МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

«Розробка згідно законодавчих вимог методів та програмного додатку для реєстрації, зберігання та аналізу подій безпеки на базі ОС Windows»

Завідувач випускаючої кафедри **Любчак В.О.**

Керівник роботи **Любчак В.О.**

Студента групи КБ – 81 **Резніка М.М.**

СУМИ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____
Зав. кафедрою Любчак В.О.
“____”_____2022р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-81 спеціальності “Кібербезпека” денної форми навчання Резніка Миколи Миколайовича.

Тема: “ Розробка згідно законодавчих вимог методів та програмного додатку для реєстрації, зберігання та аналізу подій безпеки на базі ОС Windows ”

Затверджена наказом по СумДУ
№_____від_____2022 р.

Зміст пояснювальної записки 1) Інформаційний огляд; 2)Засоби реєстрації та аналізу подій; 3). Впровадження системи моніторингу Zabbix.

Дата видачі завдання “_____”_____2022 р.

Керівник випускної роботи _____Любчак В.О.
Завдання прийняв до виконання _____Любчак В.О.

РЕФЕРАТ

Записка: 39 стор., 14 рис., 3 табл, 2 додатків, 10 джерел.

Мета роботи – налаштувати систему моніторингу локальної мережі згідно вимог Постанови Кабінету Міністрів України №518.

Об'єкт дослідження – аудит інформаційної безпеки, зберігання та реєстрація подій безпеки.

Предмет дослідження – вивчення можливостей автоматизації моніторингу журналів подій IT інфраструктури на базі ОС Windows

Результати – налагоджена та продемонстрована система моніторингу журналів подій для операційної системи Windows, задовольняє вимоги чинних пунктів 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури", на операційній системі Windows з використанням Системи моніторингу Zabbix.

ЗМІСТ

ВСТУП

В сучасних умовах розвитку суспільства, зберігається тенденція впровадження нових інформаційних технологій у всі сфери нашого життя. Наявність надійної IT інфраструктури давно перейшло в розряд критичних вимог для забезпечення функціонування бізнес-процесів організації, припинення функціонування інформаційної інфраструктури може призвести до зупинки діяльності всієї організації.

З одного боку, організації мають забезпечити доступ авторизованих користувачів до своїх інформаційних ресурсів, а з іншого мати налагоджену систему менеджменту інцидентів інформаційної безпеки, це необхідно для мінімізації наслідків виникнення внутрішніх і зовнішніх загроз. Для детальної оцінки захищеності інформаційної системи, а також її спроможності забезпечити функціонування під час внутрішніх і зовнішніх загроз інформаційної безпеки, які постійно змінюються, організаціям необхідно регулярно проводити аудит інформаційної безпеки [1].

Проведення аудиту інформаційної безпеки дозволяє оцінити поточний стан безпеки функціонування інформаційної системи, прогнозувати майбутні ризики, та керувати впливом ризиків на бізнес-процеси організації.

Інструментом для проведення аудиту безпеки IT-інфраструктури можуть слугувати системи моніторингу, які забезпечують безперервний збір даних про події в операційній системі, та їх подальшу централізовану обробку.

Сьогодні перед адміністраторами безпеки постає питання впровадження систем моніторингу, адже через постійне розширення IT-інфраструктури та вдосконалення українського законодавства, яке вимагає дедалі вищий рівень кіберзахисту інформаційних систем, проведення аудиту безпеки стає дедалі складнішим.

1. ІНФОРМАЦІЙНИЙ ОГЛЯД

1.1 Вимоги Українського законодавства

Відповідно до глобального контексту указу Президента України №447/2021 “Про Стратегію кібербезпеки України у XXI столітті” продовжується формування шостого технологічного укладу, що призведе до виникнення ризиків, пов’язаних з впровадженням нових технологій. Звісно внаслідок атаки РФ на Україну, саме загроза ворожих кібератаки стає загрозою номер один, вони можуть мати різні цілі наприклад: крадіжку важливих документів , виявлення позиції військових , маніпуляція цивільних громадян на окупованих територіях та небезпеку вразливості об'єктів критичної інфраструктури.

Поширення кіберзагроз на всі сфери життєдіяльності та збереження тенденції розвитку засобів кібератак зумовлює необхідність зміни національної тактики протидії кіберзагрозам. Для гарантування громадянам України безпечної цифровізації всіх сфер суспільного життя у невпинно змінюваному цифровому світі потрібно створити ефективну та збалансовану систему національної кібербезпеки.

На перший план висувається питання швидкого виявлення вразливостей і кібератак, та подальше реагування з поширенням даних про них для мінімізації майбутньої шкоди [2].

Вимоги щодо реєстрації події інформаційної системи в інформаційних, телекомунікаційних та змішаних системах, які є державними інформаційними ресурсами або обробляють інформацію, встановлена у пункті 11 Постанови Кабінету Міністрів України від 29 березня 2006 р. №373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”:

Система повинна реєструвати такі події:

- ідентифікація та аутентифікація облікових даних користувача;
- виконання процедури з обробки інформації, яка може становити державну таємницю;
- несанкціонований доступ до інформації;
- управління правами доступу до обробки інформації;
- перевірка компонентів засобів захисту інформації.

Під час роботи системи моніторингу повинні виконуватися наступні правила:

- забезпечується можливість проведення аналізу зареєстрованих даних виключно адміністратором безпеки;
- реєстрація повинна здійснюватися автоматично, а зареєстровані дані повинні бути захищені від знищення та модифікації користувачами без необхідних повноважень адміністратора безпеки;
- реєстрація несанкціонованого доступу, видалення або змінення інформації, що становить державну таємницю; забезпечення службовим журналом, що зберігає повідомлення для адміністратора безпеки [3].

Українське законодавство відносить до об’єктів критичної інфраструктури організації та установи незалежно від форми власності; діяльність яких пов’язана наданням послуг або виконанням технологічних процесів, що мають велике економічне та промислове значення; безпосередньо пов’язана з технологічними процесами та/або наданням послуг, критичних для економіки та промисловості, функціонування суспільства та безпеки населення. Зупинка функціонування або виникнення збоїв роботи цих підприємств має негативний вплив на національну безпеку та обороноздатність української держави, навколишнє природне середовище; створює економічну шкоду або загрожує життю і здоров’ю людей [4].

Вимоги до реєстрації подій на об’єктах критичної інфраструктури у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518

“Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”.

У системі об’єктів критичної інфраструктури повинна здійснюватися обов'язкова реєстрація щонайменше про такі події:

- доступ та будь-які дії з інформацією що оброблюється на об’єкті критичної інфраструктури;
- зміни прав доступу до служб та функцій;
- активності акаунтів користувачів та адміністраторів(вхід, вихід, зміна пароля, перевищення кількості спроб введення пароля);
- налаштування програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури;
- створення, блокування, видалення, зміна конфігурації облікових записів, як користувачів так і адміністраторів.
- зміни конфігурації та налаштувань на об'єкті ІТ інфраструктури;
- про спроби несанкціонованого доступу користувачів до інформаційних ресурсів;
- негативні результати перевірок цілісності журналів реєстрації подій, програмного та апаратного забезпечення;
- налаштування параметрів реєстрації та дії з журналами подій.

Під час роботи системи моніторингу повинні виконуватися наступні правила:

- журнали реєстрації подій мають містити дані про місце, дату, час, тип і успішність/неуспішність кожної події;
- повинно бути забезпечення захисту журналів реєстрації подій від модифікацій та доступу користувачів без необхідних прав.
- система моніторингу повинна реєструвати події як програмного так і апаратного забезпечення на об’єктах ІТ інфраструктури. Вона має

надавати можливість фільтрування журналів реєстрації подій за різними критеріями;

- оброблення журналів реєстрації подій не повинно впливати на функціонування критичних бізнес/операційних процесів об’єкта критичної інфраструктури;
- повинна бути можливість зчитувати дані з архівних журналів реєстрації подій, при цьому сам архів може бути завантажено із фізично відокремленого джерела;
- архівовані журнали реєстрації подій повинні зберігатися на фізичному носію або фізично відокремлених вузлах ІТ інфраструктури, не менш як рік з дати їх утворення [5].

1.2 Аудит інформаційної безпеки

Аудит інформаційної безпеки – системний процес отримання даних аудиту, необхідних для подальшого проведення об’єктивної якісної і кількісної оцінки рівня забезпечення безпеки інформаційної системи відповідно до визначених критеріїв та показників безпеки.

Дані аудиту – інформація зібрана під час роботи інформаційної системи, перелік фактів та інші дані.

Метою аудиту безпеки є:

- знаходження слабких місць у системі захисту ІС;
- надання оцінки рівню захищеності ІС;
- детальний аналіз загроз, які можуть спричинити виникнення ризиків інформаційної безпеки у відношенні до ресурсів ІС;
- перевірка на відповідність галузевим стандартам;
- розробка рекомендацій щодо модернізації існуючих та створення нових рекомендацій механізмів безпеки.

Види аудиту ІБ:

- експертний аудит ІБ, проводиться шляхом залучення експертів для оцінки і знаходження недоліків засобів захисту.
- активний аудит, оперативний аудит головною метою якого є виявлення підозрілої активності та проведення заходів автоматичного реагування. Підозрілою активністю може бути як порушення користувачем політики інформаційної безпеки, нетипові дії з системою, підозріла активність.
- аудит ІБ перевірки на відповідність міжнародним стандартам;
- комплексний аудит, охоплює всі перераховані вище варіанти проведення діагностики.

Таким чином, будь-якій організації, котрій необхідно забезпечити інформаційну безпеку в інформаційній системі, слід розв’язати проблему інформування, виявлення та ведення обліку системних подій. Це потрібно як для забезпечення можливості проведення аудиту ІБ ,так і для здійснення оперативного реагування на події інформаційної безпеки .

Для обробки системних подій ІТ інфраструктури зазвичай використовуються системи моніторингу, які ведуть облік подій критичних компонентів. Які саме події потрібно відстежувати повинно бути формалізовано у політиці інформаційної безпеки організації, залежно від особливостей ІТ інфраструктури та бізнес-процесів конкретної організації.

1.3 Система моніторингу

Система моніторингу – це комплекс технологій, програмних та апаратних засобів, головною метою яких є забезпечення неперервного спостереження та збору інформації в локальній мережі. Зібрана інформація використовується для виявлення некоректної роботи вузлів мережі або інцидентів безпеки і оповіщення відповідних осіб.

Політика інформаційної безпеки(ПІБ) – набір правил, рекомендацій, вимог та обмежень які регламентують процес супроводження і функціонування бізнес-процесів

Метою ПІБ має бути впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на:

- захист інформаційних активів;
- стабільне функціонування організації;
- зведення ризиків інформаційної безпеки до мінімуму;
- створення позитивних бізнес відносин.

Основним завданням інформаційної безпеки є захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз.

Отже, ПІБ регулює які саме системні події (під системною подією слід розуміти записи котрі були збережені у лог-файлах об’єктів критичної інфраструктури) слід реєструвати системі моніторингу для подальшого проведення аудиту ІБ.

1.4 Огляд чинних програмних рішень

Вимоги описані у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”[5] визначають мінімальні організаційно-методологічні, технічні та технологічні вимоги до кіберзахисту об’єктів критичної інфраструктури. На практиці реалізації цих вимог повинні реалізовувати системні адміністратори.

Під час роботи інформаційної системи операційні системи що є її складовою реєструють події відповідно до своїх налаштувань у журналі подій.

У операційній системі Windows подією називається будь-яка значна подія в роботі системи або прикладної програми, про які варто повідомити користувачів. реєструються в системних журналах подій. Туди реєструються як події що виникли у прикладних програмах, так і записи пов’язані з безпекою та роботою системи. Якщо цього не достатньо для забезпечення виконання вимог локальної політики безпеки підприємства, відповідальним особам потрібно розробити власну систему легування та інтегрувати її до системи моніторингу.

Завдання системи моніторингу вести єдиний журнал аудиту для всієї інфраструктури, ПІБ регулює список події які необхідно реєструвати. Треба розуміти що найчастіше система моніторингу оперує саме подіями які були зареєстровані на компонентах IT інфраструктури. Невпинний розвиток мережевих та інформаційних технологій сприяє стрімкому розвитку систем моніторингу IT інфраструктури, розглянемо найбільш поширені рішення:

1.4.1 Zabbix

Zabbix – це програмне забезпечення, яке відстежує численні параметри IT інфраструктури. Zabbix надає гнучку систему сповіщень електронною поштою або іншими засобами сповіщення, як реакцію на виникнення інцидентів безпеки, яка надає широкий спектр можливостей у налаштуванні сповіщень електронною поштою. Це дозволяє реагувати на інциденти інформаційної безпеки сервера.

Також Zabbix надає функції візуалізації даних на основі збережених даних, це допомагає при огляді навантаження на апаратні ресурси. Доступ до всіх звітів і статистики Zabbix, а також до параметрів конфігурації здійснюється через вебінтерфейс. Вебінтерфейс гарантує, що дізнатися про стан мережі та працездатність серверів можна оцінити віддалено.

При належному налаштуванні Zabbix стає найважливішим компонентом моніторингу IT-інфраструктури. Це однаково справедливо як для невеликих компаній з кількома серверами, так і для великих компаній з великою з великою IT інфраструктурою. Zabbix є безкоштовним, написаний і розповсюджується під GPL (General Public License версії).

Функціонал Zabbix:

- автоматичне виявлення серверів і мережевих пристроїв;
- розподілений моніторинг із централізованим WEB адмініструванням;
- підтримка механізмів опитування та захоплення серверне програмне забезпечення для Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD;
- власні високопродуктивні агенти повідомлення електронною поштою про попередньо визначені події високорівневий огляд ресурсів, що відстежуються ведення журналу аудиту [6].

Саме Zabbix буде обрано для впровадження систему моніторингу через гнучку систему налаштування та можливість інтеграції з іншими системами моніторингу та лог-аналізу.

1.4.2 Nagios

Nagios – це інструмент безперервного моніторингу з відкритим вихідним кодом, який контролює мережу, програми та сервери. Він може знаходити та виправляти проблеми, виявлені в інфраструктурі, і усувати майбутні проблеми, перш ніж вони вплинуть на кінцевих користувачів. Це підвищує продуктивність IT-інфраструктури.

Nagios пропонує наступні функції:

- може контролювати сервери баз даних, такі як SQL Server, Oracle;
- надає інформацію на рівні програми (Apache, Postfix, LDAP, Citrix тощо). Забезпечує активний розвиток;
- має чудову підтримку від величезної активної спільноти. Nagios працює на будь-якій операційній системі;
- виявляє проблеми сервера та мережі;
- знаходить першопричину збою;
- може автоматично розв'язувати проблеми при виявленні. Це гарантує, що сервери, служби, програми, мережа завжди доступні і працюють.
- контролює всю інфраструктуру щосекунди [7].

1.4.3 ELK stack

ELK Stack – це пакет технологій з відкритим кодом для збору, пошуку, аналізу та візуалізації великих обсягів даних, створених різними джерелами. Спочатку стек включав лише Elasticsearch, Logstash та Kibana. Але в 2015 році Elastic додала ще одну технологію з відкритим кодом: Beats.

Elasticsearch - це сучасна система повнотекстового пошуку та аналітики з відкритим вихідним кодом. Серце стека ELK, Elasticsearch, можна використовувати для пошуку повного масиву типів даних від тексту і чисел до інших типів структурованих і неструктурованих даних.

Logstash це конвеєр обробки даних на стороні сервера з відкритим вихідним кодом, який динамічно поглинає дані, перетворює їх і відправляє їх у будь-яке місце (або «схованку»), яке ви визначаєте.

Kibana це інструмент для аналізу та візуалізації даних з відкритим вихідним кодом, який перетворює дані, що зберігаються в Elasticsearch, у легко споживані діаграми, графіки, гістограми та інші візуальні уявлення [8].

1.4.4 Graylog

Graylog – платформа з відкритим вихідним кодом надає програмне забезпечення для керування журналами. Graylog є одним із прикладів централізованої платформи керування журналами подій. Graylog може приймати багато терабайтів журналів щодня, а його вебінтерфейс дозволяє IT-адміністраторам ефективно сортувати та шукати всі ці дані.

Головні переваги і особливості Graylog:

- зберігає дані у базі даних MongoDB;
- агрегація повідомлень в потоки;
- можливість об’єднати хости до однієї групи; [9]

2. ЗАСОБИ РЕЄСТРАЦІЇ ТА АНАЛІЗУ ПОДІЙ

2.1 Аудит безпеки Windows

Аудит безпеки Windows – це функція Windows, яка допомагає підтримувати безпеку на комп'ютері та в корпоративних мережах. Аудит Windows призначений для моніторингу активності користувачів, проведення аналізу та розслідування інцидентів безпеки, а також усунення загроз. Аудит безпеки дозволяє впроваджувати політику безпеки у вашому середовищі для виконання корпоративних, державних або промислових вимог.

Аудит безпеки є одним з найпотужніших інструментів, які надає операційна система Windows для підтримки цілісності системи. Аудит безпеки Windows можна ввімкнути за допомогою групової політики (у середовищі Active Directory) або локальної політики безпеки (для одного комп'ютера). Відкрийте панель керування Windows, виберіть «Інструменти адміністрування», а потім запустіть «Локальна політика безпеки». Відкрийте гілку «Локальні політики» та виберіть «Політика аудиту». На правій панелі вікна локальної політики безпеки ви побачите список політик аудиту (дивитися рисунок 2.1).

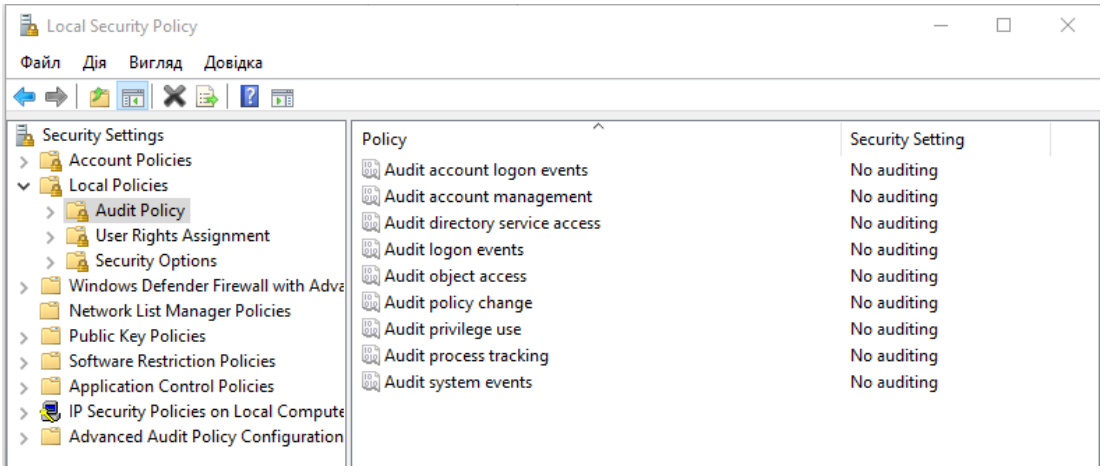

Рисунок 2.1 — Налаштування політики аудиту

Політику аудиту слід розглядати як частину загальної стратегії безпеки, рівень аудиту визначається окремо для кожного середовища. Аудит повинен виявляти атаки (успішні чи ні), які становлять загрозу для IT інфраструктури, і атаки на ресурси, які були визначені цінними під час оцінки ризиків.

2.2 Розширені налаштування політики аудиту системи

Саме налаштування політики аудиту будуть визначати які події будуть занесені до журналів подій. Розширені налаштування політики аудиту безпеки, доступні в операційних системах Windows, починаючи з Windows Server 2008 R2 і Windows 7, розглянемо принцип їх роботи.

Усього 53 параметри політики аудиту безпеки можуть допомогти організації перевірити відповідність важливих правил, пов’язаних з бізнес-процесами та безпекою, відстежуючи точно визначені дії, такі як:

Адміністратор групи змінив налаштування або дані на серверах.

Співробітник у визначеній групі отримав доступ до важливого файлу.

Правильний список контролю доступу до системи (SACL) застосовується до кожного файлу, теки чи розділу реєстру на комп’ютері як надійний захист від невиявленого доступу.

Ці 53 параметри дозволяють вибрати лише ту поведінку(виражену у списку реєстру подій), яку потрібно відстежувати, і виключити результати аудиту для поведінки, яка мало цікавить або взагалі не стосується ПІБ. Крім того, оскільки політику аудиту безпеки Windows 7 і Windows Server 2008 R2 можна застосовувати за допомогою групової політики домену, параметри політики аудиту можна змінювати, тестувати та розгортати для вибраних користувачів і груп із відносною простотою. Параметри політики конфігурація політики аудиту доступні в таких категоріях(дивитися Додаток А).

2.3 **Журнали подій Windows**

Журнали подій ОС Windows використовуються додатками та операційною системою для запису даних важливих апаратних і програмних подій і їх подальшого зберігання. Існують наступні види журналів:

- Application – містить події, зареєстровані програмами. Наприклад, програма бази даних може записати помилку файлу. Розробник програми вирішує, які події записувати.;
- Security – містить події недійсних та дійсних спроб входу, а також події, пов'язані з використанням системних ресурсів, наприклад видаленням, переміщенням або відкриттям файлів чи інших об’єктів. Адміністратор може розпочати аудит для запису подій у журналі безпеки;
- System – для подій драйверів пристроїв.
- CustomLog – особистий журнал програми що містить події, зареєстровані програмою власником. Використання власного журналу дозволяє програмі контролювати розмір журналу або додавати списки керування доступом з метою безпеки, не впливаючи на інші програми.[10]

Додатки та компоненти операційної системи використовуючи програмний інтерфейс (API) використовують цю централізовану службу журналів для запису виконаних операцій. Події з усіх джерел зберігаються в єдиному журналі подій службою журналів подій, звідки користувач за допомогою програми перегляду подій може знайти потрібні йому дані, додаткам теж дозволено переглядати та додавати нові записи. Запис про подію охоплює такі дані:

- ідентифікатор події;
- тип події.(дивитися таблиця 2.1);
- категорію події;
- масив рядків;

- двійкові дані.

Для кожного джерела подій існує свій файл-повідомлення, він складається з опису ідентифікатору повідомлення, параметру і категорії. Для визначення унікально ідентифікованих подій, з якими може зіткнутися комп'ютер на базі ОС Windows, система використовує eventID.

Таблиця 2.1 Типи подій

Тип події	Опис події
Успішний аудит	Події безпеки, які генеруються якщо був встановлено успішне звернення до ресурсів, аудит яких здійснюється відповідно до налаштувань локальної політики аудиту. Наприклад успішний вихід користувача або успішне видалення файлу.
Не успішний аудит	Події безпеки, які генеруються якщо був встановлено успішне звернення до ресурсів, аудит яких здійснюється відповідно до налаштувань локальної політики аудиту. Наприклад неуспішний вхід користувача.
Помилка	Події, які генеруються якщо зафіксована некоректна подія що ймовірно призведе до втрати даних або спричинить припинення функціонування частини системи. Наприклад збій роботи драйверів.
Попередження	Даний тип події вказує на відсутність необхідності негайного втручання, але ігнорування проблеми може призвести до появи помилок та збоїв. Наприклад переповнення жорсткого диску.
Інформація	Даний тип події вказує на успішне проведення важливих і рідкісних операцій.

2.4 Структура Zabbix

Архітектура системи моніторингу Zabbix має дві найважливіші частини це агент та сервер. Сервер Zabbix є центральним процесом програмного забезпечення Zabbix. Сервер здійснює опитування та перехоплення даних, він розраховує тригери, надсилає сповіщення користувачам. Це центральний компонент, якому агенти та проксі Zabbix повідомляють дані про доступність та цілісність систем. Сервер може сам віддалено перевіряти мережеві служби (наприклад, веб-сервери та поштові сервери) за допомогою простих перевірок.

Сервер – це центральне сховище, в якому зберігаються всі конфігураційні, статистичні та операційні дані, і це об’єкт у Zabbix, який буде активно сповіщати адміністраторів, коли виникають проблеми в будь-якій із систем, що контролюються. Функціонування базового сервера Zabbix розбивається на три окремі компоненти; це:

- сервер Zabbix;
- веб-інтерфейс;
- сховище бази даних.

Сервер Zabbix надсилає запит на отримання даних, наприклад, про навантаження ЦП, а отримані дані від агенту зберігає в базі даних.

Режим активної перевірки або моніторинг у реальному часі працює інакше. Спочатку агент повинен отримати список елементів, які підлягають активному моніторингу, від сервера Zabbix для. Потім агент через визначені на сервері проміжки часу буде надсилати нові дані.

Виконання пасивних чи активних перевірок налаштовується шляхом вибору відповідного типу елемента моніторингу. Zabbix агент обробляє елементи типу 'Zabbix agent' або 'Zabbix agent (active)

Вся інформація про конфігурацію Zabbix зберігається в базі даних, з якою взаємодіють як сервер, так і веб-інтерфейс. Наприклад, коли ви створюєте новий

елемент за допомогою веб-інтерфейсу (або API), він додається до таблиці елементів у базі даних. Потім приблизно раз на хвилину сервер Zabbix буде запитувати в таблиці елементів список активних елементів, який потім зберігатиметься в кеші на сервері Zabbix

Агент Zabbix розгортається на цілі моніторингу для активного моніторингу локальних ресурсів і програм (жорсткі диски, пам'ять, статистика процесора тощо). Агент збирає дані на клієнті та передає зібрану інформацію на сервер Zabbix для подальшої обробки. У разі збоїв (наприклад, переповнений жорсткий диск або аварійний процес обслуговування) сервер Zabbix може активно сповіщати адміністраторів конкретної машини, яка повідомила про збій.

Агенти Zabbix надзвичайно ефективні завдяки використанню вбудованих системних викликів для збору статистичної інформації. Пасивні та активні перевірки агенти Zabbix можуть виконувати пасивні та активні перевірки. При пасивній перевірці агент відповідає після того, як сервер відправить запит агенту [7].

3. ВПРОВАДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ ZABBIX

Проаналізувавши наведені вище вимоги до реєстрації подій на об’єктах критичної інфраструктури у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”[2], було сформовано список перелік аудитів подій котрі повинна проводити система моніторингу незалежно від архітектури IT інфраструктури та політики безпеки організації:

- Аудит управління обліковими записами
- Аудит доступу до об’єктів файлової системи
- Аудит цілісності системи

3.1 Аудит управління обліковими записами

Для того, щоб система Windows зареєструвала події входу/виходу користувачів в журналі подій, потрібно ввімкнути відповідні параметри аудиту системи (дивитися рисунок 3.1):

Audit Credential Validation визначає, чи генерує операційна система події аудиту для облікових даних, які надсилаються для запиту входу в обліковий запис користувача. Ці події відбуваються на комп’ютері, який є авторитетним для облікових даних(для локальних облікових записів локальний комп’ютер є авторитетним)

Audit Kerberos Authentication Service визначає, чи потрібно генерувати події автентифікації для запитів на надання квитків аутентифікації Kerberos (TGT).Якщо ви налаштуєте цей параметр політики, подія аудиту генерується після запиту TGT аутентифікації Kerberos. Аудит успіху реєструє успішні спроби, а аудит невдач невдалі спроби.

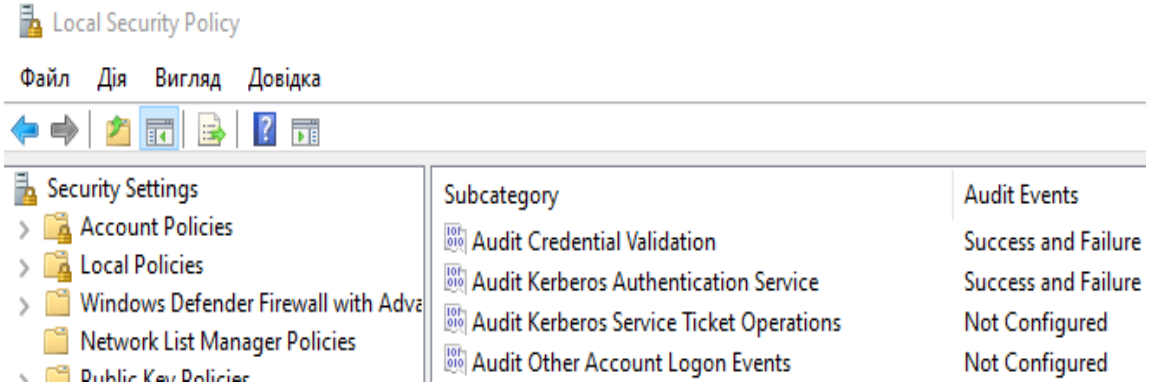

Рисунок 3.1 — Політики аудиту для реєстрації подій входу/виходу облікових записів користувачів

Для реєстрації подій видалення, блокування та реєстрації облікових записів користувача, необхідно ввімкнути під категорії Audit Computer Account Management та Audit User Account Management (дивитися рисунок 3.2):

Audit Computer Account Management визначає, чи генерує операційна система події аудиту, коли обліковий запис комп'ютера створюється, змінюється або видаляється. Цей параметр політики корисний для відстеження змін, пов'язаних з обліковими записами, на комп'ютерах, які входять до домену.

Audit User Account Management дозволяє перевіряти зміни в облікових записах користувачів. Події включають наступне:

- обліковий запис користувача створюється, змінюється, видаляється, перейменовується, вимкнено, увімкнено, заблоковано або розблоковано;
- пароль облікового запису користувача встановлено або змінено;
- ідентифікатор безпеки (SID) додається до історії SID облікового запису користувача або його не додається;
- пароль режиму відновлення служб каталогів налаштовано;
- дозволи для облікових записів адміністраторів змінено;
- було перераховано членство користувача в локальній групі;
- облікові дані диспетчера облікових даних створено або відновлено.

Нижче описані eventID подій які мають реєструватися виконання аудиту облікових записів.(дивитися додаток Б).

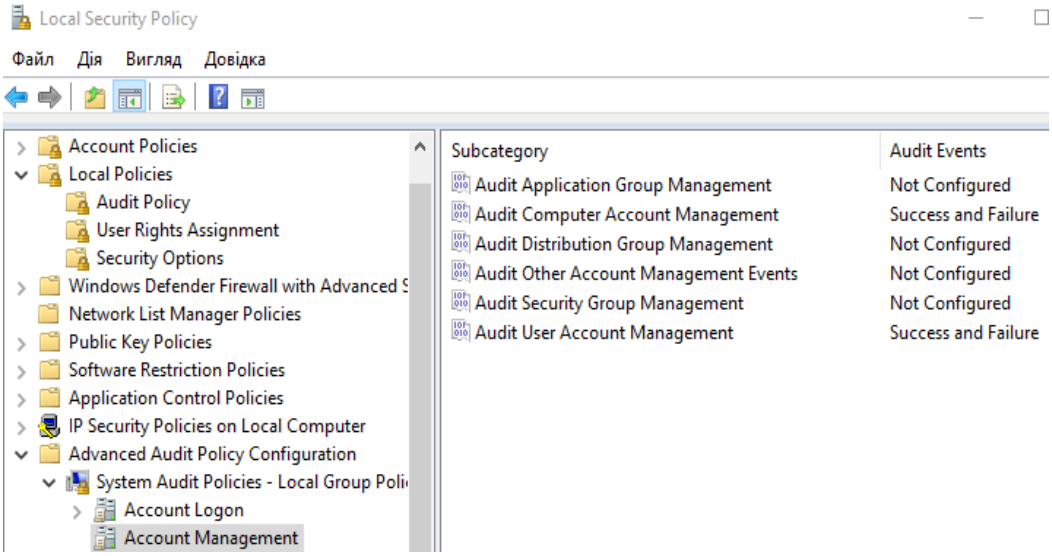

Рисунок 3.2 — Політика аудиту для реєстрації подій видалення та створення облікових записів користувачів.

3.2 Аудит доступу до об’єктів файлової системи

Щоб забезпечити проведення аудиту доступу до об’єктів файлової системи, система моніторингу повинна реєструвати події які пов'язані з читанням, модифікацією, створенням або видаленням об’єктів файлової системи(дивитися таблицю 3.1). Потрібно ввімкнути параметр Audit File System(дивитися рисунок 3.3). Потрібні події аудиту будуть генеруватися для об’єктів, які мають налаштовані списки керування доступом до системи (SACL), і лише якщо тип запитуваного доступу (наприклад, запис, читання чи зміна) та обліковий запис, що робить запит, відповідають параметрам встановленим у SACL.

Список контролю доступу до системи (SACL) це традиційний механізм делегування подій, який визначає, як перевіряється доступ до файлів і тек. Він не може обмежувати доступ до файлів і тек.

SACL використовуються для встановлення загальносистемних політик безпеки для таких дій, як ведення журналів або аудит доступу до ресурсів. SACL закріплений до системи, каталогу або файлу Які принципали безпеки (користувачі, групи, комп'ютери) слід перевіряти під час доступу до об'єкта Які події доступу слід перевіряти для цих принципалів Чи створюється атрибут успіху чи невдачі для події доступу, залежно від дозволів, наданих у DACL(списку виборчого управління доступом) об'єкта.

Зазвичай список керування доступом налаштовують до критичних об'єктів файлової системи. Попри те що генерувати події політики аудиту Audit File System можна для всієї системи, на практиці генерується надто багато подій що значно збільшує необхідні ресурси для зберігання та ведення журналів подій.

Таблиця 3.1 Події роботи з файловою системою

ID	Опис
4656	Ідентифікує початок роботи з файлом
4663	Ідентифікує виконану операцію над об’єктом
4660	Ідентифікує операцію видалення
4658	Ідентифікує кінець роботи з файлом
4670	Режим контролю доступу було змінено

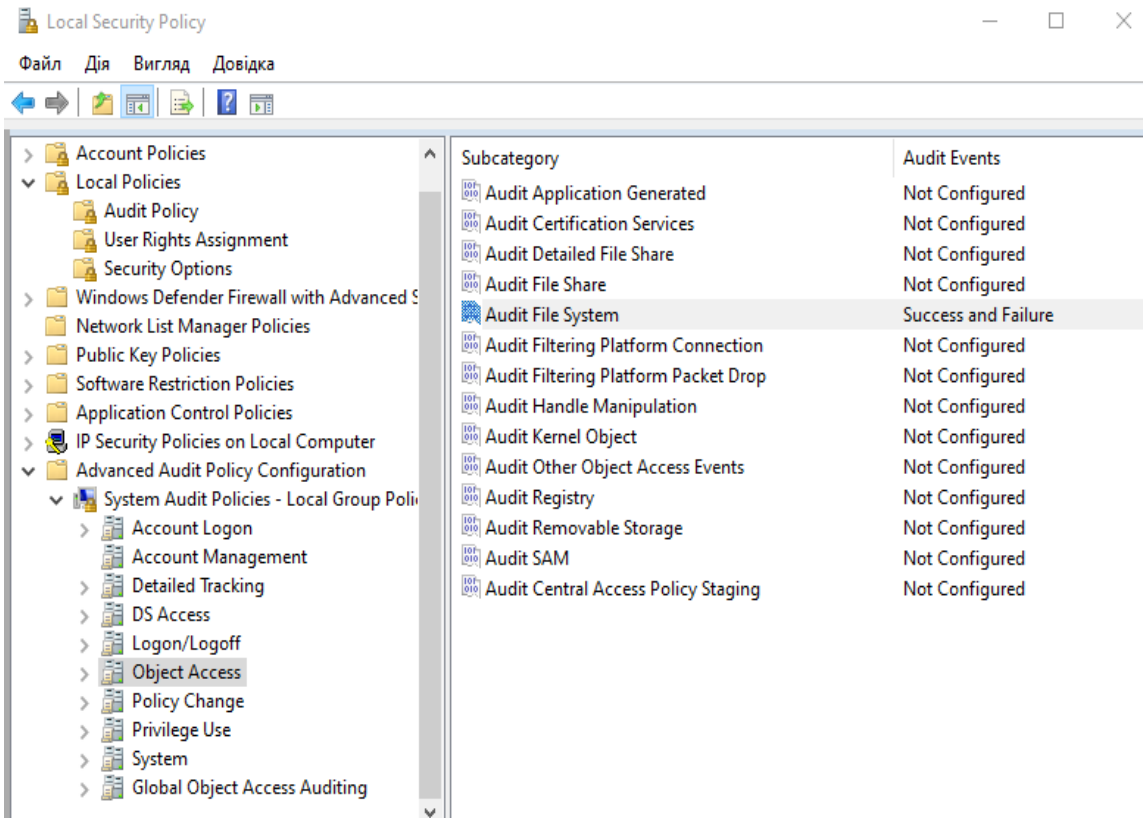

Рисунок 3.3 — Політика аудиту для реєстрації подій доступу до об’єктів файлової системи.

3.3 Аудит цілісності системи

Щоб забезпечити перевірку цілісності даних та програмного забезпечення можна використовувати параметр Audit System Integrity(дивитися рисунок 3.4). Audit System Integrity визначає, чи перевіряє операційна система події, які порушують цілісність підсистеми безпеки. До дій, які порушують цілісність підсистеми безпеки, належать(дивитися 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.

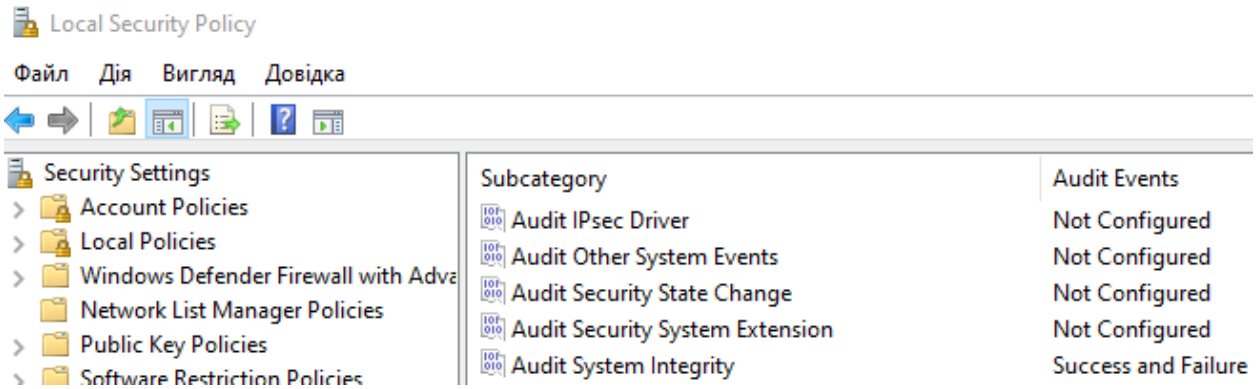

Рисунок — 3.4 Політика аудиту для перевірки цілісності системи

Таблиця 3.2 Події що входять до Audit System Integrity

EventID	Опис
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	Криптографічна операція.
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 численних параметрів мережі, а також працездатності та цілісності серверів, віртуальних машин, додатків, служб, баз даних, веб сайтів, хмари тощо. Zabbix використовує гнучкий механізм сповіщень, який сповіщає користувачів про проблеми через ряд платформ, таких як електронна пошта, Slack, Jira, Brevis.one тощо.

Однією з його основних переваг є те, що це програмне забезпечення з відкритим вихідним кодом, що означає, що воно є абсолютно безкоштовним і також поставляється разом із можливістю візуалізації даних.

Сервер Zabbix збирає дані від усіх своїх агентів, аналізує та дає належне представлення даних. Він також забезпечує настроюваний і простий спосіб інтерпретації вебінтерфейсу / інформаційної панелі з різними графіками, мережевими картами, слайд-шоу та звітами(дивитися рисунок 3.5).

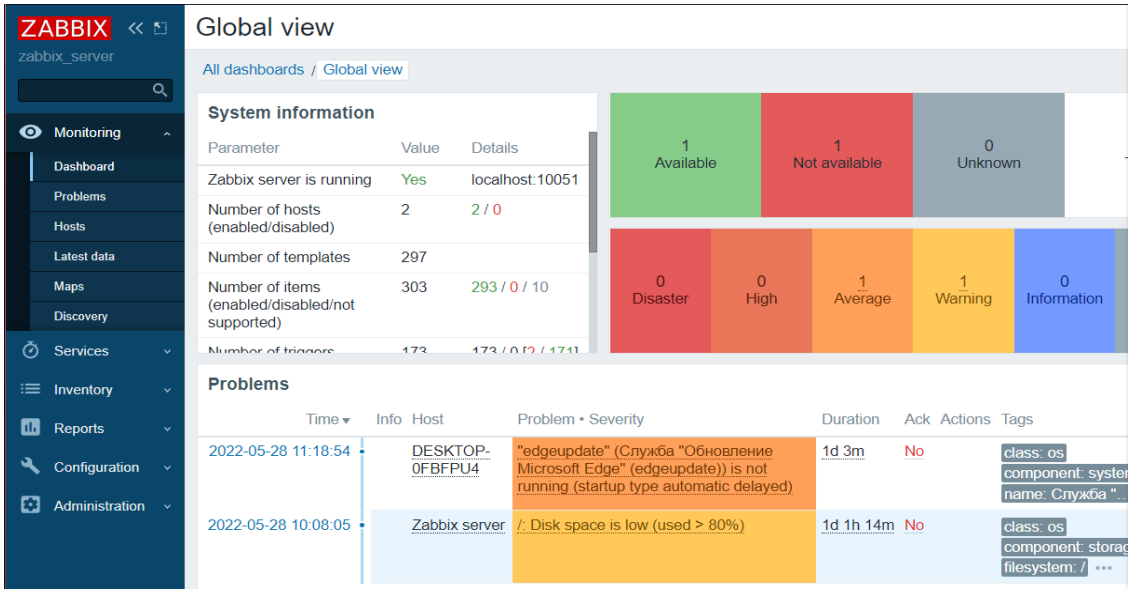

Рисунок — 3.5 Web-інтерфейс Zabbix

З точки зору користувача Zabbix ділиться на дві великі частини: сервер і агенти. Сервер розташовується на одній машині, яка збирає і зберігає статистичні дані, а агенти на тих машинах збирають дані, для їх подальшого відправлення на сервер.

Відповідно до вимог перелічених у пунктах 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури” на Zabbix сервері ведеться збір даних аудиту з доданих хостів.(дивитися рисунок 3.6)

Записи подій містять інформацію про дату та час реєстрації події, тип і ступінь успішності. Там детально описані такі подробиці, як ім'я користувача, назва системи, ідентифікатор процесу і мережевого об’єкта.

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.(дивитися рисунки 3.7, 3.8)

Збереження результатів моніторингу об’єктів IT інфраструктури відбувається у базі даних сервера Zabbix, для архівування даних моніторингу слід зробити дамп бази даних на окремий носій інформації.

За наявності елементів, які збирають дані, і тригерів, що переходять у стан "Проблема" при виняткових ситуаціях, корисно мати механізм оповіщення, який буде повідомляти про важливі події, тоді коли ми не можемо дивитися безпосередньо у вебінтерфейс.

Email оповіщення є найбільш популярним способом відправлення повідомлень. Тому налаштовувати будемо саме їх. Для цього, перейдемо до панелі *Administration – Media Types* та виберемо *Email* у списку попередньо встановлених способів сповіщень.(дивитися рисунок 3.9)

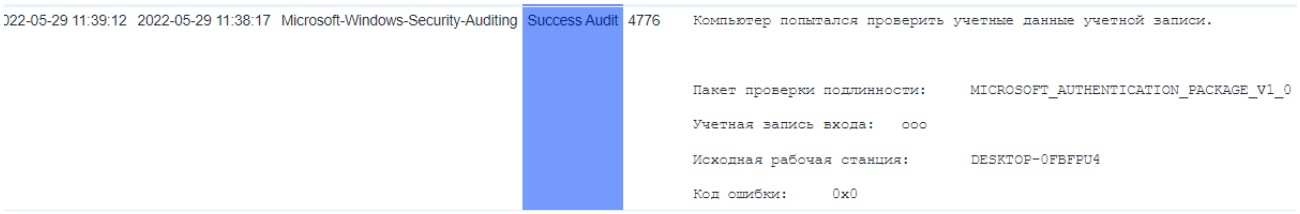

Рисунок 3.6 — Запис даних аудиту з хостів Zabbix

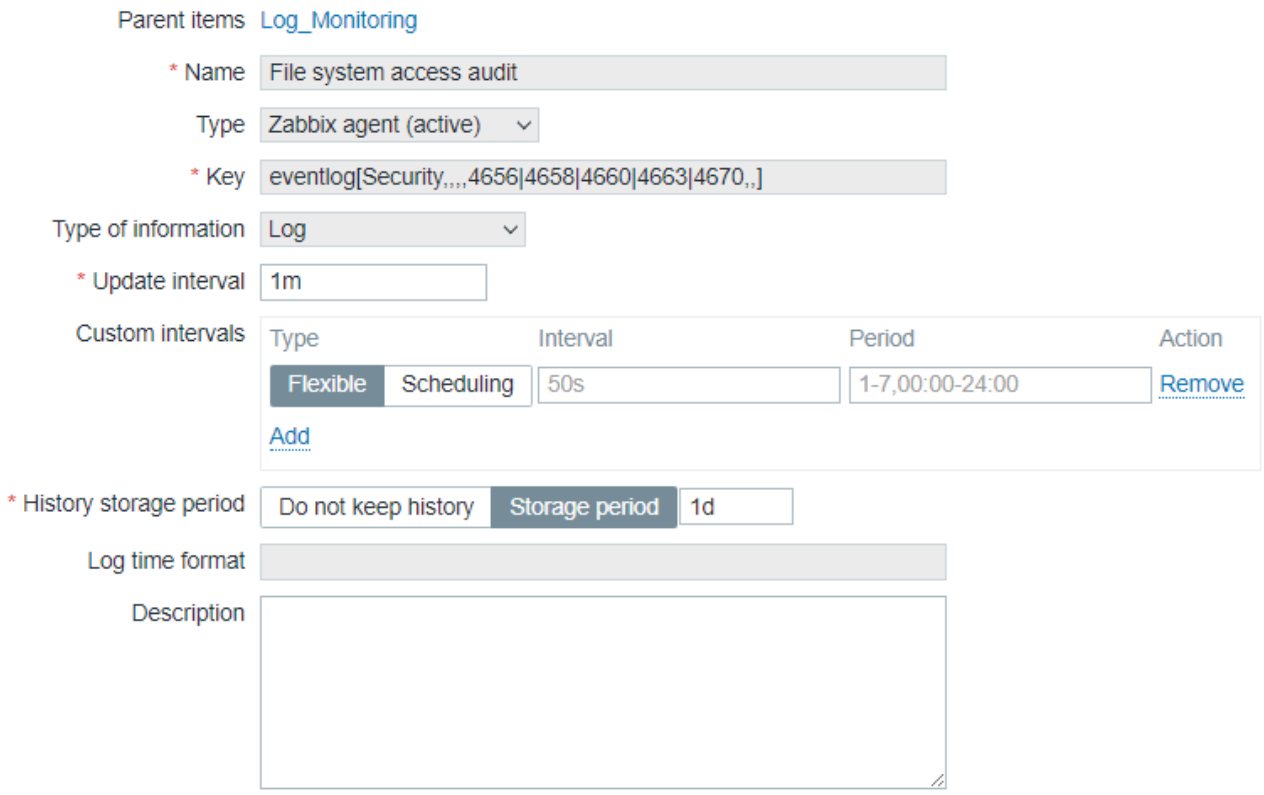

Рисунок 3.7 — Створення шаблону моніторингу

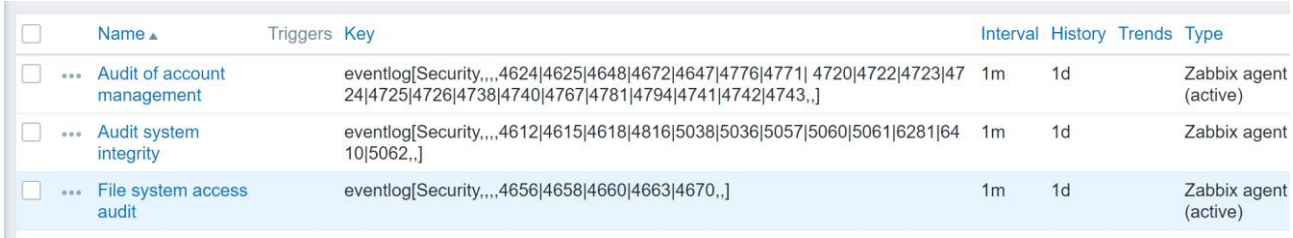

Рисунок 3.8 — Список шаблонів моніторингу

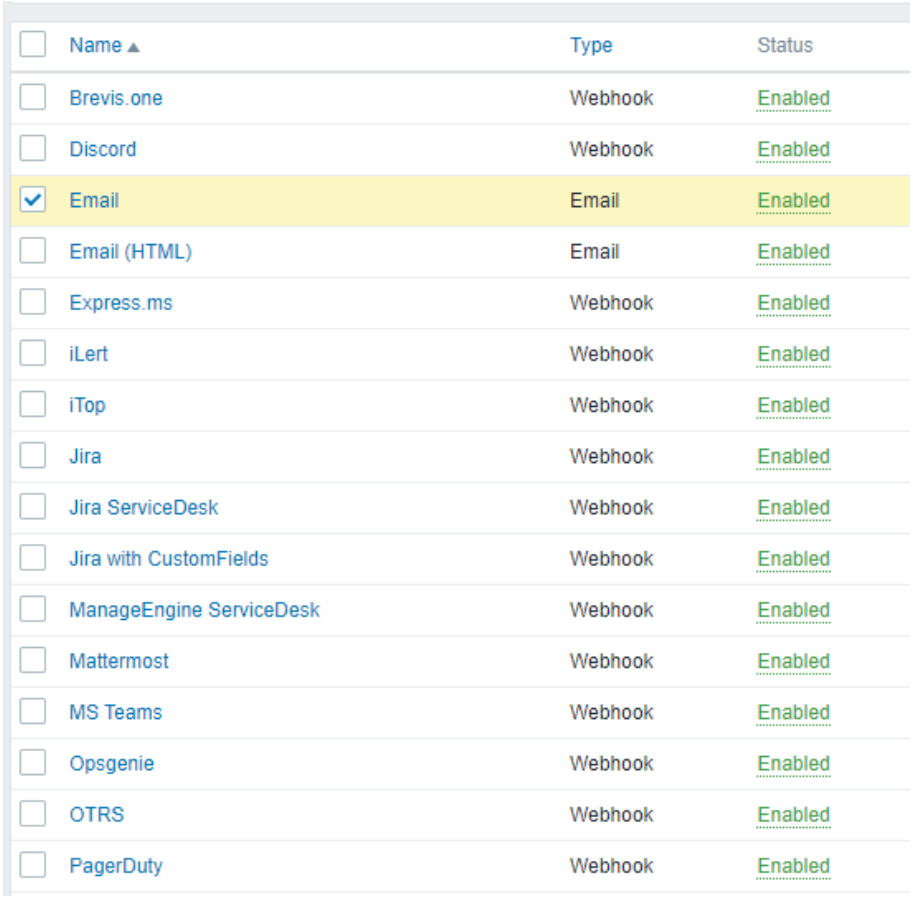

Рисунок 3.9 — Список варіантів сповіщення

Zabbix надає змогу вибрати більшість чинних медіа та соціальних сервісів, або під'єднати власний за допомогою опції *Create Media Type*. Zabbix забезпечує повний робочий процес: відправлення оповіщень, можливість підтвердження отриманої інформації, пересилання іншим особам та можливість застосування дій. Натиснемо на Email для виклику вікна налаштувань. У графі *SMTP email* введемо адресу відправника повідомлень та налаштування мережевих протоколів. Збережемо зміни.(дивитися рисунок 3.10)

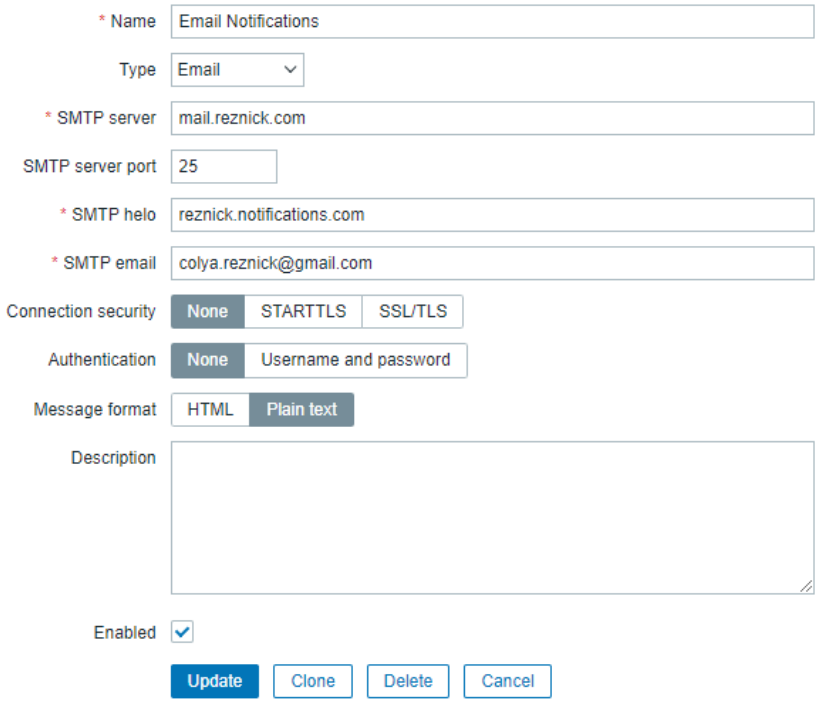

Рисунок 3.10 — Список варіантів сповіщення

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.

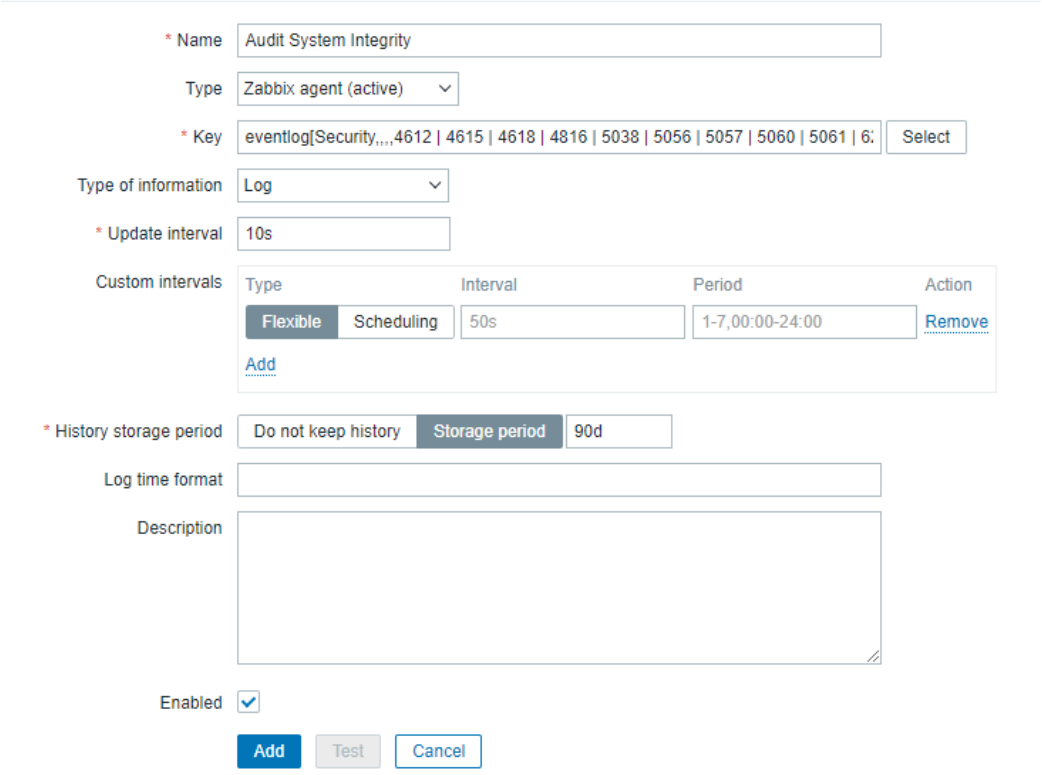

Рисунок 3.11 — Фільтр подій для *Audit System Integrity*

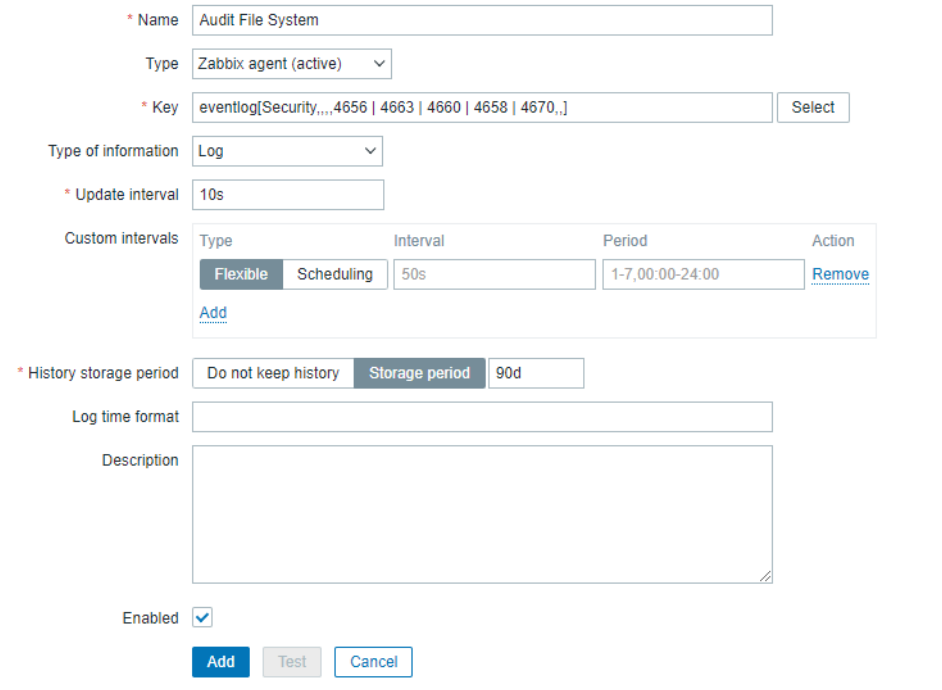

Рисунок 3.12 — Фільтр подій для *Audit File* System

Налаштуємо повідомлення у вебінтерфейсі та рівень логування даної інформації. Для цього перейдемо на панель *Triggers – Create Trigger* та додамо умову настання виняткової ситуації (дивитися рисунок 3.13). Виберемо рівень серйозності даного повідомлення, як “Попередження” та умову – одне чи більше спрацювання шуканих ідентифікаторів подій персонального комп’ютера. Аналогічно повторимо для двох інших груп.

На додачу, у цьому меню ми можемо виставити 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 *Configuration – Action – Trigger Action,* де ми можемо додати групу (чи декілька) користувачів, що отримають повідомлення про помилку чи попередження.

Для наочності налаштуємо сповіщення про помилки для адміністраторів на електронну пошту. Натиснемо *Create Action,* введемо ім’я, умову та додамо групу користувачів, що будуть отримувати сповіщення. (дивитися рисунок 3.14)

Створити чи відредагувати групу користувачів можливо у меню Administration – *User Groups/User Roles/Users*.//забезпечує активний аудит (пункт1.2)

Таким чином системи моніторингу Zabbix реалізує визначенні аудит управління обліковими, записами аудит, доступу об'єктів до файлової системи та аудит цілісності системи, та проведення активного аудиту 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 р. №518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”[5].

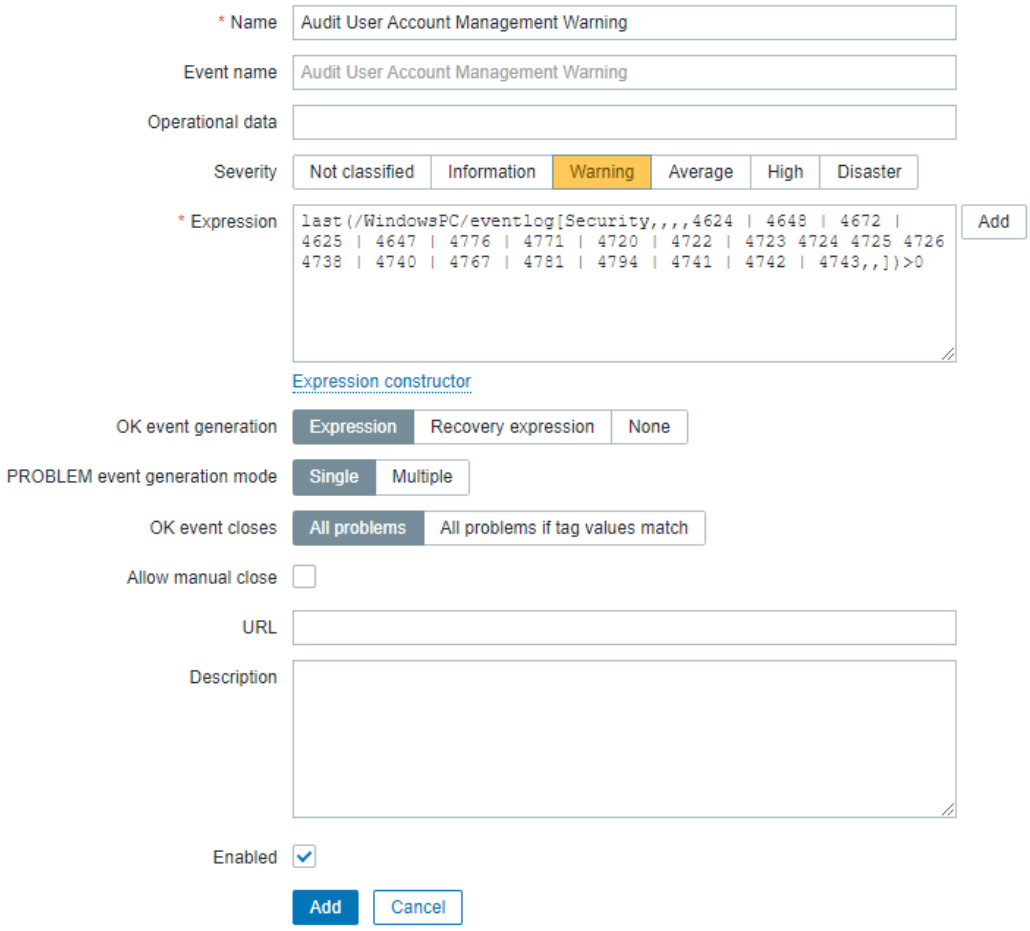

Рисунок 3.13 — Умова активації тригеру

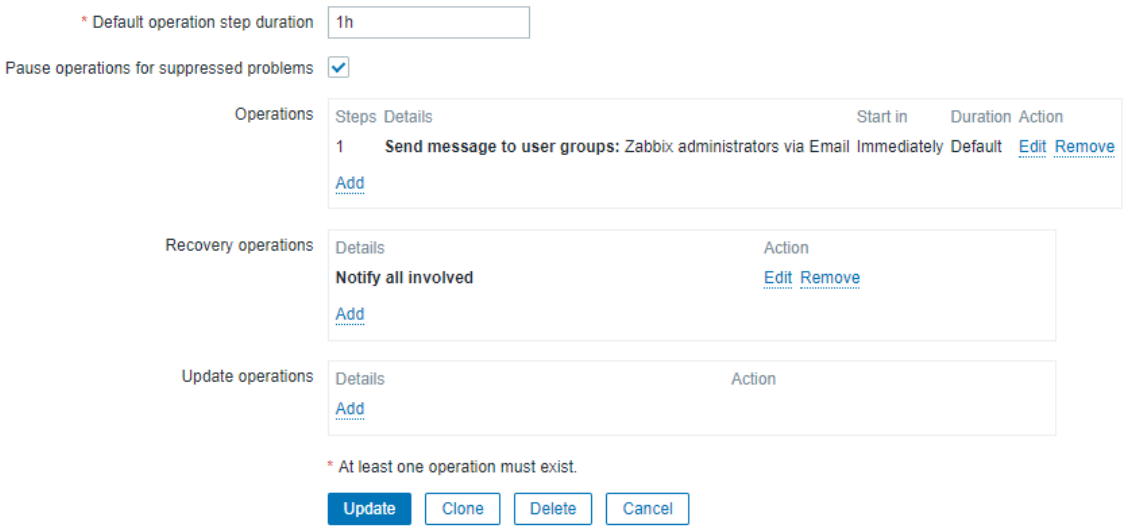

Рисунок 3.14 — Встановлення групи отримувачів email листа

ВИСНОВОК

Дана робота розглядає практичні проблеми при використанні системи моніторингу для реєстрації, зберігання та аналізу подій безпеки, для державних підприємств. Завдяки їй є можливим провести аудит інформаційної безпеки, це життєво необхідно на об’єктах критичної інфраструктури, оскільки вірно налаштована система моніторингу журналів подій надає змогу швидко та ефективно усувати проблеми що виникають. Розглядаються мінімальні вимоги українського законодавства до реєстрації подій в системі, та запропоновано налаштування політики аудиту відповідно до пунктів 19-23 Постанови Кабінету Міністрів України від 19 червня 2019 р. №518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”[5].

У локальній мережі було протестоване програмне рішення компанії Zabbix для моніторингу мережі та ведення журналів аудити. Сервер був встановлений на Ubuntu v18.04.01, база даних MySQL, агенти було встановлено на КС з операційною системою Windows. Також описано функціонал встановленого рішення для моніторингу мережі та журналів аудиту. Потрібно відзначити ,що розібраний список політик аудиту та подій, що підлягають реєстрації, можуть змінюватися в залежності від програмного, апаратного забезпечення та політики безпеки організації. Головним недоліком системи моніторингу Zabbix є необхідність встановлення серверної частини на Linux системі, та відносно невеликий об’єм логів що зберігаються. Незважаючи на ці недоліки Zabbix надає можливість інтегрувати додаткові рішення наприклад Graylog, що виправляє ці недоліки. Саме тому дане програмне рішення являється одним з найкращих, оскільки гарантує гнучку систему налаштування, можливість інтеграції з іншими системами моніторингу та лог-аналізу.

СПИСОК ЛІТЕРАТУРИ

1. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.06.2022).
3. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. *Офіційний веб портал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 26.05.2022).
4. Про основні засади забезпечення кібербезпеки України. *Офіційний веб портал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.05.2022).
5. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. *Офіційний веб портал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 26.05.2022).
6. Overview of Zabbix. *Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution*. URL: https://www.zabbix.com/documentation/1.8/en/manual/about/overview_of_zabbix#:~:text=Zabbix%20is%20an%20enterprise-class,alerts%20for%20virtually%20any%20event (date of access:25.05.2022).

7. Nagios – Overview. *Online Tutorials Library*. URL: https://www.tutorialspoint.com/nagios/nagios_overview.htm#:~:text=Nagios%20is%20an%20open%20source,IT%20infrastructure%20and%20its%20performance (date of access:22.05.2022).
8. Complete overview of the ELK stack. *Instaclustr*. URL: https://www.instaclustr.com/blog/elk-stack/ (date of access:19.05.2022).
9. 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-watcher-analyze-nsg-flow-logs-graylog (date of access: 12.06.2022).
10. Eventlog Key – Win32 apps. *Developer tools, technical documentation and coding examples | Microsoft Docs*. URL: https://docs.microsoft.com/en-us/windows/win32/eventlog/eventlog-key (date of access: 12.06.2022).

ДОДАТОК А

Тема	Опис
Audit account logon events	Визначає, чи проводити аудит кожного екземпляра користувача, який входить або виходить з іншого пристрою, на якому цей пристрій використовується для перевірки облікового запису.
Audit account management	Визначає, чи проводити аудит кожної події керування обліковим записом на пристрої.
Audit directory service access	Визначає, чи проводити аудит події, коли користувач звертається до об’єкта Active Directory, який має власний список керування доступом до системи (SACL).
Audit logon events	Визначає, чи проводити аудит кожного екземпляра користувача, який входить на пристрій чи виходить із нього.
Audit object access	Визначає, чи проводити аудит події, коли користувач звертається до об’єкта, наприклад, до файлу, папки, ключа реєстру, принтера тощо, для якого вказано власний список керування доступом до системи (SACL).
Audit policy change	Визначає, чи проводити аудит кожного випадку зміни політики призначення прав користувачів, політик аудиту чи політики довіри.
Audit privilege use	Визначає, чи проводити аудит кожного екземпляра користувача, який користується правом користувача.
Audit process tracking	Визначає, чи потрібно перевіряти детальну інформацію відстеження для таких подій, як активація програми, завершення процесу, обробка дублювання та непрямий доступ до об’єктів.
Audit system events	Визначає, чи проводити аудит, коли користувач перезавантажує або вимикає комп’ютер, або коли відбувається подія, яка впливає на безпеку системи або журнал безпеки.

ДОДАТОК Б

ID	Опис
4624	Вхід в обліковий запис виконаний успішно
4648	Виконана спроба входу в систему з явним зазначенням облікових даних.
4672	Для нового сеансу входу призначені спеціальні привілеї.
4625	Обліковому запису не вдалося виконати вхід в систему
4647	Вихід користувача з ініціативи користувача
4776	Контролер домену намагався перевірити дані для облікового запису
4771	Невдалий запит на вхід квитка не вдасться, Windows
4720	Створено обліковий запис
4722	Обліковий запис вимкнено
4723	Була зроблена спроба змінити пароль облікового запису.
4724	Була зроблена спроба скинути пароль облікового запису.
4725	Обліковий запис користувача було вимкнено.
4726	Обліковий запис користувача було видалено.
4738	Обліковий запис користувача було змінено.
4740	Обліковий запис користувача було заблоковано.
4767	Обліковий запис користувача було розблоковано.
4781	Ім'я облікового запису було змінено.
4794	Була зроблена спроба встановити пароль адміністратора.
4741	Обліковий запис комп’ютера створено.
4742	Обліковий запис комп’ютера змінено.
4743	Обліковий запис комп’ютера видалено.