтерфейс Zabbix



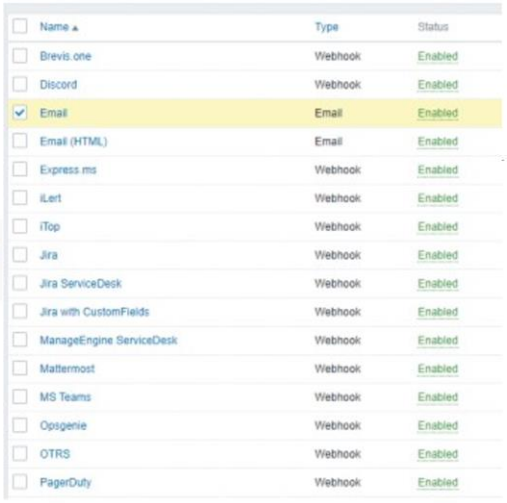
Головне вікно запуску сервісу

Розробката тестування алгоритміввиявленняаномалій

7



Створення шаблону моніторингу

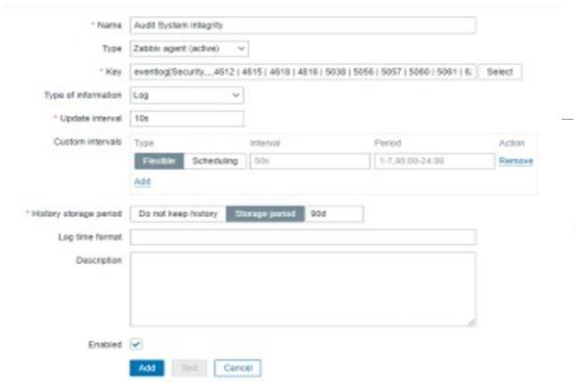


Список варіантів сповіщення

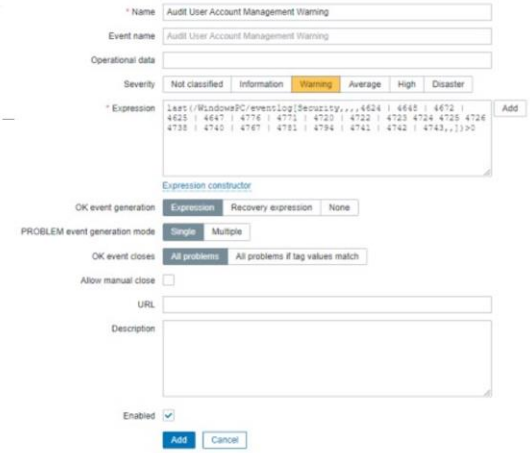
Рисунок 9 – Отримані події в режимі реального часу

Фільтрування подійвивленняаномалій за допомогоюZabbix

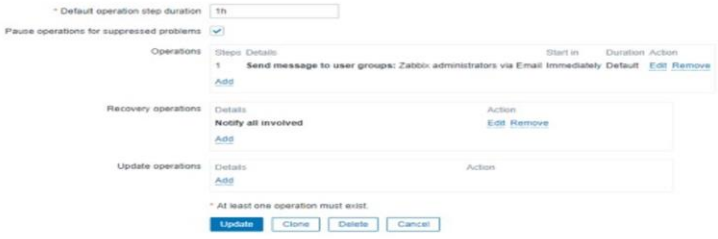
8



Фільтр подій для Audit System Integrity



Умова активації тригеру



Встановлення групи отримувачів email листа

ВИСНОВКИ

9

- Виявлено, що система моніторингу має численні переваги, включаючи простоту встановлення та конфігурації , розширюваність , можливості моніторингу різноманітних ресурсів, а також потужність та гнучкість. За допомогою своєї архітектури, яка базується на розподіленій моделі, Zabbix може ефективно моніторити навіть найбільш складні інфраструктури .
- Під час аналізу існуючих систем аналогів безперервного моніторингу загроз було виявлено, що кожна з них має свої переваги та обмеження. Деякі системи спеціалізуються на певних аспектах моніторингу, таких як мережевий трафік або виявлення загроз безпеки, тоді як інші пропонують більш широкий спектр функцій . Ефективний вибір системи залежить від конкретних потреб та характеристик інфраструктури організації .
- У результаті аналізу огляду понять та термінів в галузі кібербезпеки, а також огляду систем моніторингу, стало очевидним, що правильно налаштована політика аудиту, використання потужних та гнучких систем моніторингу, таких як Zabbix, та уважний аналіз існуючих систем аналогів, є важливими складовими ефективного кіберзахисту організації . Тільки за умови вивчення та розуміння цих аспектів організація може ефективно виявляти та запобігати потенційним загрозам та атакам на її інформаційну інфраструктуру.