МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Система керування інформаційною безпекою на базі хмарної платформи FortiSIEM»

Виконавець: _____ Владислав ХОМЕНКО
(підпис)

Керівник: _____ Володимир КЛИМЧУК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Володимир ВАЩЕНКО
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Хоменка Владислава Юрійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Система керування інформаційною безпекою на базі хмарної платформи FortiSIEM»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи: система Security Information & Event Management
4. Зміст пояснювальної записки: аналіз системи Security Information & Event Management, практичне використання системи Forti Security Information & Event Management, аналіз і оцінка ризиків інформаційної безпеки
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: графічна демонстрація налаштування хмарної платформи FortiSIEM, слайди презентації в програмному пакеті Microsoft Power Point

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Аналіз системи Security Information & Event Management	12.09.2022-05.10.2022	Виконано
4	Практичне використання системи Forti Security Information & Event Management	06.10.2022-15.10.2022	Виконано
5	Аналіз і оцінка ризиків інформаційної безпеки	17.10.2022-05.11.2022	Виконано
6	Охорона праці	07.11.2022-12.11.2022	Виконано
7	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколиш-нього середовища	д.ф.-м.н., проф. Володимир ВАЩЕНКО		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Володимир КЛИМЧУК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Владислав ХОМЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Система керування інформаційною безпекою на базі хмарної платформи FortiSIEM» містить 84 сторінки, 40 рисунків, 9 таблиць, 30 використаних джерел.

SECURITY INFORMATION & EVENT MANAGEMENT, ІНФОРМАЦІЙНА БЕЗПЕКА, VPN-СЕРВЕР.

Мета кваліфікаційної роботи – виділити найбільш важливі інформаційні активи, що підлягають захисту та проаналізувати ризикові ситуації для даних активів, а також провести розрахунок максимальних та залишкових ризиків (таких, що залишаються після впровадження захисних заходів).

Об'єктом дослідження – є процес виявлення інцидентів інформаційної безпеки на базі хмарних систем виявлення.

Предметом дослідження – є система Security Information & Event Management.

Практичне значення отриманих результатів. Продемонстровано роботу SIEM системи, що дозволяє отримати максимально повне уявлення про те, що в ній відбувається. Також вона дає можливість будувати докладні звіти про інциденти ІБ та реагувати на них швидше. Також продемонстровано реакції SIEM системи на спроби несанкціонованого входу. Для вирішення проблем пов'язаних з інцидентами інформаційної безпеки було використано VPN-сервер на базі Debian 9.5 сімейства ОС Linux.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

SIEM - Security Information And Event Management (Інформація про безпеку та управління подіями).

SIM - Security Information Management (Управління інформацією про безпеку).

SEM - Security Event Management (Керування подіями безпеки).

VPN - Virtual Private Network (Віртуальна приватна мережа).

CMDB - Configuration Management Database (База даних керування конфігураціями).

ІБ - Інформаційна безпека.

SOC - Security operations center (Оперативний центр безпеки).

СМПБ – Системи моніторингу подій безпеки.

НСД - Несанкціонований доступ.

IDS - Intrusion detection system (Система виявлення вторгнень).

IPS - Intrusion prevention system (Система Запобігання Вторгнення).

DLP - Data leak prevention (Запобігання витоків).

СУБД – Система управління базами даних.

ПЗ - Програмне забезпечення.

КВІ - Критичний важлива інфраструктури.

ІТ – Інформаційні технології.

ІС - Інформаційні системи.

ОС – операційна система.

UDP - User Datagram Protocol (Протокол користувальницьких датаграм).

TCP - Transmission Control Protocol (Протокол керування передачею).

СВВ - Система виявлення вторгнень.

МЕ - Міжмережеві екрани.

ВСТУП

Актуальність теми. У наш час кількість та різноманітність загроз, пов'язаних з порушенням цілісності та конфіденційності інформації щороку зростає. І системи безпеки повинні встигати додавати нові компоненти, розширюючи інфраструктуру інформаційної безпеки. У випадку, коли є кілька систем інформаційної безпеки, важко продуктивно їх адмініструвати і розуміти, що відбувається в інфраструктурі. Провідні фахівці у цій галузі вважають, що необхідно створити комплексний підхід у сфері реагування та розслідування інцидентів інформаційної безпеки у вигляді єдиного централізованого рішення. Тому багато компаній інтегрують у свої системи SIEM (Security Information Event Management).

SIEM система дозволяє отримати максимально повне уявлення про те, що відбувається у системі. Також вона дає можливість будувати докладні звіти про інциденти ІБ та реагувати на них швидше.

Управління інформацією про безпеку та події, або визначення SIEM – це підхід до управління безпекою, що поєднує функції SIM (управління інформацією про безпеку) та SEM (управління подіями безпеки) в єдину систему управління безпекою. Рішення щодо безпеки інформації та управління подіями збирають журнали та аналізують події безпеки разом з іншими даними для прискорення виявлення загроз та підтримки управління інцидентами та подіями безпеки, а також дотримання вимог. По суті, система технологій SIEM збирає дані з кількох джерел, що дозволяє швидше реагувати на загрози. Якщо виявлено аномалію, вона може зібрати більше інформації, викликати попередження або ізолювати актив.

SIEM - система підтримує інтеграцію зі сторонніми пристроями, взаємодіючи з інфраструктурою, опитуючи її про події безпеки, логи і продуктивність, що виникають. При цьому система дозволяє обмінюватися даними із зовнішніми системами управління вразливостей та оповіщення про виявлені вразливості і тим самим розширювати можливості протидії та захисту від них [1-14].

Мета кваліфікаційної роботи – виділити найбільш важливі інформаційні активи, що підлягають захисту та проаналізувати ризикові ситуації для даних активів, а також провести розрахунок максимальних та залишкових ризиків (таких, що залишаються після впровадження захисних заходів).

Для досягнення поставленої мети вирішуються такі **наукові завдання**:

1. проаналізувати структуру та принцип роботи SIEM систем;
2. аналіз ринку та порівняльна робота популярних SIEM систем;
3. дослідження можливостей системи FortiSIEM для досягнення поставленої мети;
4. імітаційне моделювання роботи з інцидентами інформаційної безпеки на базі системи FortiSIEM;
5. імітаційне моделювання роботи VPN - сервера на базі ОС Linux з демонстрацією його роботи.

Об'єктом дослідження – є процес виявлення інцидентів інформаційної безпеки на базі хмарних систем виявлення.

Предметом дослідження – є система Security Information & Event Management.

Практичне значення отриманих результатів.

Продемонстровано роботу SIEM системи, що дозволяє отримати максимально повне уявлення про те, що в ній відбувається. Також вона дає можливість будувати докладні звіти про інциденти ІБ та реагувати на них швидше. Також продемонстровано реакції SIEM системи на спроби несанкціонованого входу. Для вирішення проблем пов'язаних з інцидентами інформаційної безпеки було використано VPN-сервер на базі Debian 9.5 сімейства ОС Linux.

Проведено аналіз умов праці з розрахунком системи кондиціювання та пожежної безпеки.

РОЗДІЛ 1
АНАЛІЗ СИСТЕМИ SECURITY INFORMATION & EVENT MANAGEMENT

1.1. Система Security Information & Event Management

До моменту виявлення зловмисника в мережі або будь-якої вразливості можуть проходити багато місяців. Все було добре, доки не виник реальний інцидент інформаційної безпеки. Припустимо, необхідний лог деякого додатка за тривалий проміжок часу. Знайшовши цей лог виявляється, що в ньому немає необхідної інформації для розслідування. Все це веде до великих втрат компанії. Площа атак стрімко зростає із високою динамікою. Чим вище площа атаки, тим нижче можливість керування поведінкою атаки. Для того, щоб нівелювати негативну ситуацію пропонується рішення класу SIEM. Для того, щоб швидко розслідувати інциденти безпеки та впроваджувати заходи протидії [1].

SIEM – Security Information & Event Management складається з двох систем:

SIM – Security Information Management. Система, що відповідає за збір, зберігання, індексацію та історичний пошук за подіями, що надходять від відстежувальних систем інфраструктури, таких як міжмережні екрани, маршрутизатори, сервери тощо.

SEM – Security Event Management. У цій системі відбувається ідентифікація подій, кореляція між різними системами, побудова звітності та автоматизація висновків. У 2020 році 51% організацій повідомили про проблемну нестачу навичок кібербезпеки порівняно з 45% у 2017-2019 році. Організації прагнуть підвищити ефективність і дієвість і звертаються до автоматизованих або автоматизованих інструментів, щоб полегшити тягар ручного або завдання, що повторюється [1].

FortiSIEM збирає дані з різнорідних хост-систем, мережевих пристроїв та платформ безпеки в організації та додає контекст у реальному часі, аналітику та оповіщення для більш повного розуміння середовища, чим це можливо зробити з допомогою традиційної системи SIEM. FortiSIEM дозволяє швидко та ефективно аналізувати

та ідентифікувати інциденти з використанням даних із кількох доменів з високим ступенем достовірності. ESG Lab підтвердила, що FortiSIEM змогла збирати, індексувати та аналізувати реальний мережевий трафік, що складається із сотень мільйонів щоденних подій від тисяч пристроїв та систем, та надавати короткий, оперативний, дієвий штучний інтелект [1].

FortiSIEM може автоматизувати як моніторинг, так і реагування на загрози та інциденти, щоб звести до мінімуму вплив та час простою, дозволяючи IT-відділам та командам безпеки зосередитися на більш активних діях [1].

Рис. 1.1. Сценарії роботи SIEM

Подібні системи допоможуть вирішити нам наступні завдання:

- ***консолідація і зберігання журналів подій від різних джерел*** - мережевих пристроїв, журналів ОС, додатків та СЗІ. Подивившись будь-який стандарт ІБ, ми побачимо технічні вимоги до збору та аналізу подій. Вони потрібні не тільки для того, щоб виконати вимоги стандарту, адже бувають ситуації, коли побачили інцидент пізно, а події вже давно видалені чи журнали подій чомусь недоступні і причини того, що сталося, виявити практично неможливо;

- ***надання інструментів для аналізу подій та розбору інцидентів.*** Створює читабельну відповідь. У тому числі безпосередньо з потрібною Вам фільтрацією. Наприклад, щоденний звіт про інциденти, звіт про працездатність тощо;

- ***кореляція та обробка за правилами.*** Найпростіший приклад - "login failed": один випадок нічого не означає, але три і більше таких події з одним обліковим записом вже можуть свідчити про спроби добору. У найпростішому випадку в SIEM правила представлені у форматі RBR (Rule Based Reasoning) і містять набір умов, тригери, лічильники, сценарій дій;

- ***автоматичні оповіщення та інцидент-менеджмент.*** Основне завдання таких систем – не простий збір подій, а автоматизація процесу виявлення інцидентів зі збором у журналі, і навіть своєчасне інформування про подію;

- за наявності сканера вразливостей ***система частково допоможе оцінити ризики*** [1].

Розглянемо послідовність аналізу подій у SIEM.

На першому етапі відбувається збір інформації, потім система здійснює її аналіз, далі сортування, тобто відкидання лишнього та нормалізація подій, на наступному етапі кореляція між подіями різних спрямованостей.

Після кореляції відбувається збереження з одного боку та оповіщення з іншого, тобто формуються звіти і інциденти безпеки.

На останньому етапі відбувається автоматичне прийняття дія на основі аналізу звітності [2]. Алгоритм роботи SIEM-системи представлений рисунку 1.2.

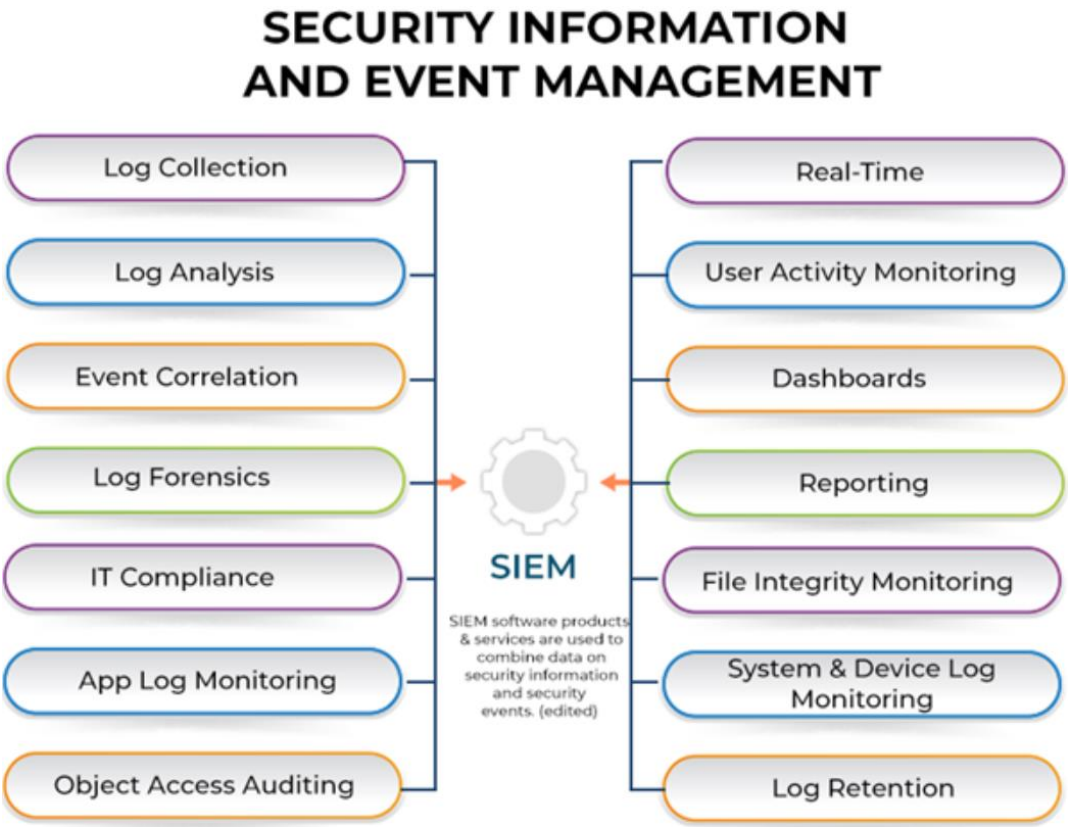

Рис. 1.2. Розбір подій в SIEM

1.2. Архітектура SIEM системи

В основному, SIEM-система розгортається над інформаційною системою, яка знаходиться під захистом і має архітектуру «джерела даних» - «сервер додатків» - «сховище даних». SIEM-рішення представляються як інтегровані пристрої (***all -in-one***) або дво-трикомпонентні комплекси. Розподілена архітектура зазвичай передбачає високу продуктивність і найбільш відповідні можливості масштабування, а також дозволяє розгорнути SIEM-рішення в IT-інфраструктурах з кількома майданчиками [2].

Агенти виконують початкову обробку, фільтрацію та збирання подій безпеки. Передача інформації від джерел даних може здійснюватися кількома способами:

- джерело ініціює передачу подій (наприклад, відправляє по syslog -протоколу);
- події з джерела забираються пасивно [2].

Архітектура класичною SIEM-системи представлена на рисунку 1.3.

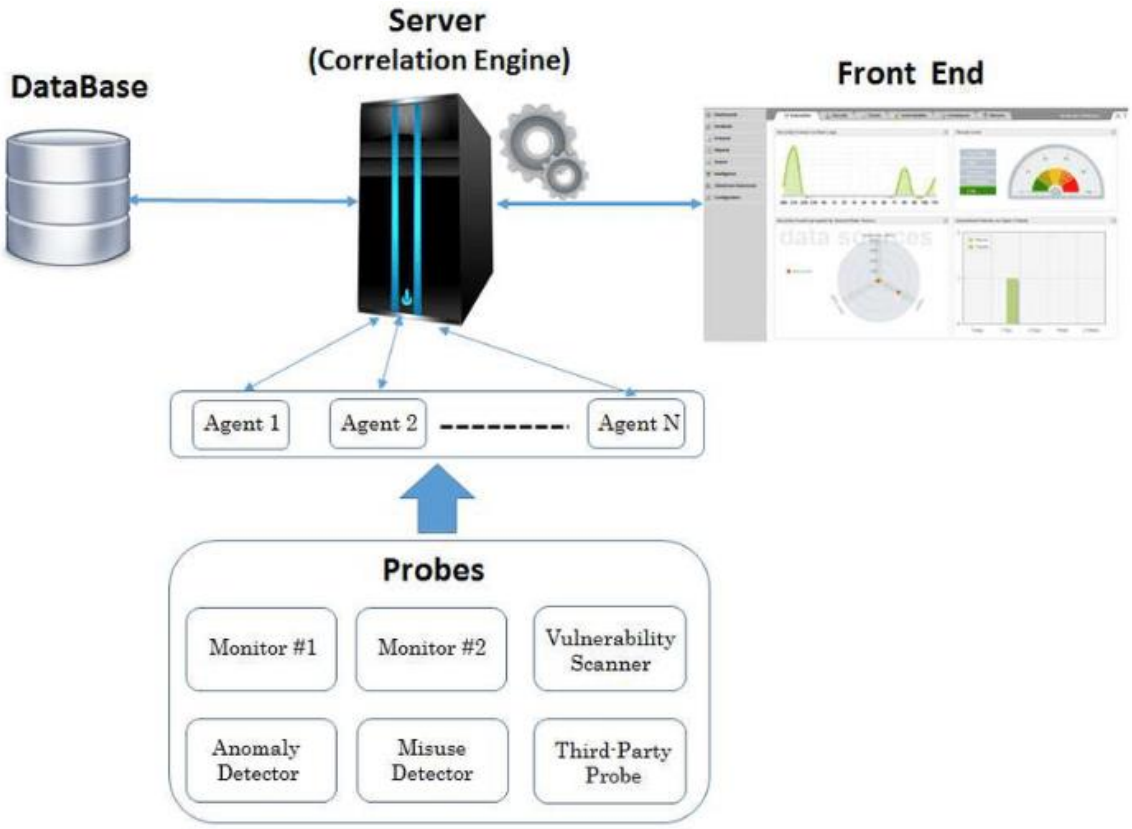

Рис. 1.3. Архітектура типової SIEM системи

Зібрана та відфільтрована інформація про події безпеки надходить у сховище даних, де вона зберігається у внутрішньому форматі подання з метою подальшого використання та аналізу сервером додатків [2].

Сервер додатків реалізує основні функції захисту інформації. Він аналізує інформацію, що зберігається в репозиторії, і перетворює її на вироблення попереджень чи управлінських рішень із захисту інформації [2].

1.3. Завдання і функції SIEM- системи

Основне завдання SIEM — не просто зібрати події, а й автоматизувати процес виявлення інцидентів із документуванням у власному журналі чи зовнішній системі HelpDesk, а також своєчасно інформувати про подію [4].

SIEM здатна виявляти:

- мережеві атаки у внутрішньому та зовнішньому периметрах;
- вірусні епідемії або окремі вірусні зараження, невіддалені віруси, бекдори та трояни;
- спроби несанкціонованого доступу до конфіденційної інформації;
- фрід та шахрайство;
- помилки і збої в роботі інформаційних систем;
- вразливості;
- помилки конфігурацій у засобах захисту та інформаційних системах.

Система SIEM є універсальною за рахунок своєї логіки. Але для того, щоб покладені на неї завдання вирішувалися, необхідні корисні джерела та правила кореляції. Будь-яка подія (наприклад, якщо у певній кімнаті відчинилися двері) може бути подано на вхід SIEM і використано [2].

Джерела вибираються на підставі наступних факторів:

- критичність системи (цінність, ризики) та інформації (оброблюваної та збереженої);
- достовірність і інформативність джерела подій;
- покриття каналів передачі інформації (мають враховуватися як зовнішній, а й внутрішній периметр мережі);
- вирішення спектра завдань IT та ІБ (забезпечення безперервності, розслідування інцидентів, дотримання політик, запобігання витоку інформації [4].

1.4. Кореляція і аналітика

Кореляція та аналітика є ядром технології SIEM, і вона включає зв'язування воєдино різних подій, про які повідомляється в журналах, для виявлення ознак компромісу. Один приклад: сканування порту з подальшим доступом користувачів до певних типів даних. Важливо, щоб функціональність аналітики була представлена таким чином, щоб мати можливість ефективно використовувати її [5].

Ключем до цієї здатності виявляти загрози є використання правил кореляції, основний набір яких може бути надано системою SIEM, але до яким адміністратори

можуть додати. Наприклад, одне правило кореляції може полягати в тому, що якщо чотири або більше невдалих спроб входу в систему відбуваються з однієї й тієї ж IP-адреси з використанням різних імен користувачів протягом 15 хвилин, і за цим слідує успішний вхід з цієї IP- адреси на будь-який пристрій у мережі. Потім має бути видано попередження. У цьому випадку механізм кореляції системи SIEM починає працювати для виявлення моделі поведінки (невдалі спроби входу в систему, що супроводжуються успішною), які можуть вказувати на те, що атака методом перебору була успішною [5].

Кореляція є одним із ключових компонентів будь-якого ефективного інструменту SIEM. Оскільки інформація про ваше цифрове середовище надходить на платформу SIEM, ця платформа використовує кореляцію для виявлення будь-яких можливих проблем. Це досягається шляхом порівняння послідовності дій із встановленими правилами, які можуть бути встановлені постачальником SIEM або налаштуваннями користувача, створеними вами і вашою командою [5].

Наведений вище приклад повторних невдалих спроб входу до системи є типовим випадком, коли кореляція виявляється корисною. Хоча ця інформація може не виглядати загрозливою для неозброєного ока, що читає безліч даних, інструменти SIEM з необхідними правилами кореляції зможуть визначити потенційну загрозу та попередження. Для новачків у платформі налаштування правил кореляції SIEM може здатися складним. Зрештою, інструменти SIEM, як правило, шукатимуть тільки те, що ви їм скажете, тому створення правил, що передбачають реальні загрози, є обов'язковим. На щастя, багато продуктів SIEM поставляються з підготовленими правилами кореляції. Вам потрібно буде виконати їх, щоб визначити, які з них мають сенс для бізнесу, і у вас також буде можливість включити власні правила кореляції на власний розсуд [5].

Слід зазначити, що інструменти моніторингу SIEM можуть виявляти хибні спрацьовування, тому тут важливо знайти правильний баланс. Якщо ви налаштуєте свої правила кореляції таким чином, щоб вони викликали занадто багато хибних спрацьовувань, ви, можливо, втрачаєте час, спускаючись у кролячі нори. Однак якщо ви

зайдете надто далеко в іншому напрямку, ви ризикуєте дозволити зловмисній діяльності продовжуватись без адекватної та своєчасної відповіді. Таким чином, правила кореляції SIEM дозволяють професіоналам у галузі кібербезпеки розширювати ці інструменти, щоб вони працювали для конкретних потреб кожного бізнесу. Конкретний продукт SIEM може пропонувати клієнтам той самий тип захисту та ті ж функції, але це залежить від MSP, щоб розгорнути ці інструменти, щоб вони були максимально ефективними для кожного бізнесу. Схема, що демонструє роль кореляції, представлена рисунку 1.4.

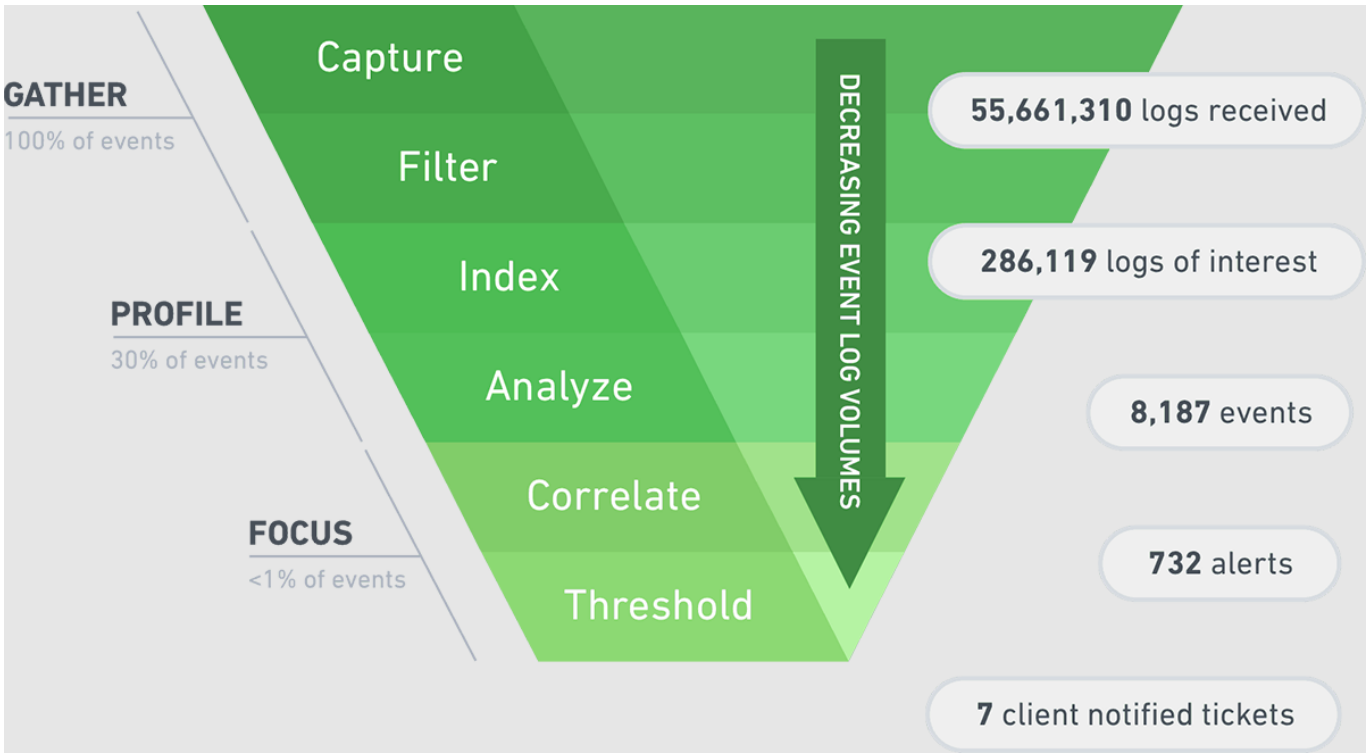

Рис. 1.4. Роль кореляції

Аналітика SIEM ґрунтується на функціях пошуку, виконанні правил та формування звітів. Функція пошуку SIEM складається з пошуку в реальному часі та історичного пошуку інформації [4], яка була зібрана на основі IT-інфраструктури. У режимі пошуку в реальному часі виводяться події, що вже виникли, тоді як історичний пошук базується на інформації з баз даних подій. Простий пошук за ключовими словами та структуровані пошукові запити, що дозволяють виконувати пошук, ґрунтуючись на

конкретних атрибутах та значеннях . подій, потім групування результатів за атрибутами можуть бути включені в обидва типи пошуку. SIEM безперервно спостерігає за інфраструктурою та формує інформацію, яку можна використовувати для аналізу безпеки, продуктивності та доступності. Для швидкого реагування на події безпеки потрібно вчасно отримувати попередження про те, що могли виникнути виняткові, підозрілі чи потенційні несправності та порушення. З цією метою використовуються правила, що визначають умови, на які необхідно звернути увагу та які ініціюють інцидент [5].

1.5. Принцип роботи

Принцип роботи SIEM зводиться до послідовного алгоритму процесів. Система збирає інформацію з різних джерел, аналізує її в режимі реального часу, при потребі робить превентивні заходи, систематизує бази даних, аналізує дії користувачів на основі результатів попереднього моніторингу, створює попередження та сповіщення про критичні події [4].

Джерелами даних для SIEM служать різноманітні корпоративні системи:

- ***системи контролю доступу та аутентифікації.*** Призначені для спостереження отримання доступу до інформаційного потоку;
- ***DLP системи.*** Передають дані про несанкціонований вихід інформації за межі корпоративної мережі та про порушення у використанні привілеїв;
- ***ресурси IDS/IPS.*** Передають дані про мережеві атаки, зміну прав доступу;
- ***антивірусні платформи.*** Повідомляють про загрози у вигляді шкідливого коду, заміну конфігурацій або політик конфіденційності, повідомляють про роботу баз даних та ПЗ;
- ***журнали подій серверів та тонких клієнтів.*** Контролюють дотримання прав доступу та політики ІБ;
- ***міжмережевих екранів.*** Передають дані про небезпечні інциденти, шкідливе ПЗ;

- ***обладнання мережі.*** Враховує трафік мережі, контролює доступ користувачів до інформаційних потоків;
- ***системи веб-фільтрації.*** Узагальнюють та спрямовують дані про те, які заборонені чи шкідливі сайти в інтернеті відвідують користувачі.

Система SIEM – це, по суті, спеціалізована система аналізу великих даних, яка прагне отримати корисну інформацію про масу подій та інших даних, які вона приймає та зберігає.

Основним джерелом даних є журнали, згенеровані системами, включаючи ваші сервери та пристрої безпеки, але SIEM можуть приймати різні інші типи даних, включаючи мережні пакети, а також контекстну інформацію про користувачів, ресурси, загрози та вразливості. це можна знайти всередині або поза вашою організацією. Потім ці дані з різних джерел повинні бути «нормалізовані» або переформатовані , щоб SIEM могла їх зрозуміти [4].

На рисунку 1.5 показаний алгоритм роботи SIEM.

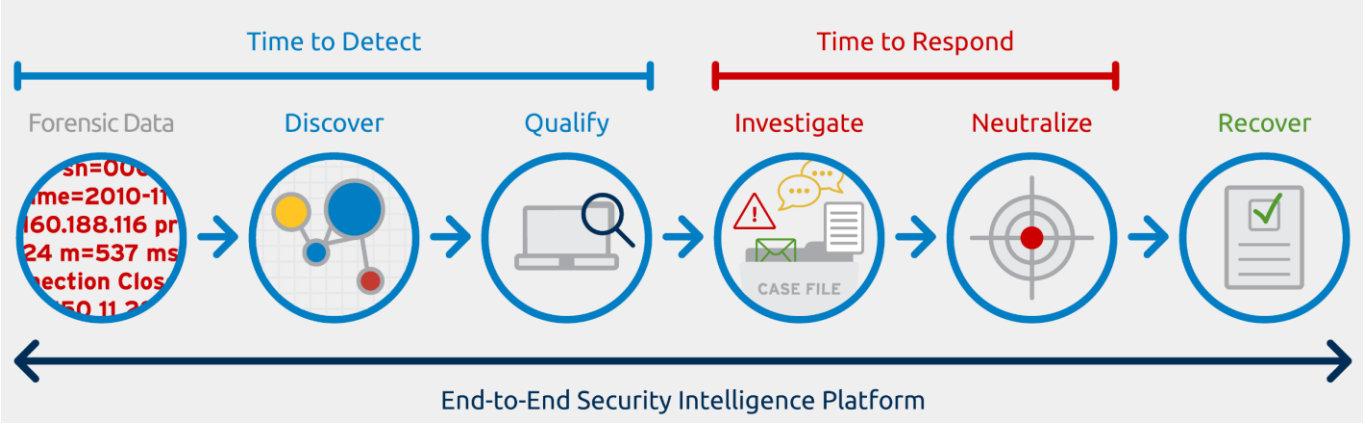

Рис. 1.5. Алгоритм роботи SIEM

SIEM-система обробляє та аналізує отримані дані на основі математичних обчислень та порівняння статистичних даних. Правила аналізу у традиційних рішеннях найчастіше задаються вручну. Наприклад, під час налаштування створюється скрипт, за яким одноразовий інцидент не становить загрози, а повторюваний під одним обліковим записом означає спробу підібрати код доступу [4].

SIEM-рішення дозволяє виявити:

- зовнішні і внутрішні кібератаки;
- окремі зараження та вірусні епідемії;
- спроби отримати несанкціонований доступ до захищених інформаційних потоків;
- факти корпоративного шахрайства;
- похибки і порушення у роботі інформаційних систем;
- слабкі місця системи захисту;
- порушення структури засобів захисту;
- цільові розкрадання.

1.6. Переваги SIEM системи

Оцінити переваги SIEM-рішення допоможе аналіз за основними характеристиками.

Деякі з переваг SIEM включають наступне:

- скорочує час, необхідний на виявлення загроз, зводячи до мінімуму збитки від цих загроз;
- пропонує цілісне уявлення про середовище інформаційної безпеки організації, полегшуючи збирання та аналіз інформації про безпеку для забезпечення безпеки систем - всі ці організації надходять до централізованого сховища, де вони зберігаються і легко доступні;
- можуть використовуватися компаніями для різних варіантів використання, які обертаються навколо даних або журналів, включаючи програми безпеки, аудит та звіти про відповідність, службу підтримки та усунення несправностей у мережі;
- підтримує великі обсяги даних, щоб організації могли продовжувати масштабування та збільшення своїх даних;
- забезпечує виявлення загроз і оповіщення про безпеки;
- може виконати детальний судовий аналіз в випадку серйозного порушення безпеки [4].

Комплексний аналіз стану мережі як реального часу:

- Висока продуктивність та швидкість аналізу подій у режимі реального часу.
- Велика кількість правил кореляції і звітів, що генеруються, доступних при впровадженні продукту з коробки.
- Велика кількість протоколів інтеграції зі сторонніми пристроями та системами.
- Взаємна кореляція даних аналізу SOC та NOC.
- Реалізація практично будь-якого сценарію реагування на інцидент безпеки, проведення розслідування за рахунок можливості визначення ланцюжка послідовних дій.
- Автоматизація процесів виявлення загроз та аномалій.
- Автоматизація процесів реєстрації та контролю інцидентів, з наступною можливістю їхнього розслідування.
- Контроль за станом інфраструктури.
- Наявність агентів збору даних та моніторингу для Microsoft Windows та агентів контролю цілісності файлів для Linux.
- Підтримка кількох сценаріїв розгортання.
- Підтримка горизонтального масштабування та віртуалізованої архітектури.
- Гібридна архітектура бази даних.
- Розподілена кореляція подій у режимі реального часу.
- Оперативна обробка журналів, що настроюється.
- Передбачено кілька сценаріїв розгортання в залежності від потреб і інфраструктури замовника [4].

Важливий маркер зручності роботи із SIEM – можливість централізовано координувати компоненти платформи з єдиної консолі, а також автоматично оновлювати встановлені політики та шаблони звітності. Все це полегшить аналіз спеціаліста з інформаційної безпеки. Ще один плюс на користь рішення – оперативність та якість

технічної підтримки. За цим параметром у більшості випадків виграють вітчизняні виробники, головним чином, через невисокої вартості [4].

1.7. Огляд і порівняння SIEM рішень

На етапі вибору критеріїв порівняння у цій робочій групі виникають розбіжності щодо коректності порівняння існуючих рішень або недостатнього розкриття низки функціональних можливостей. Потреби сервісного SOC разюче відрізняються від потреб інфраструктурного внутрішнього SOC. І якщо для першого важливо підключити з коробки максимальну кількість джерел і мати можливість гнучкого управління даними, що надходять від них, то для другого великим пріоритетом може стати зручний інтерфейс користувача. У залежності від потреб функціональність продуктів визначає їх можливості. Це орієнтування на інтеграцію всередині власної екосистеми, як у Positive Technologies та IBM, або спрямованість на інтеграцію зі сторонніми рішеннями, як у FortiSIEM та Micro Focus Security. Крім того, підходи до візуалізації та навігації в консолі кожного з рішень відповідають певній логіці, яку не завжди можна оцінити чіткими критеріями, проте можна емпірично прийняти за живої демонстрації.

Угруповання критеріїв здійснювалося з урахуванням базових впливів компаній - споживачів напрямів, диктованих часом: ступінь автоматизації, стратегія розвитку (зокрема стійкість над ринком), еластичність архітектури. Можливість компанії-споживача враховувати ризики при таких умовах надалі визначає її вибір.

Наприклад, варто придивитися до комплексного моновендорного рішення. Далі проводилася деталізація напрямів у групи, які розкладалися, своєю чергою, на підгрупи. По можливості та експертно оціненій вазі впливу критерію на оцінку підгрупи розбивалися оціночні параметри [6].

Архітектура рішення SIEM-системи -масштабованість, методи управління подіями та схема ліцензування – важливий параметр для Enterprise-установок, де необхідно підрахувати та ефективність реалізації у розподілених мережах. Інтеграційні можливості - наявність розвинених вбудованих та інтегрованих підсистем управ-

ління вразливістю, інцидентами та активами дозволить у початковому періоді експлуатації обмежитися використанням одного продукту, без збільшення кількості використовуваних адміністратором та аналітиком консолей. А інтеграція із сторонніми рішеннями з метою збагачення інформації про події ІБ, відомості про API та підтримувані джерела подій вказують на відкриту позицію компанії на ринку, уміння знаходити спільну мову з іншими гравцями, говорить про напрямки розвитку продукту.

Додаткові критерії — параметри, які піддаються впливу зовнішнього середовища. Це і звітність, зручність, це і глибина занурення під час навігації в рамках інтерфейсу системи. Все це впливає на оперативність при обробці подій ІБ та виявлення інцидентів ІБ і дозволяє примірятися до існуючих усередині компанії KPI. Нижче будуть розглянуті деякі системи як приклад і порівняємо їх:

- RSA NetWitness ;
- IBM QRadar SIEM;
- Splunk .

Розглянемо SIEM-систему - IBM QRadar SIEM.

QRadar SIEM забезпечує тотальну видимість усередині мережі, здійснюючи збирання та аналіз даних, які дозволяють оперативно отримувати всю необхідну інформацію про події безпеки та роботу мережевих пристроїв, незалежно від складності мережної конфігурації. Максимальна прозорість мережі дозволяє з найбільшою ефективністю керувати її безпекою та виявляти всі існуючі та потенційні загрози задовго до їх реалізації [6].

Рис. 1.6. IBM QRadar SIEM

QRadar SIEM - це інтегрований засіб, що чудово справляється із завданнями управління політиками щодо відповідності вимогам і стандартам, збору та аналізу логів та надає найсучасніший інструментарій для виявлення загроз. Рішення засноване на гнучкій платформі QRadar Security Intelligence Platform, яка може розвиватися паралельно з підприємством і підлаштовуватися під його інфраструктуру, що розширюється, легко і оперативно забезпечуючи моніторинг корпоративної безпеки [6].

QRadar SIEM збирає інформацію з наступних джерел:

- події системи безпеки - події від брандмауерів, VPNs, IDS/IPS і т.д.;
- мережеві події - події від свитчів, роутерів, серверів, хостів і т.д.;
- монітор активності мережі - контекстні ідентифікатори протоколів 7-го рівня від мережевого трафіку і додатків;
- монітор активності користувачів - дані продуктів типу IAM та сканерів уразливостей;
- журнали подій додатків – ERP (Enterprise Resource Planning), документообіг, бази даних додатків, адміністративні платформи тощо;
- контроль загроз, логів та відповідності політикам у режимі реального часу [6].

Поєднуючи розрізнену інформацію, QRadar SIEM робить ефективнішим виявлення всіх сучасних загроз. Дані нормуються та корелюються для своєчасного виявлення, повідомлення та реагування на загрози, які не в змозі визначити інші засоби захисту з обмеженою видимістю. Моніторинг QRadar SIEM дозволить підприємствам виявити складні загрози, серед яких інсайдерське шахрайство, нецільове використання додатків і багато інших [6].

Особливо ефективним є застосування QRadar SIEM для підприємств з великомасштабними мережами, в яких реєструються мільйони і більше подій на день. QRadar SIEM здійснює збір, аналіз та зберігання даних та надає кореляцію подій у режимі реального часу. Це дозволяє серед величезної кількості даних розпізнати ті, що можуть призвести до інцидентам безпеки. Мільярди мережевих подій та потоків можуть бути спрощені, що, відповідно, спростить процеси виявлення загроз, аудиту та створення звітності, що відповідає вимогам і стандартів. У цілях

аудиту і захисту мережевої інфраструктури QRadar SIEM забезпечить довгостроковий збір подій та прикладних даних, їх архівування, пошук необхідних даних та звітність [6].

QRadar SIEM контролює всі серйозні інциденти та загрози, надаючи хронологію обслуговування та всю необхідну супутню інформацію. Завдяки цьому рішенню служби безпеки зможуть завжди дізнатися відповіді на такі питання, як: хто порушує безпеку, який об'єкт зазнає нападу, де проводити розслідування, які наслідки для бізнесу? QRadar SIEM надасть повну інформацію про фактори, що порушують нормальний режим роботи, користувачів, моделі порушників, важливість ресурсів, характеристики вразливостей, рівень активності загроз та звіти про попередні порушення тощо. Таким чином служба безпеки зможе отримати всі необхідні відомості для своєчасного реагування на будь-які інциденти безпеки [6].

За допомогою QRadar SIEM можна виявити будь-які відхилення та зміни в роботі додатків, серверів, хостів та сегментів мережі. Можливість ідентифікації трафіку на прикладному рівні дозволяє QRadar SIEM досить точно аналізувати та розуміти політики та загрози корпоративної мережі підприємства, а також проводити загальний моніторинг активності мережі. Функція контролю роботи з таким додатком, як Skype, і соціальними мережами (включаючи Twitter , LinkedIn і т.д.), також дозволяє покращити видимість мережі. Підтримуючи виявлення великої кількості відхилень і правил, QRadar SIEM може детально відповісти на питання про те, який користувач що використовує. Контентний аналіз та оповіщення при передачі контенту, кореляція з іншою мережевою активністю та журналами подій дозволяють виявити нецільову передачу даних. Можливості фільтрації та вибір будь-якого часового проміжку для аналізу дозволяють користувачеві налаштувати варіант виведення результатів на власний розсуд. [6]

Тепер IT-фахівцям доступна покращена видимість активності широкого спектру бізнес-додатків у віртуальних мережах. Віртуальні сервери, як і фізичні, мають вразливість у системі безпеки, тому прозорість віртуального середовища обробки даних потрібна для точного визначення необхідних заходів щодо захисту додатків та даних.

Централізована інтуїтивно зрозуміла консоль управління забезпечує рольовий доступ, надаючи глобальний огляд управління інцидентами та звітності. Панелі керування QRadar SIEM пропонуються як функціонал, і користувачі можуть самі створити та налаштувати свій робочий простір відповідно до розв'язуваних завдань. Така деталізація наддасть можливість набагато простіше виявляти та вибирати сплески подій та мережеві потоки, пов'язані з порушеннями.

QRadar SIEM пропонує близько 3500 шаблонів звітів, пов'язаних з конкретними пристроями, ролями та вимогами регуляторів [7].

Рішення QRadar SIEM в першу чергу призначене для малого та середнього бізнесу, але може бути успішно розгорнуто в компанії будь-якого масштабу за рахунок своєї легкої масштабованості. QRadar SIEM уможливлює автоматичний перехід з іншого рішення та повну синхронізацію між системами. Впроваджувати додаткові рішення сторонніх виробників немає необхідності, оскільки QRadar SIEM забезпечує високий рівень аналізу та зберігання даних завдяки plug - andplay пристроям, що входять до сімейства продуктів QRadar . Графічний інтерфейс QRadar SIEM показаний рисунку 1.7.

Рис. 1.7. Графічний інтерфейс QRadar SIEM

У липні 2016 року RSA, підрозділ безпеки EMC, повторно представив свою SIEM-систему як платформу RSA NetWitness Suite, яка включає: управління журналами RSA NetWitness Logs & Packets (раніше RSA Security Analytics); засіб виявлення загроз на робітників станціях RSA NetWitness Endpoint (раніше RSA Enterprise Compromise Assessment Tool); менеджер центру оперативного управління RSA NetWitness SecOps Manager (раніше RSA SecOps). RSA NetWitness Suite забезпечує видимість загроз з використанням даних з подій безпеки та інших джерел журналів, повного захоплення пакетів, NetFlow та кінцевих точок (через RSA NetWitness Endpoint). Система RSA NetWitness орієнтована на моніторинг, аналіз та оповіщення в режимі реального часу на додаток до підтримки попереджувальної загрози, а також реагування на інциденти та судове розслідування. Алгоритм роботи RSA NetWitness Suite показано рисунку 1.8.

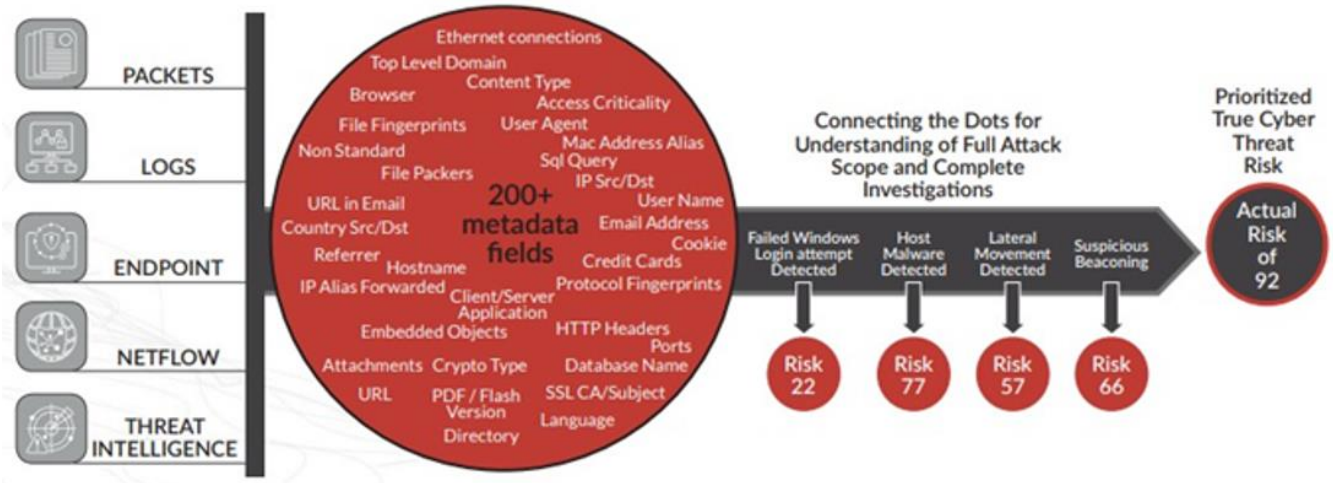

Рис. 1.8. Алгоритм роботи RSA NetWitness Suite

Платформа використовує комбінацію одного або кількох фізичних або віртуальних пристроїв для реєстрації журналів та пакетів (декодер), запитів та пошуку необроблених даних (концентратори), аналітики в реальному часі (Event Stream Analysis) та довготривалого зберігання журналів та звітів (Archiver). Гібридні пристрої, що поєднують декодери та концентратори в одну систему, доступні для невеликих середовищ. Декодери та концентратори доступні для підтримки великих та регіональних ро-

зподілених архітектур. Сервер NetWitness надає уніфікований інтерфейс для адміністрування та аналізу. Він також надає інтерфейс для звітів і аналітики шкідливих програм [8].

RSA Live Connect - це хмарна служба, яка забезпечує автоматичне оновлення контенту, включаючи правила виявлення, парсери пакетів та журналів, звіти та джерела загроз. Користувачі RSA NetWitness Suite також можуть використовувати RSA NetWitness SecOps Management (модуль у рішенні RSA Archer Governance , Risk and Compliance), який додає розширений процес керування інцидентами, панелі керування та звіти.

Переваги RSA NetWitness Suite: Платформа RSA NetWitness поєднує аналітику виявлення загроз та моніторинг подій, розслідування та аналіз загроз у мережевому трафіку, кінцевих точках та інших джерелах подій безпеки та журналів. Модульні варіанти розгортання дозволяють клієнтам вибирати моніторинг мережного трафіку, а також можливості моніторингу та аналізу подій та журналів у міру потреби. RSA Live забезпечивши дає простий та автоматизований підхід для забезпечення безперебійної доставки інформації про загрози, контент та інші оновлень. Інтеграція з RSA NetWitness SecOps Manager забезпечує уніфіковані можливості SOC. Візуалізація RSA NetWitness Suite представлена рисунку 1.9.

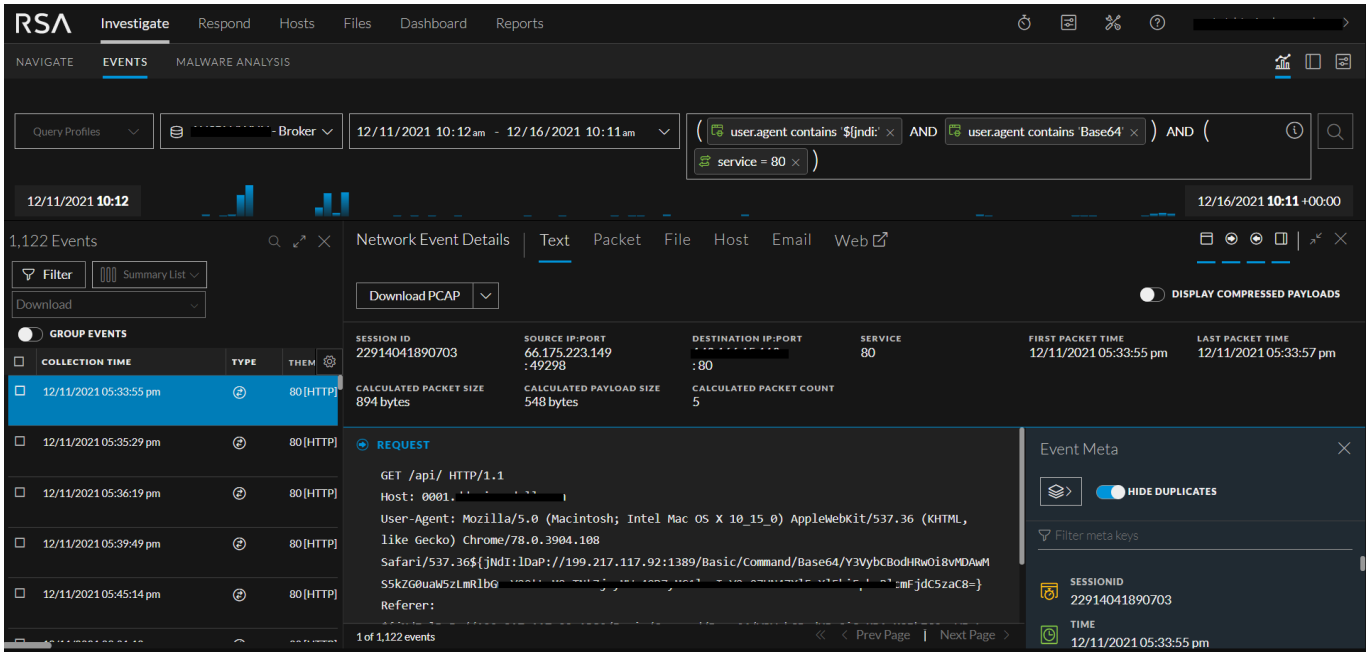

Рис. 1.9. Візуалізація RSA NetWitness Suite

Наступна розглядається SIEM - Splunk Enterprise Security

Рис. 1.10. SIEM - Splunk Enterprise Security

Splunk – це багатофункціональна платформа для збирання, зберігання, обробки та аналізу машинних даних. На сьогоднішній день вона є вкрай популярною у США та Європі і поступово виходить на інші ринки, включаючи Україну. Однією з головних особливостей платформи є те, що вона може працювати з даними практично з будь-яких джерел, що дозволяє широко застосовувати платформу у різних галузях. Одним із ключових напрямів розвитку є SIEM-система Splunk Enterprise Security [8].

До складу Splunk Enterprise Security входять такі функціональні рішення:

- Incident Review - гнучкий інструмент огляду та управління інцидентами, збагачений інформацією із зовнішніх джерел;
- Investigator - візуальний інструмент виявлення;
- Kill Chain - створення нових кореляційних пошуків на базі зібраного досвіду;
- Glass Tables - наочна побудова логічних схем ресурсів, що захищаються з вбудованим редактором. Можливість створення індивідуально налаштованих візуалізацій із ключовими показниками роботи SOC, що змінюються у масштабі реального часу;

- Security Intelligence - великий набір передбачених інтеграцій із зовнішніми джерелами інформації про загрози, включаючи інтеграцію з Facebook Threat Exchange.

Платформа Splunk може бути розгорнута як на фізичних, так і на віртуальних серверах, а також користувачам доступна хмарна версія рішення.

Splunk пропонує два види ліцензій: постійну та річну передплату, вартість яких прямо пропорційна обсягу оброблених даних на день, у гігабайтах. За останні роки у зв'язку із сильним розвитком напрямку Machine Learning та Artificial Intelligence Splunk розробив та інтегрував у свій продукт окремий модуль – Splunk Machine Learning Toolkit , що дозволяє будувати розширену аналітику в галузі прогнозування, виявлення аномалій, кластеризації та ін. Цей модуль підвищує аналітичні можливості SIEM-curry Splu . У середині 2015 року Splunk додав власну функціональність UEBA з придбанням Caspida , яка була перейменована в Splunk UBA (Splunk також працює з низкою інших продуктів UEBA). Більш жорстка інтеграція між продуктами Enterprise Security та UBA була запроваджена на початку 2016 року.

Переваги Splunk: Splunk здійснює збір, пошук, моніторинг та аналіз з різних і досить великих обсягів даних як у режимі історичного пошуку, так і в реальному часі, видаючи швидкий результат та високу інтерактивність пошукових запитів на надзвичайно великих обсягах даних. Splunk є повноцінною Big Data платформою. Splunk є універсальною системою для машинних даних, яка забезпечує комплексний збір даних, їхню обробку та аналіз. Таким чином система здатна об'єднати в собі машинні дані, бізнес дані, дані користувача і будувати аналітику в різних розрізах, що робить її вкрай універсальним. Splunk використовує технологію MapReduce [9], що забезпечує розподіл навантажень та швидку горизонтальну масштабованість системи. Також завдяки технології MapReduce зростає її продуктивність. на малюнку наведено панель моніторингу [8].

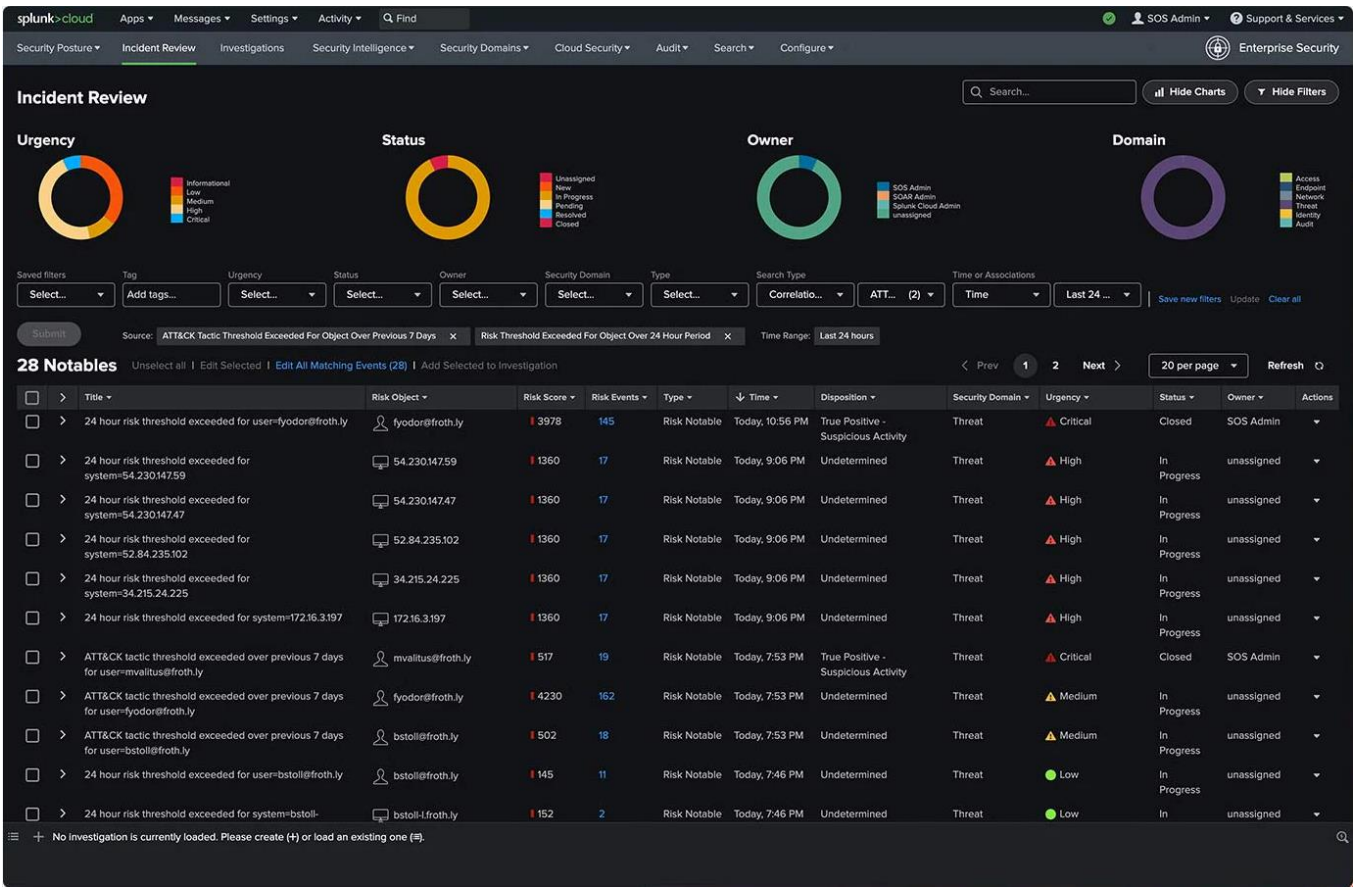

Рис. 1.11. Панель моніторингу Splunk Enterprise Security

Таблиця 1.1.

Порівняння різних SIEM систем

Критерій оцінки / Вендор	IBM Qradar	RSA NetWitness	Splunk
Автореєстрація вразливостей (інтеграція зі сканерами)	Інтеграція з усіма популярними сканерами великих вендорів, можливості з інтеграції через API та звіти різних форматів	Ні	Інтеграція зі сканерами з відкритих протоколів. Для популярних сканерів є модулі розбору подій (Qualys , Netxpose Rapid7 та ін.)
Ризик-кореляція, облік ризик-кореляції у правилах	Ризик-кореляція з урахуванням складових показника Magnitude (Relevance , Credibility та Severity)	Ні	Скорингована модель, яка враховує дані про активи та облікові записи користувачів

Закінчення таблиці 1.1

Перед настроєні панелі візуалізації та звіти щодо відповідності стандартам (Compliance)	COBIT, FISMA, GLBA, GSX-Memo22, HIPAA, NERC, PCI DSS, SOX	FISMA, ISO27002, FERPA, GLBA, FFIEC, NERC-CIP, BILL 198, BASEL II, GPG-13, HIPAA, NISPOM, PCI DSS, SOX, SSAE 16	GDPR, HIPAA, FISMA, PCI DSS (платні та безкоштовні доповнення до платформи SPLUNK ENTERPRISE та SPLUNK ES)
Довільні формули розрахунку ризиків	Ні	Ні	Вбудовано в мову SPL, на який спираються правила кореляції

РОЗДІЛ 2
ПРАКТИЧНЕ ВИКОРИСТАННЯ СИСТЕМИ FORTI SECURITY INFORMATION & EVENT MANAGEMENT

2.1. Опис системи FortiSIEM

FortiSIEM - це комплексний, масштабований засіб управління безпекою, продуктивністю та забезпеченням відповідності вимогам всіх компонентів інфраструктури, здатний працювати як з хмарами [10], так і з інтернетом речей (IoT). Рішення FortiSIEM спрямовано зниження складності виявлення загроз при підвищенні ефективності системи безпеки. SIEM-система такого рівня спрямована на захист не тільки інформації, а й репутації клієнтів, знижуючи негативні наслідки від загроз та протидіючи виникненню нових атак. FortiSIEM є розвитком відомої компанією AccelOps , що зарекомендувала себе на ринку SIEM-системи, яку Fortinet придбала в 2016 році. Fortinet додала до класичної SIEM-системи низку своїх запатентованих технологій: розподіленої кореляції подій у режимі реального часу; автоматизованого виявлення інфраструктури та додатків (CMDB); настроюваної обробки журналів. FortiSIEM підтримує інтеграцію зі сторонніми пристроями, опитуючи інфраструктуру про події безпеки, логи , продуктивність тощо. FortiSIEM є частиною фабрики безпеки Fortinet Security Fabric, тобто інші засоби захисту Fortinet можуть бути інтегровані з FortiSIEM та обмінюватися з продуктом інформацією, у тому числі і про виявлені вразливості [9].

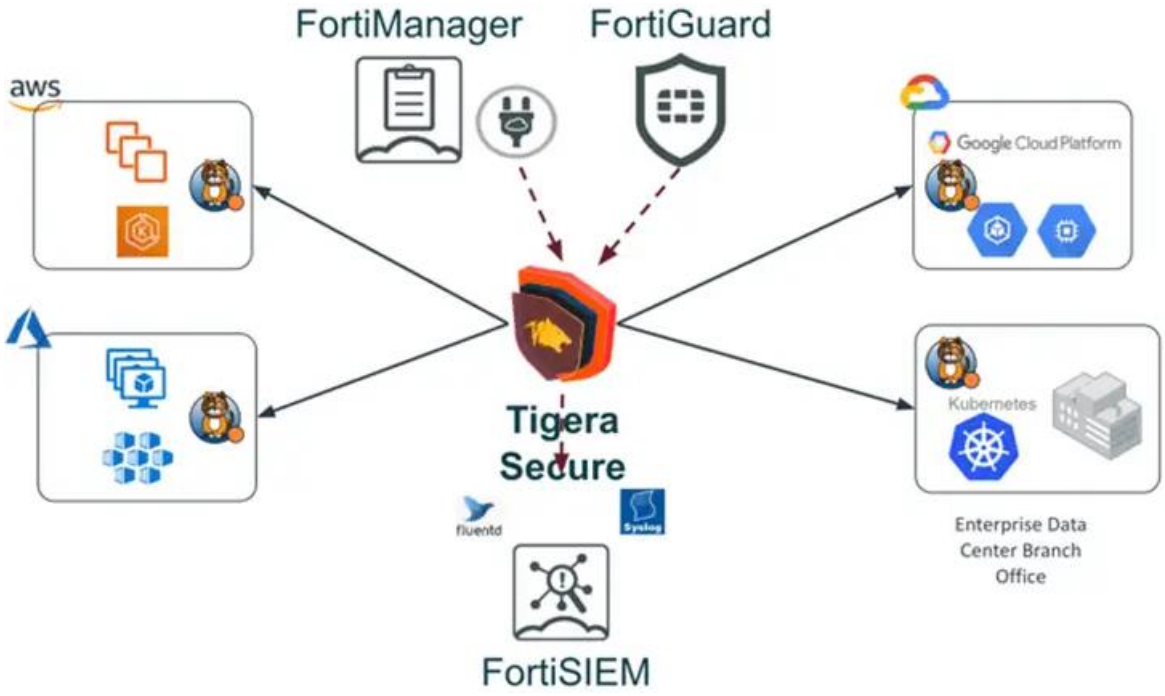

Рис. 2.1. FortiSIEM в концепції

Система FortiSIEM розташовується на межі окремих технологій SOC (Security Operations Center) та NOC (Network Operations Center), дозволяючи використовувати крос-кореляцію інформації від одного і від іншого і підвищити ефективність взаємодії між SOC та NOC, знижуючи час на розслідування інцидентів інформаційної безпеки [9].

FortiSIEM є комплексним і масштабованим корпоративним рішенням, що забезпечує охоплення мережі від IoT до хмари і включає запатентовані аналітичні інструменти, які забезпечують ефективне управління мережевою безпекою і продуктивністю в режимі реального часу.

Розглянемо основні можливості FortiSIEM. Масштабований та гнучкий збір журналів:

- збирання, обробка, зберігання, нормалізація, індексування та кореляція подій безпеки з підтримкою десятків тисяч подій за секунду (один супервізор — в єдиному виконанні до 20000 EPS, з можливістю масштабування до необхідного обсягу);
- підтримка великої кількості систем безпеки та API постачальників (локальних та хмарних);

- збір подій за допомогою агентів Windows, моніторинг цілісності файлів, змін встановлених програм та змін реєстру; моніторинг цілісності файлів за допомогою агентів Linux;
- створення та зміна засобів синтаксичного аналізу (шаблонів XML) у рамках графічного інтерфейсу та надання доступу іншим користувачам за допомогою функції експорту/імпорту.

Сповіщення і управління інцидентами:

- побудова інфраструктури повідомлення про інциденти на основі політик; можливість запуску сценарію оновлення у разі виникнення вказаного інциденту;
- інтеграція на основі API з зовнішніми системами відправки запитів
- ServiceNow , ConnectWise і Remedy;
- вбудована система надсилання запитів. Надання користувачеві повнофункціональних панелей моніторингу, що настроюються: в режимі реального часу панелі моніторингу з функцією прокручування слайд-шоу для показу ключових показників ефективності;
- генерація звітів та аналітичних даних, доступних для колективного використання співробітниками організацій та користувачами;
- колірне маркування для оперативного виявлення критичних проблем;
- спеціалізовані багаторівневі панелі моніторингу для бізнес-служб, віртуалізованих інфраструктур та спеціальних додатків.

Інтеграція зовнішніх даних про погроз:

- надання API для інтеграції зовнішніх джерел даних про загрози — домени зі шкідливими програмами, IP-адресами, URL-адресами, хешами, вузлами Tor;
- інтеграція популярних джерел даних про загрози - ThreatStream, CyberArk, SANS, Zeus ;
- технологія обробки великих обсягів даних про загрози - додаткове завантаження та розповсюдження в рамках кластера, зіставлення шаблонів з мережевим трафіком у режимі реального часу.

Надання масштабованої функції аналізу:

- пошук подій в режимі реального часу;
- пошук за ключовим словом та обробленими атрибутами події; пошук історичних подій - запити за типом SQL з булевими умовами фільтрації, угруповання за відповідними агрегуваннями, фільтрація в залежності від часу доби, зіставлення регулярних виразів, вирази, що обчислюються - графічний інтерфейс і API;
- тригер для шаблонів складних подій у режимі реального часу; використання виявлених об'єктів CMDB, даних користувача/посвідчення та відомостей про розташування у процесі пошуку та створення правил;
- планування складання звітів та доставка результатів ключовим співробітникам за допомогою електронної пошти; пошук подій у рамках усієї корпоративної мережі або фізичного чи логічного домену складання звітів;
- списки відстеження, що динамічно змінюються, призначені для виявлення критичних порушень — підтримується використання списків відстеження для створення правил складання звітів; масштабування каналів аналітичних даних за рахунок додавання робочих вузлів без простою;
- можливість розгортання функції визначення пріоритету у процесі складання звітів про інцидентах з допомогою критичних бізнес-служб.

Архітектура FortiSIEM (показана рисунку 2.2) є ієрархічну структуру, яка будується з урахуванням різних елементів залежно від розташування системи (власна інфраструктура, хмара, ЦОД) і обсягу оброблюваних даних [9].

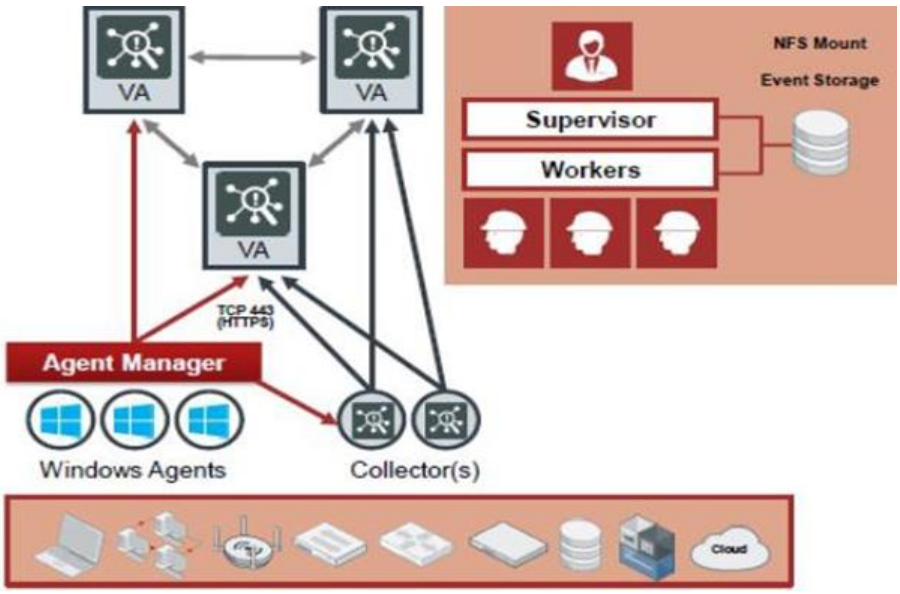

Рис. 2.2. Архітектури FortiSIEM

Основним елементом FortiSIEM є супервізор (Supervisor), на якому розташовуються всі служби з обробки, веб-сервер, сервер додатків, сервер баз даних, інтерфейс рішення. Далі йдуть обробники (Workers), які займаються аналітикою та відповідають за частину подій безпеки, знімаючи навантаження із супервізора. Наступним елементом архітектури є колектори (Collectors), що збирають та нормалізують події на віддалених вузлах для подальшої передачі даних з інфраструктури на обробники та супервізор [9].

2.2. Впровадження SIEM системи

В даний час існує безліч систем моніторингу мережі. Конкуренція серед вендорів систем на тлі зростання в Україні інформаційних атак на інформаційні системи призвели до масштабного впровадження такої системи як "SIEM".

Сценарії впровадження FortiSIEM. Архітектура FortiSIEM передбачає низку варіантів впровадження для підприємств будь-якого масштабу та постачальників послуг. Використання автономного супервізора — «Все-в-одному» Це найпростіший варіант розгортання, в якому один супервізор здійснює всю роботу зі збирання, моніторингу, обробки та аналізу даних та відстеження виникаючих інцидентів безпеки. Супервізор може використовувати локальне або NFS-сховища залежно від вимог до

сховища даних подій. Для підвищення точності моніторингу на робочих станціях та серверах можуть використовуватися Windows Agents та Agent Manager. Схема сценарію застосування супервізора представлена рисунку 2.3.

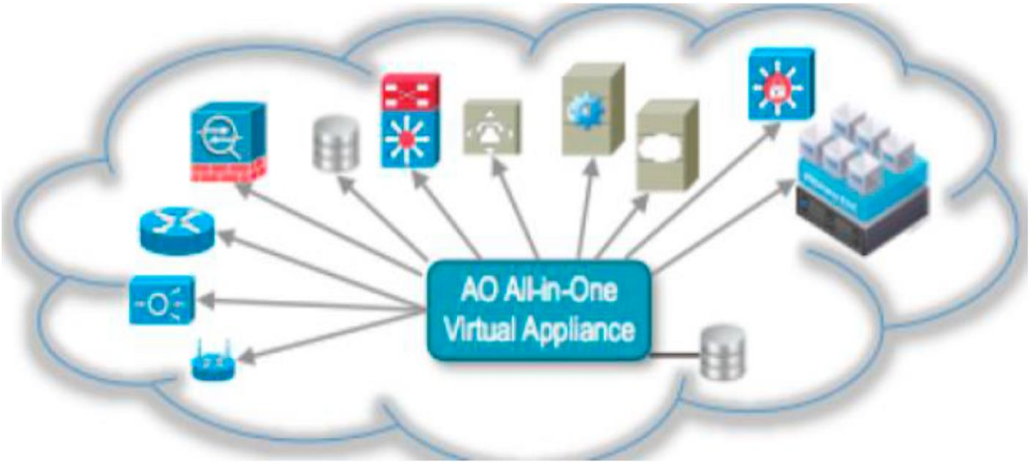

Рис. 2.3. Сценарій впровадження супервізора всі в одному

Оскільки продукт Forti є комерційним, для отримання ліцензії необхідно зробити запит на отримання ліцензії SIEM-системи. В даному випадку був зроблений запит на хмарний сервіс all -in- all . Процес отримання доступу показано рисунку 2.4. Головна сторінка хмарного сервісу представлена рисунку 2.5.

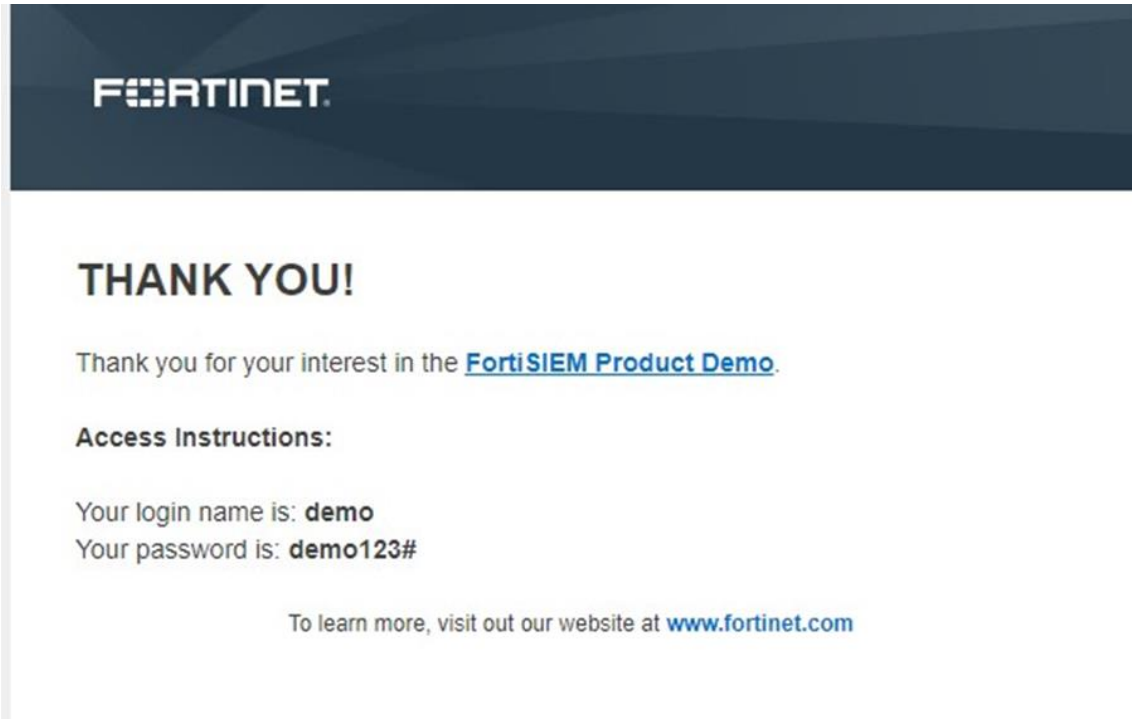

Рис. 2.4. Отримання доступу до SIEM

Рис. 2.5. Хмарний сервіс

2.3. Веб інтерфейс системи

Інтерфейс дозволяє здійснювати поточний моніторинг подій на будь-якому пристрої, великих екранах і плазмових панелях. Відображення виконується за панелями (Dashboard) або інцидентами (Incidents) та різними критеріями. Цей розділ показує повне уявлення про всі компоненти, таких як серйозність загрози, вразливості в мережевому вузлі, стан розгортання, карти ризиків та статистика OTX. Підменю дашборда показані нижче.

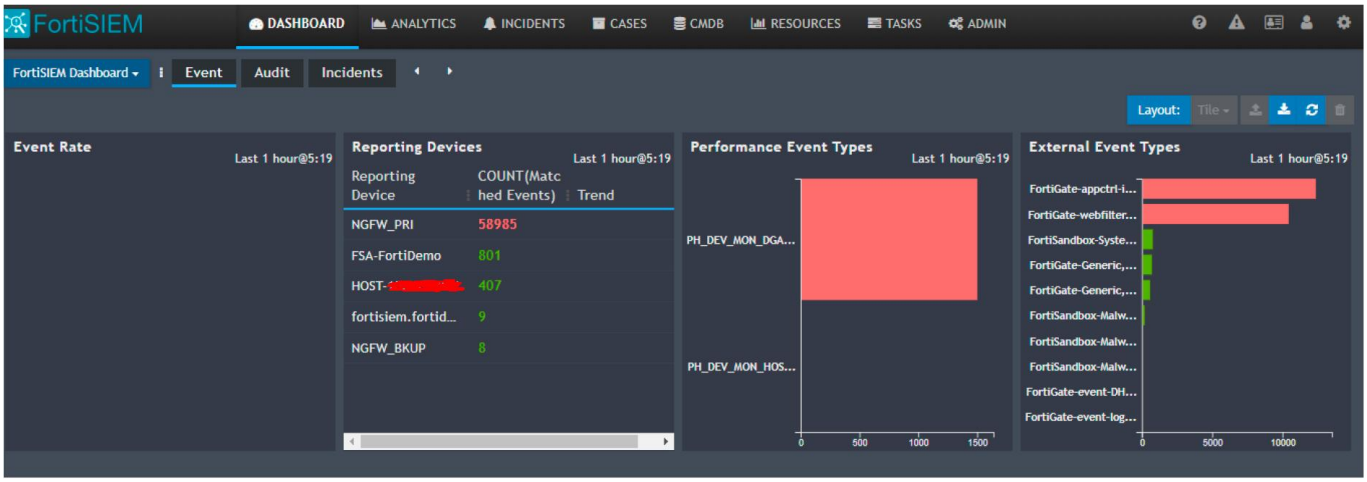

Рис. 2.6. Dashboard

Рис. 2.7. Інциденти

Наступне вікно з'явиться у налаштуваннях особистих даних. Змінимо пароль та ім'я користувача та заповнимо контактні дані для оповіщення про події ІБ.

Панель інструментів віджетів відображає графічне представлення звітів FortiSIEM. Звіти можуть бути з даних CMDB або даних подій. Звіти можуть бути агрегованими звітами типу Top N або неагрегованими, ймовірно, з необробленими повідомленнями. Агреговані звіти можуть відображатися у різних формах: гаджети, стовпчики, таблиці, лінії, складові лінії, точкові діаграми, теплові карти, деревоподібні карти та геокарти [11].

На даному етапі виконується автоматичне виявлення мережних пристроїв у вкладці CMDB, представленій на рис. 2.8. Воно підтримує автоматичне та ручне виявлення пристроїв.

Є три типу хостів у системі:

- Windows;
- Linux;
- мережеве пристрій.

Виявлено пристрої.: брендмауери і машини з ОС Лінукс.

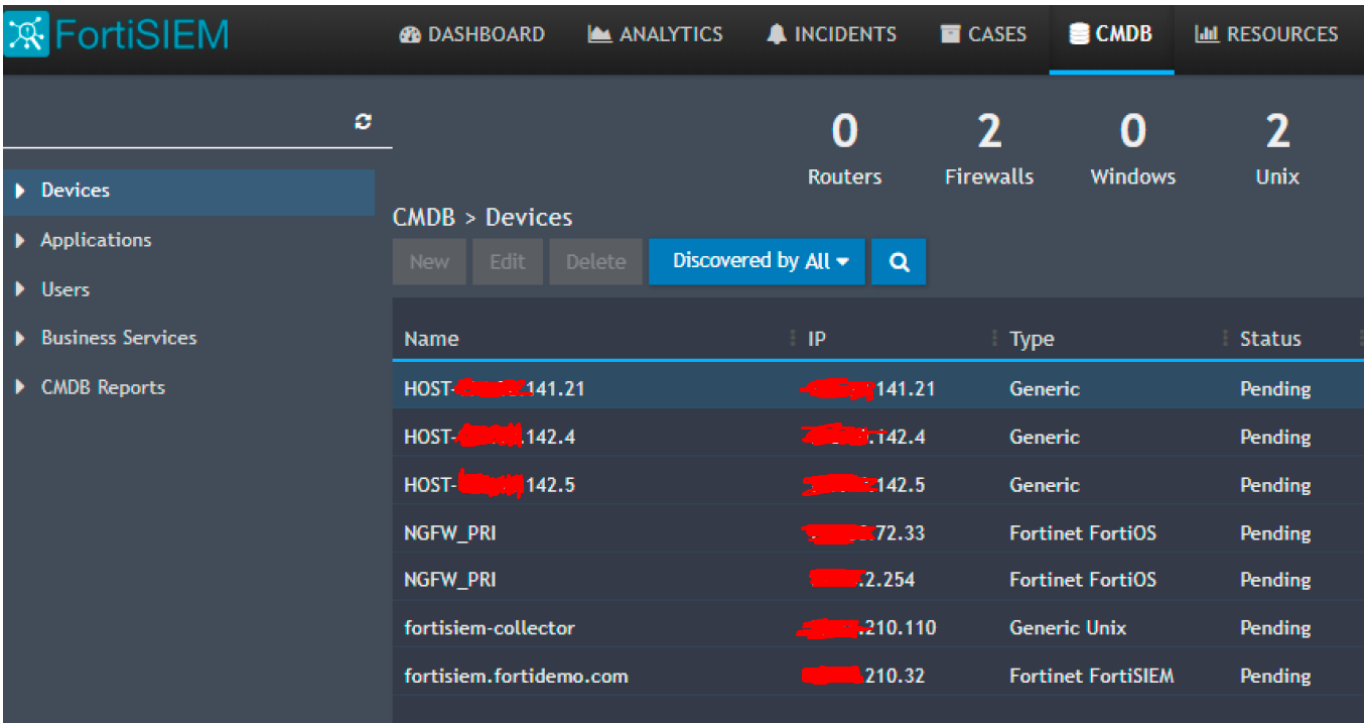

Рис. 2.8. CMDB

Усі інциденти поділені за категоріями. Наведено низку можливих інцидентів та складено топ виявлених погроз. За кожною виявленою загрозою створюється звіт, один із них представлений на рисунках нижче.

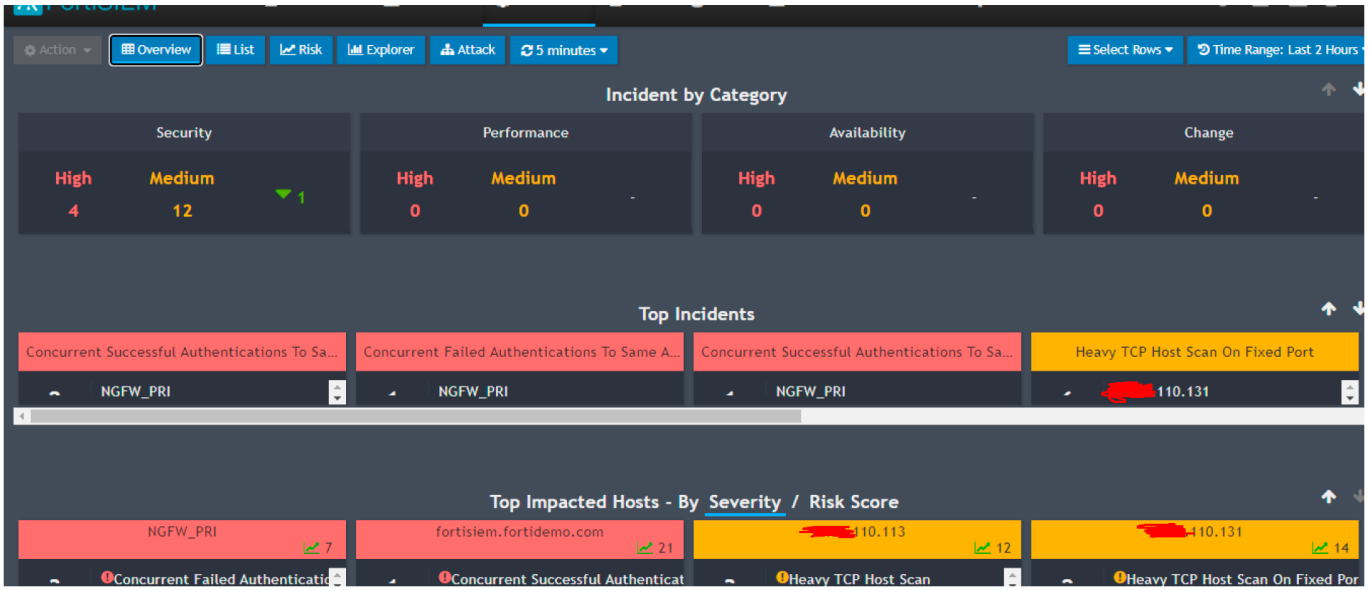

Рис. 2.9. Категорії інцидентів

Аналітика є дуже важливою складовою будь-якого пристрою SIEM. SIEM проаналізує хости на основі їх логів. Це меню показує сигнали тривоги, SIEM (події безпеки), тикети та необроблені логи.

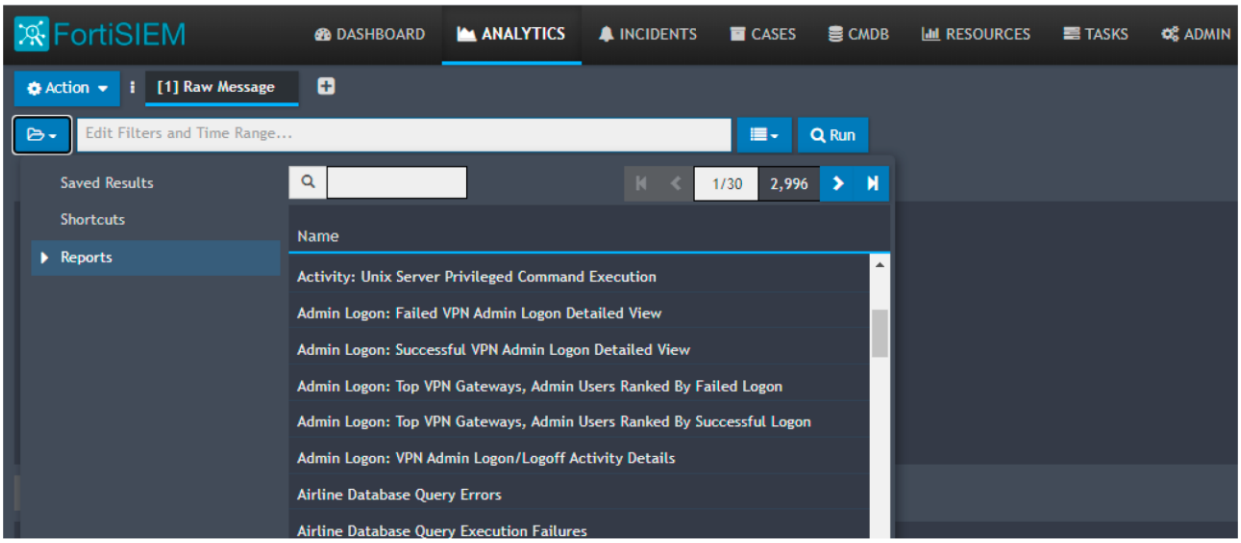

Рис. 2.10. Розділ аналітики

2.4. Неавторизований Вхід

Здійснимо спробу неавторизованого входу до SIEM. Для цього вводиться неправильний пароль. Як можна, можливо побачити, через кілька спроб невдалого входу SIEM блокує обліковий запис (наведено на рисунках нижче) [11].

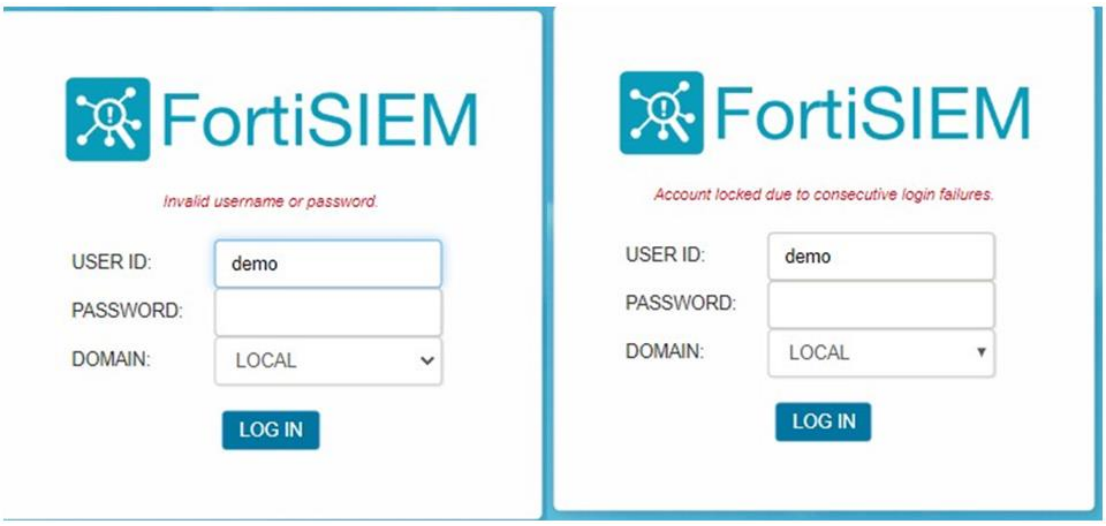

Рис. 2.11. Спроба входу та блокування акаунту

Щоб розблокувати обліковий запис необхідно написати листа в службу підтримки компанії Forti. Після чого було відновлено обліковий запис і вдалося увійти в систему. Далі буде розбір інциденту. У вкладці Dashboard видно, що було здійснено спроби невдалого входу у систему (рисунок 2.12). Далі переходимо у вкладку інцидентів для отримання подробиць. Деталі звіту представлені нижче.

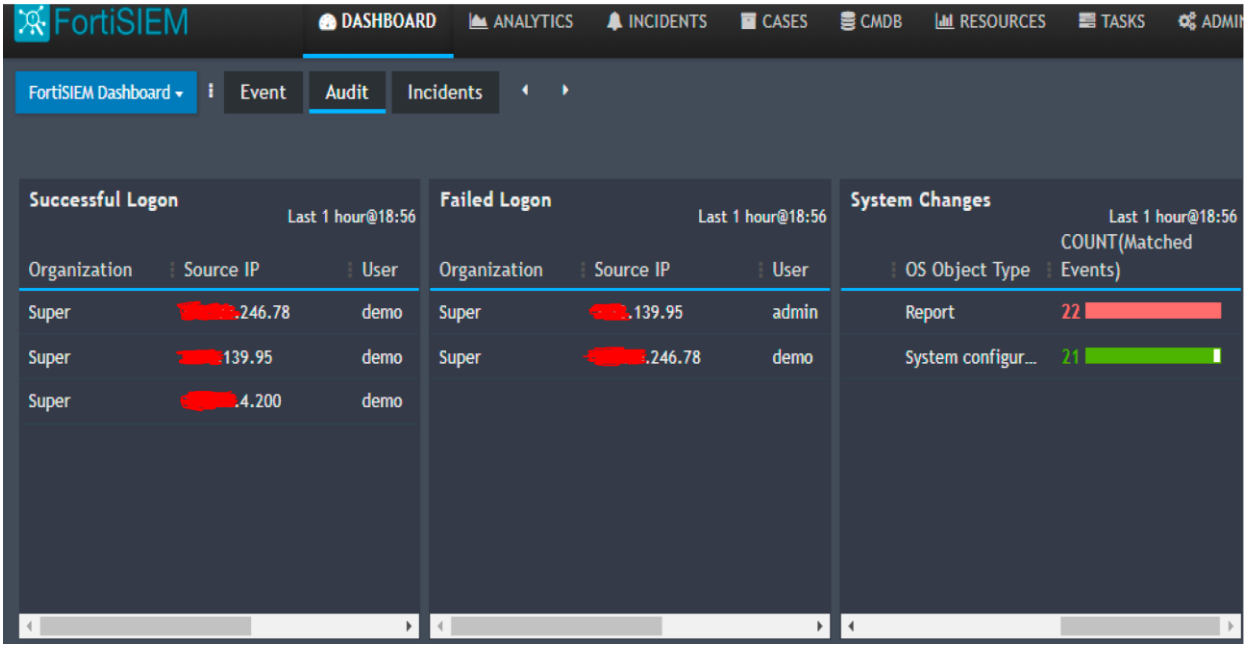

Рис. 2.12. Аудит системи

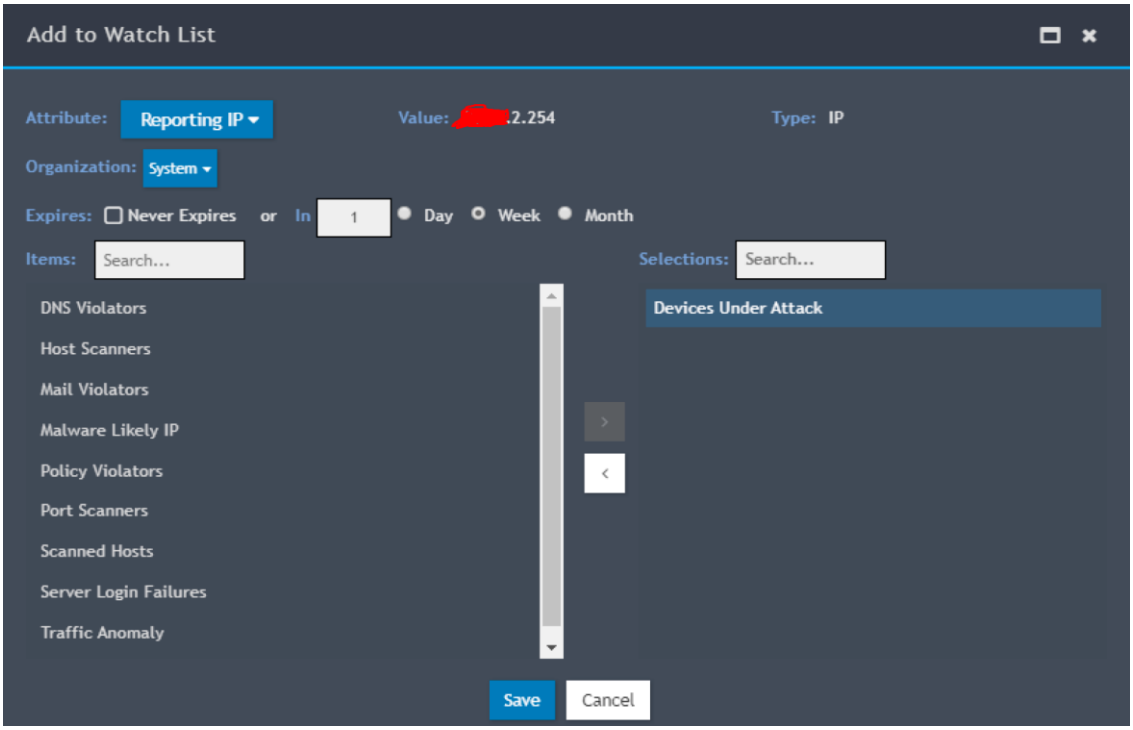

Рис. 2.13. Пристрій під атакою

Для виявлення порушника необхідно створити звіт. У вкладці аналітики створюємо звіт. У звіті зазначено, що була спроба невдалого входу та вжиті заходи у вигляді блокування облікового запису. Створимо логи для детального перегляду.

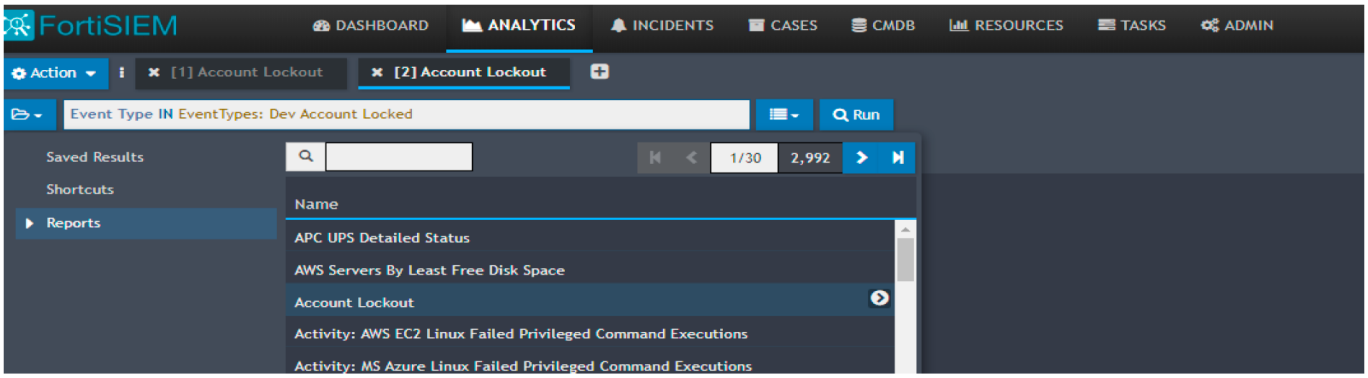

Рис. 2.14. Звіт про інциденти ІБ

У звіті можна побачити IP-адресу порушника. Далі по IP у SIEM є можливість дізнатися докладніші дані про порушника.

SIEM система вжила заходів у вигляді блокування облікового запису, далі вдалося дізнатися дані про порушника. Щоб уникнути наступних блокувань облікового запису, потрібно дозволити вхід до SIEM лише конкретної підмережі. Для цього потрібно підняти VPN-сервер. Це дасть можливість вирішення проблем, що масштабуються, пов'язаних з інцидентом. Тобто залучення співробітників із різних регіонів за допомогою захищеного підключення VPN.

2.5. створіння VPN-сервера

За допомогою звичайного Інтернет-з'єднання між пристроєм та VPN-сервером встановлюється спеціальне з'єднання - VPN-тунель. Всі передані та отримані дані в цьому з'єднанні шифруються. З цього моменту вся ваша мережева активність здійснюється через даний тунель, а не через основний канал провайдера, і з'являється можливість авторизованого входу в SIEM.

Для того щоб створити VPN-сервер, необхідно орендувати віртуальний сервер (Virtual Private Server) у одного з хостинг-провайдерів. На нього потрібно

встановити Linux і налаштувати його. З найбільш популярних на сьогоднішній день глобальних хостингових компаній можна виділити такі:

- Amazon Web Services ;
- DigitalOcean ;
- Hetzner ;
- Vultr ;
- Bluehost ;
- ArubaCloud .

Вибір упав **Amazon Web Services (AWS)**. В основному, через популярність бренду, велику кількість доступних географічних зон для розміщення сервера та високої стабільності. Насправді багато популярних інтернет-сервісів працюють на базі AWS, орендуючи там сервери для своїх потреб, наприклад, Facebook. Компанія AWS була піонером у хмарних технологіях і по суті відкрила цю галузь. Сьогодні AWS надає безліч рішень для хмарних обчислень на будь-який вибір та гаманець, але для подальшого виконання потрібна звичайна віртуальна машина. Для цього можна скористатися однією з розробок AWS: Lightsail .

Lightsail - це спрощене рішення для створення віртуальних серверів, на відміну від старшого побратима EC2. Все загорнуто в дуже простий інтерфейс, в якому розбереться навіть новачок, тому для мети створення VPN-сервера, AWS Lightsail підходить найкраще.

Підніматися VPN-сервер буде на основі операційної системи Linux Debian, а не Linux Ubuntu, яку часто використовують. Ubuntu спочатку створювалася саме як користувальницька система, а не серверна. Debian надійний і стабільний. Установка показана рисунку 2.15 [12].

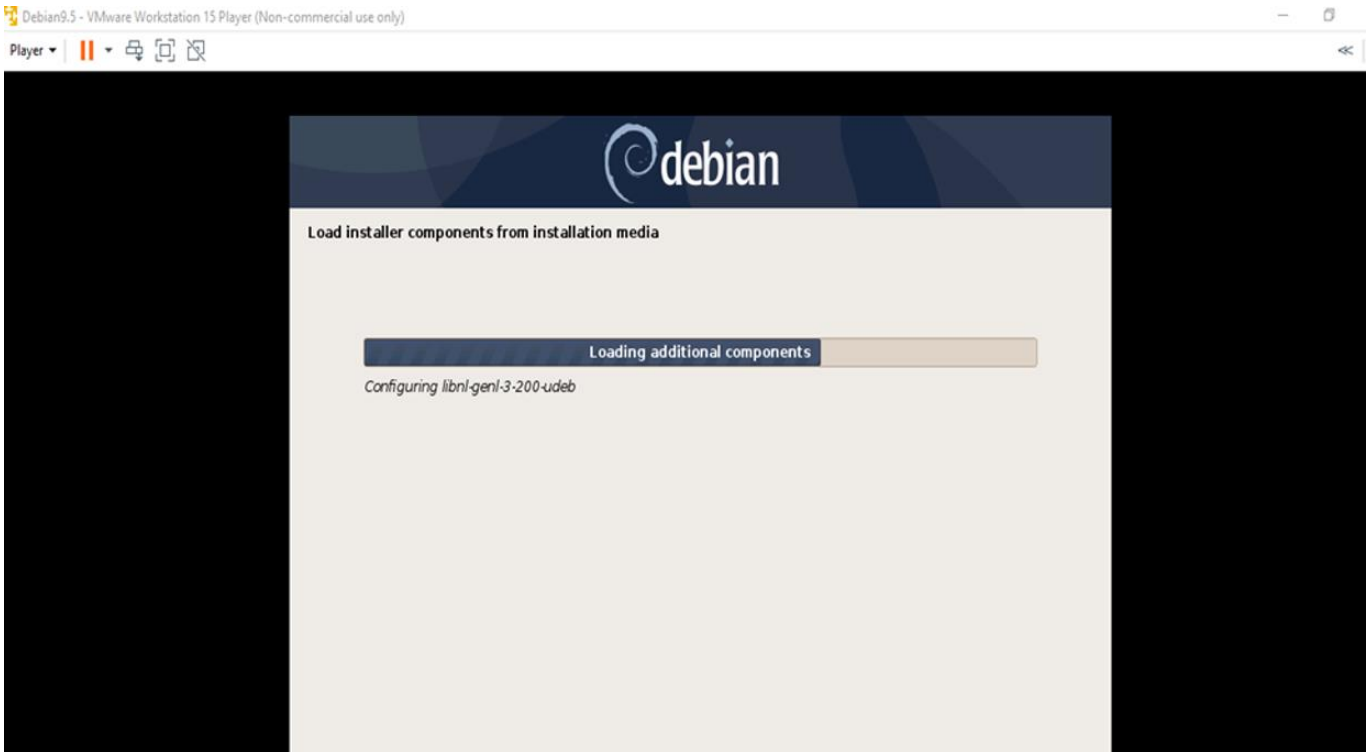

Рис. 2.15. Встановлення Debian 9.5

На сьогоднішній день існують різні протоколи VPN-з'єднання. Серед них найбільш популярні IPsec IKEv2 та OpenVPN. Обидва протоколи хороші і надійні, але використовуватиметься IKEv2, оскільки OpenVPN має істотний недолік, який перекриває його інші переваги. OpenVPN вимагає встановлення своєї програми, яка завжди повинна бути запущена на пристроях, що, по-перше, незручно у використанні, а, по-друге, додатково витрачає батарею iPhone, iPad і, меншою мірою, Mac. IKEv2 ж "вшитий" в iOS, iPadOS, macOS та Android і є для них нативним, не вимагаючи встановлення жодного додаткового ПЗ. Як серверну частину ми будемо використовувати StrongSwan - популярний VPN-сервер для Linux.

Таким чином, VPN-сервер буде підніматися, використовуючи такі технології:

- AWS Lightsail в якості віртуального сервера;
- IKEv2 як протокол VPN;
- Linux Debian в якості серверної ОС;
- StrongSwan в якості VPN- сервера.

Після реєстрації необхідно перейти в Lightsail, вибирати гео-зону, в якій необхідно підняти VPN-сервер. Було створено новий інстанс, і вибрано OS Only та операційну систему Debian 9.5 (рис. 2.16).

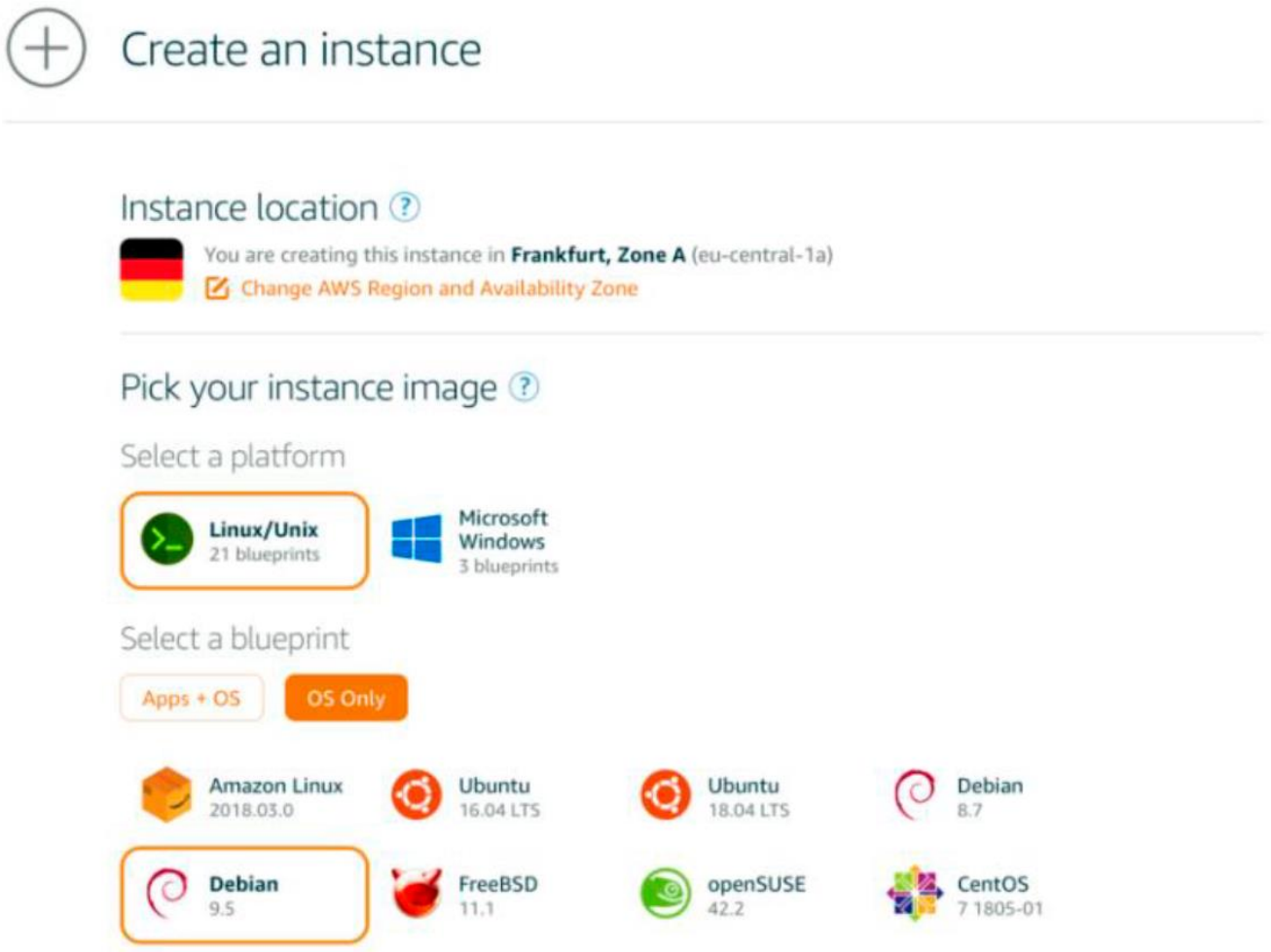

Рис. 2.16. Вибір Debian

Деякі сайти необґрунтовано блокують візити з IP-адрес популярних хостерів, вважаючи, що останні часто беруть участь у DDOS-атаках. Щоб цього не відбувалося і щоб не ділили одну IP-адресу з тисячами інших машин AWS, потрібно перейти в "Networking " і виділити Static IP.

Далі необхідно завантажити SSH key для клієнта сервера. Надалі підключення до сервера без ключа не буде доступним.

Рис. 2.17. Завантаження ключа SSH

Далі всі налаштування будуть здійснюватися в Debian. Переходимо ОС Лінукс. Необхідно зайти під ROOT. Для початку необхідно встановити StrongSwan.

До детального налаштування StrongSwan трохи пізніше, а поки що будуть створені сертифікати, щоб пристрої змогли підключитися через VPN. Використовуватимуться самозавірені сертифікати, оскільки VPN-сервером плануємо використовувати лише довірені користувачі SIEM. Для створення сертифікатів потрібно пакет `strongswan-pki`.

Далі потрібно створити сертифікати. Насамперед потрібно створити кореневий сертифікат, він же “CA” (Certificate Authority), який випустить решту сертифікатів. Створюється у файлі `ca.pem`.

Далі необхідно створити сертифікат для VPN-сервера в файлі `debian.pem`.

```
        --nc-permitted    (-n)  add permitted NameConstraint
        --nc-excluded     (-N)  add excluded NameConstraint
        --cert-policy     (-P)  certificatePolicy OID to include
        --cps-uri         (-C)  Certification Practice statement URI for certifi
catePolicy
        --user-notice     (-U)  user notice for certificatePolicy
        --policy-mapping  (-M)  policyMapping from issuer to subject OID
        --policy-explicit (-E)  requireExplicitPolicy constraint
        --policy-inhibit  (-H)  inhibitPolicyMapping constraint
        --policy-any      (-A)  inhibitAnyPolicy constraint
        --flag            (-e)  include extendedKeyUsage flag
        --crl             (-u)  CRL distribution point URI to include
        --crlissuer       (-I)  CRL Issuer for CRL at distribution point
        --ocsp            (-o)  OCSP AuthorityInfoAccess URI to include
        --digest          (-g)  digest for signature creation, default: key-spec
ific
        --outform         (-f)  encoding of generated cert, default: der
        --debug           (-v)  set debug level, default: 1
        --options         (-+)  read command line options from file
root@debianvpn:/etc/ipsec.d# ipsec pki --pub --in private/debian.pem --type rsa
| ipsec pki --issue --lifetime 3650 --digest sha256 --cacert cacerts/ca.pem --ca
key private/ca.pem --dn "CN=YOUR_LIGHTSAIL_IP" --san YOUR_LIGHTSAIL_IP --flag se
rverAuth --outform pem > certs/debian.pem
root@debianvpn:/etc/ipsec.d#
```

Рис. 2.18. Успішне встановлення VPN-сервера

А тепер, буде створено сертифікат для пристроїв в файлі (Рис. 2.19) `me.pem`.

```
strongSwan 5.5.1 PKI tool
usage:
  pki --gen   [--type rsa|ecdsa|bliss] [--size bits] [--safe-primes]
              [--shares n] [--threshold l] [--outform der|pem]
        --help            (-h)  show usage information
        --type            (-t)  type of key, default: rsa
        --size            (-s)  keylength in bits, default: rsa 2048, ecdsa 384,
 bliss 1
        --safe-primes     (-p)  generate rsa safe primes
        --shares          (-n)  number of private rsa key shares
        --threshold       (-l)  minimum number of participating rsa key shares
        --outform         (-f)  encoding of generated private key, default: der
        --debug           (-v)  set debug level, default: 1
        --options         (-+)  read command line options from file
root@debianvpn:/etc/ipsec.d# ipsec pki --gen --type rsa --size 4096 --outform pe
m > private/me.pem
root@debianvpn:/etc/ipsec.d# ipsec pki --pub --in private/me.pem --type rsa |
> ipsec pki --issue --lifetime 3650 --digest sha256 \
> --cacert cacerts/ca.pem --cakey private/ca.pem \
> --dn "CN=me" --san me \
> --flag clientAuth \
> --outform pem > certs/me.pem
root@debianvpn:/etc/ipsec.d#
```

Рис. 2.19. Створіння сертифіката для пристроїв

У цьому створення сертифікатів завершено. Далі буде проводитися налаштування StrongSwan. Вставимо зовнішню IP-адресу машини в AWS Lightsail на Рис. 2.20.

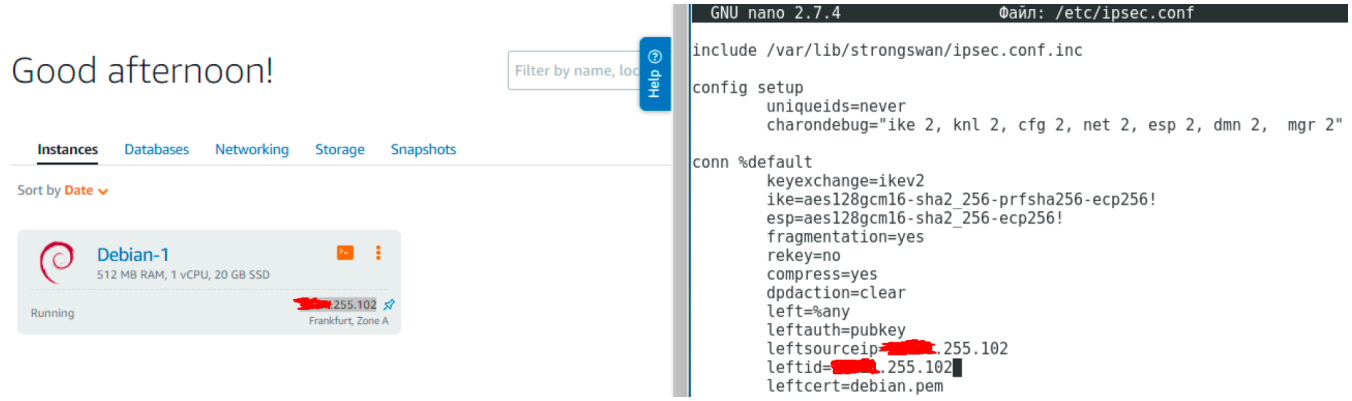

Рис. 2.20. Налаштування StrongSwan

Після збереження файлу йде додавання покажчиків на сертифікат сервера файл `ipsec.secrets`,
що є сховищем посилань на сертифікати і ключі аутентифікації (Рис. 2.22).

```
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created $
include /var/lib/strongswan/ipsec.secrets.inc

:RSA debian.pem
```

Рис. 2.22. Додавання посилання на сертифікат

Налаштування StrongSwan завершено. При перезапуску системи видно, що сервер запустився (Рис. 2.23). Далі необхідно налаштувати параметри мережі ядра.

```
###################################################################
# Magic system request Key
# 0=disable, 1=enable all
# Debian kernels have this set to 0 (disable the key)
# See https://www.kernel.org/doc/Documentation/sysrq.txt
# for what other values do
#kernel.sysrq=1

###################################################################
# Protected links
#
# Protects against creating or following links under certain conditions
# Debian kernels have both set to 1 (restricted)
# See https://www.kernel.org/doc/Documentation/sysctl/fs.txt
#fs.protected_hardlinks=0
#fs.protected_symlinks=0

net.ipv4.ip_no_pmtu_disc = 1
```

Рис. 2.23. Мережеві параметри ядра

На цьому налаштування параметрів мережі ядра закінчено. Далі буде проведено налаштування Iptables.

Iptables - це утиліта, яка управляє вбудованим у Linux файрволом netfilter. Для того, щоб зберігати правила iptables у файлі та підвантажувати їх під час кожного запуску системи, потрібно встановити пакет

`iptables-persistent`.

Далі формуються правила iptables. Для початку потрібно очистити всі ланцюжки.

Дається дозвіл для з'єднання SSH на 22 порту, щоб доступ до машини не був втрачений, дається дозвіл з'єднання на loopback-interface і вхідні ipsec- з'єднання на UDP-портах 4500 і 500.

Далі йде налаштування максимального розміру сегмента пакетів та заборона на всі інші з'єднання до сервера, крім використовуваного.

На цьому налаштування Iptables закінчено. Потрібно перезавантажити машину. Перегляд правила Iptables та працездатність StrongSwan (Рис. 2.24-2.25).

```
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m udp --dport 500 -j ACCEPT
-A INPUT -p udp -m udp --dport 4500 -j ACCEPT
-A INPUT -j DROP
-A FORWARD -s 10.10.10.0/24 -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A FORWARD -d 10.10.10.0/24 -m policy --dir out --pol ipsec --proto esp -j ACCEP
T
-A FORWARD -j DROP
```

Рис. 2.24. Результат налаштувань Ipsec

```
  malloc: sbrk 1343488, mmap 0, used 411760, free 931728
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled:
 0
  loaded plugins: charon aesni aes rc2 sha2 sha1 md5 random nonce x509 revocatio
n constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips
-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark
 stroke updown
Virtual IP pools (size/online/offline):
  10.10.10.0/24: 254/0/0
Listening IP addresses:
  [redacted].233.132
Connections:
ikev2-pubkey:  %any...%any  IKEv2, dpddelay=30s
ikev2-pubkey:   local:  [CN=YOUR_LIGHTSAIL_IP] uses public key authentication
ikev2-pubkey:    cert:  "CN=YOUR_LIGHTSAIL_IP"
ikev2-pubkey:   remote: uses public key authentication
ikev2-pubkey:   child:  0.0.0.0/0 === dynamic TUNNEL, dpdaction=clear
Security Associations (0 up, 0 connecting):
  none
```

Рис. 2.25. StrongSwan

Після переконання, що всі налаштування працюють, необхідно дати Розширення з'єднання в файрволі lightstail. AWS Lightsail використовує власний файрвол для захисту віртуальних машин Налаштування фаєрволу представлено Рис. 2.26.

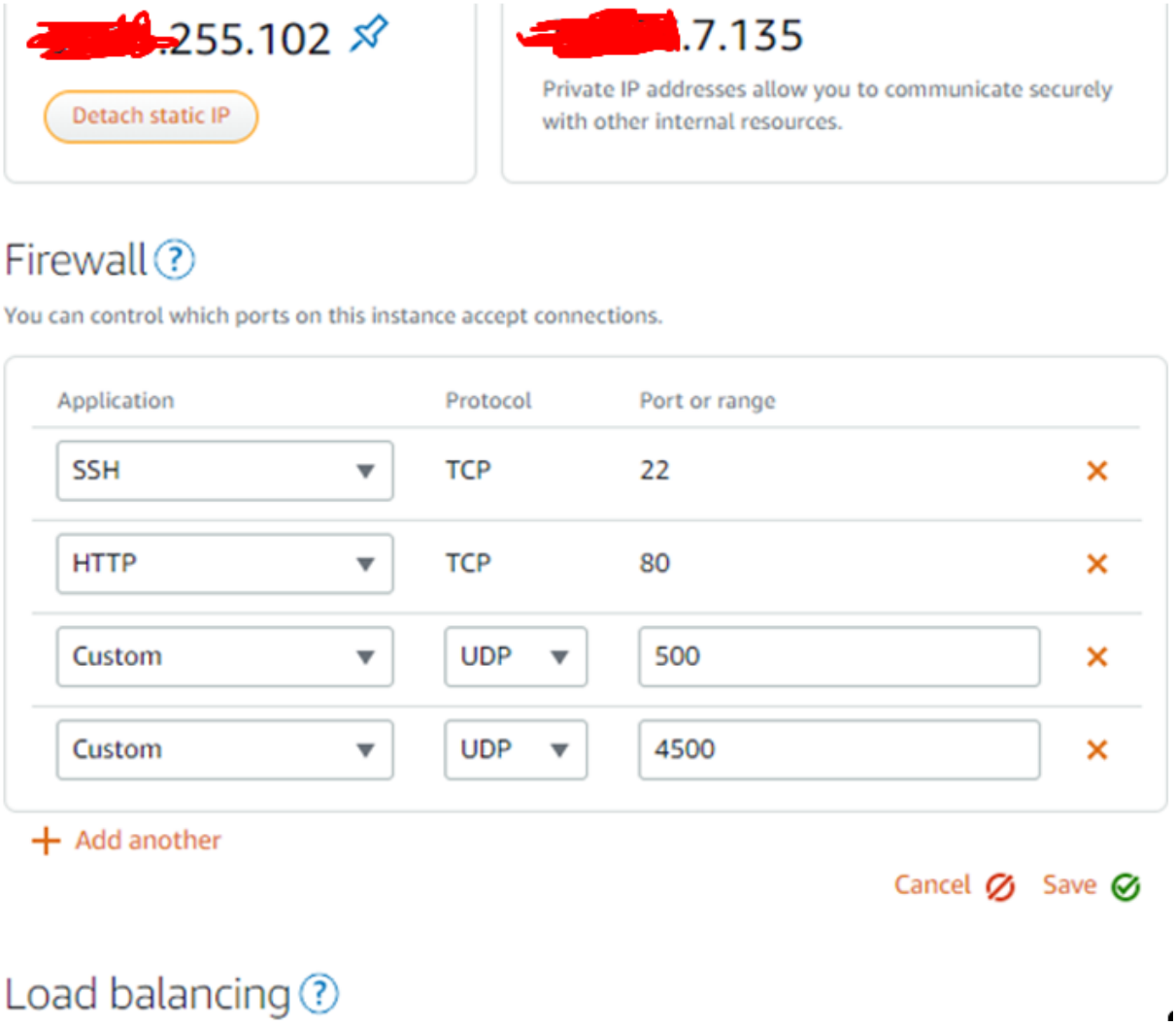

Рис. 2.26. Налаштування файрвола в lightstail

В самому кінці створюємо Mobileconfig для клієнтів. Буде використаний один VPN-профайл. Mobileconfig для всіх пристроїв. Створення конфігураційного файлу показано на Рис. 2.27. Після цього налаштування повністю завершене. Система FortiSIEM готова до використання.

```
#!/bin/zsh

CLIENT="me"
SERVER="AWS Frankfurt"
FQDN="YOUR_LIGHTSAIL_IP"
CA="ca"

# WiFi SSIDs that do not require automatic connection to VPN on network change
TRUSTED_SSIDS=("SSID1" "SSID2")

PAYLOADCERTIFICATEUUID=$( cat /proc/sys/kernel/random/uuid )
PKCS12PASSWORD=$( cat /proc/sys/kernel/random/uuid )

cat << EOF
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs$
<plist version="1.0">
<dict>
    <key>PayloadDisplayName</key>
```

Рис. 2.27. Скрипт

```
  malloc: sbrk 1613824, mmap 0, used 416208, free 1197616
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled:
 0
  loaded plugins: charon aesni aes rc2 sha2 sha1 md5 random nonce x509 revocatio
n constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips
-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark
 stroke updown
Virtual IP pools (size/online/offline):
  10.10.10.0/24: 254/0/0
Listening IP addresses:
  [redacted].233.132
Connections:
ikev2-pubkey:  %any...%any  IKEv2, dpddelay=30s
ikev2-pubkey:   local:  [CN=YOUR_LIGHTSAIL_IP] uses public key authentication
ikev2-pubkey:    cert:  "CN=YOUR_LIGHTSAIL_IP"
ikev2-pubkey:   remote: uses public key authentication
ikev2-pubkey:   child:  0.0.0.0/0 === dynamic TUNNEL, dpdaction=clear
Security Associations (0 up, 0 connecting):
  none
```

Рис. 2.28. Завершення налаштувань та увімкнення сервера

РОЗДІЛ 3
АНАЛІЗ І ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Ідентифікація активів

З метою аналізу та розрахунку ризиків інформаційної безпеки насамперед необхідно провести інвентаризацію інформаційних активів, що підлягають захисту. Серед них, спираючись на специфіку теми кваліфікаційної роботи, для аналізу та розрахунку ризиків було виділено три активи: внутрішня (локальна) мережа, VPN-сервер, веб-додатки.

Захищені активи та ризики були обрані виходячи з того, що робота присвячена переважно розбору та аналізу можливостей SIEM-системи.

Список інформаційних активів, що захищаються:

- внутрішня мережа компанії – актив був обраний, оскільки можливості моніторингу SIEM-системи спрямовані здебільшого саме на реєстрацію підозрілої активності в мережі, що захищається;
- VPN-сервер - це важливий елемент мережевої інфраструктури компанії, а також на ньому і розташовується SIEM-система;
- веб-додатки – саме через додатки (часто це саме веб-додатки) клієнт взаємодіє з сервером, тому важливо здійснювати моніторинг підозрілої активності даного елемента мережевої інфраструктури за допомогою SIEM-системи, наприклад, SIEM-система – **це засіб моніторингу, а не засіб захисту**. Проте вона є важливим елементом забезпечення інформаційної безпеки. Знання про підозрілу активність дозволяють визначити, де необхідно впровадити захисні заходи (або посилити їх, якщо сама наявність інциденту свідчить про їх неефективність). Підозрілаа активність, зареєстрована SIEM-системою може бути перервана засобами захисту. Саме тому при аналізі деяких вибраних ризиків було вказано моніторинг SIEM-системою разом із іншими захисними засобами.

3.2. Аналіз і оцінка ризиків

Для аналізу та оцінки ризиків було обрано алгоритм, представлений у стандарті ISO-27005. Розрахунок за цим алгоритмом (виходячи з цінності активу, ступеня ймовірності виникнення загрози та простоти використання вразливості) здійснюється на основі додатка Е стандарту ISO-27005. Алгоритм оцінки ризиків представлений у таблиці 3.1.

Таблиця 3.1.

Цінність активів, рівні погроз та вразливостей

Ймовірність загрози		Низька			Середня			Висока		
Простота використання		Н	З	У	Н	З	У	Н	З	У
Цінність активів	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Простий загальний рейтинг ризиків:

- низький ризик (прийнятний): 0-2 ;
- середній ризик: 3-5 ;
- високий ризик (Неприйнятний): 6-8 .

Аналіз ризиків (загроз і уразливостей) інформаційної безпеки для перерахованих вище активів представлений у таблицях 3.2-3.4.

Таблиця 3.2.

Аналіз і оцінка ризиків інформаційної безпеки

Актив 1: Внутрішня (локальна) мережа компанії

Загрози	**Вразливості**	**Максимальний рівень ризику**	**Заходи по обробці ризику**	**Залишковий рівень ризику**	**Коментарі, ресурси, відповідальні**
Мережева розвідка і, як наслідок, збирання критичної інформації по мережевій інфраструктурі	Відсутність системи виявлення вторгнень. Некоректне налаштування міжмережевого екрану	7	SIEM як засіб моніторингу підозрілої активності та фільтрація трафіку за допомогою міжмережевого екрану	1	Мережевий адміністратор
Атака "man -in- the - middle"; як слідство, перехоплення та модифікація даних , що передаються по мережі	Відсутність захисту трафіку, що передається . Відсутність шифрування трафіку	7	SIEM – для моніторингу спроб перехоплення. Шифрування трафіку, використання VPN - для запобігання перехопленню	1	Мережевий адміністратор
DDOS-атака; як наслідок - відмова в обслуговуванні елемента мережі	Відсутність обмеження обсягу трафіку	8	SIEM – для реєстрації спроб DDOS + аналізатор окремих пакетів трафіку на предмет того, чи є він дозволеним	2	Мережевий адміністратор
IP - спуфінг і, як наслідок, вставка несправжньої інформації в потік даних між клієнтом та сервером	Відсутність контролю керування мережним доступом	6	SIEM – для реєстрації спроб IP- спуфінгу . Система контролю керування доступом – для запобігання подальших інцидентів	1	Мережевий адміністратор
Отримання можливості віддаленого управління комп'ютером мережі	Неправильна конфігурація фаєрволу (фаєрвол пропускає нелегітимний трафік)	5	SIEM – для реєстрації підозрілого трафіку. Потім – застосування міжмережевого екрана	1	Мережевий адміністратор

Таблиця 3.3.

Аналіз і оцінка ризиків інформаційної безпеки

Актив 2: VPN-сервер

Загрози	**Вразливості**	**Максимальний рівень ризику**	**Заходи по обробці ризику**	**Залишковий рівень ризику**	**Коментарі, ресурси, відповідальні**
Несанкціонована автентифікація на сервері. Компрометація облікових записів користувачів та адміністраторів сервера	Відсутність моніторингу підозрілої активності на сервері	8	Впровадження системи моніторингу	2	Системний адміністратор
Зараження сервера "троянським конем". Слідство - шпигунство за діями над сервером	Відсутність антивірусної програми на сервері	7	SIEM – для моніторингу інцидентів, пов'язаних із зараженням станцій вірусами та "троянами". Використання антивірусу	1	Системний адміністратор
Впровадження на сервер rootkit- а	Некоректне налаштування міжмережевого екрану. Відсутність антирукітів	5	Використання антируткіту	1	Системний адміністратор

Таблиця 3.4.

Аналіз і оцінка ризиків інформаційної безпеки

Актив 3: Веб-програми компанії

Загрози	**Вразливості**	**Максимальний рівень ризику**	**Заходи по обробці ризику**	**Залишковий рівень ризику**	**Коментарі, ресурси, відповідальні**
Зберігається XSS- атака	Відсутність фільтрації спецсимволів у формах веб- програми	5	Використання SIEM для реєстрації підозрілої активності у веб-додатку. Потім – коректна фільтрація спецсимволів у веб-додатках	1	Розробник веб- програми
SQL-ін'єкція. Один із можливих наслідків – видалення бази даних, з якими пов'язано веб-додаток	Відсутність фільтрації параметрів, що вводяться в додатку.	7	Використання SIEM для реєстрації підозрілої активності у веб-додатку. Потім – фільтрація вхідних даних форм веб-додатків	1	Розробник веб- програми

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

Результатом даної дипломної робота є розроблена принципова схема комутаційного обладнання для оптимізації потоків трафіку.

Суб'єкт дипломної роботи інженер – проектувальник, який здійснює розробку і аналіз принципової схеми абонентського приймача кабельного цифрового телебачення.

Робоче місце інженера-проектувальника знаходиться в проектувальному відділі на другому поверсі.

4.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера

Відділ проектування знаходиться на другому поверсі п'ятиповерхового будинку. Приміщення має розміри: довжина 8 м, ширина 4 м, висота 4. Загальна площа - 32 м^2, загальний об'єм – 128 м^3. У відділі знаходиться 5 робочих місць інженерів-проектувальників, оснащені комп'ютерами.

Робоча площа одного співробітника становить:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4 \text{ м}^2$$

Робочий об'єм одного співробітника:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6 \text{ м}^3$$

N- кількість співробітників у відділі

$S_{\text{заг.пл}}$ – загальна площа;

$V_{\text{заг.об}}$ – загальний об'єм.

Відповідно до [15] площа на одне робоче місце має становити не менше ніж 6 м^2, а об'єм не менше ніж 20 м^3. Робоче місце інженера-проектувальника відповідає вимогам.

В проектному відділі інженера-проектувальника знаходяться: комп'ютери, принтер. У даному приміщенні температура повітря у теплий період року становить 30°С, використовується природне та штучне освітлення. Штучне освітлення виконано у вигляді перериввчастих ліній світлодіодних світильників. Рівень шуму в приміщенні становить 54 дБ, а згідно з Державними санітарними нормами [16] не повинен перевищувати 50 дБ.

Робоче місце розташоване так, щоб природне світло падало з лівої сторони, при цьому відстань зі світлом до робочого місця - 1 м. Висота робочої поверхні столу над підлогою 750 мм, глибина столу – 800 мм, ширина столу 1300мм. Робочий стіл має простір для ніг висотою 650 мм та шириною 600 мм.

Перелік шкідливих та небезпечних виробничих чинників.

Створення сприятливих умов праці, в роботі інженера-проектувальника, має велике значення як для полегшення , так і для підвищення продуктивності праці. Відповідно до [43] шкідливими виробничими факторами є:

1. Підвищена температура робочого приміщення
2. Недостатня освітленість робочої поверхні
3. Виробничий шум
4. Електромагнітні випромінювання радіочастотного діапазону
5. Іонізуючі випромінювання

Відповідно до [17] робота інженера-проектувальника у приміщенні з енерговитратами 90-120 ккал/год. відносяться до категорії легких фізичних робіт Іа (роботи, що виконуються сидячи і не потребують фізичного напруження).

Таблиця 4.1

Оптимальні величини температури

Період року	Категорія робіт	Температура повітря,°С
Холодний період року	Легка Іа	22-24
Теплий період року		23-25

Допустимі величини температури на постійних робочих місцях:

Період року	Категорія робіт	Температура повітря,°С	
		Верхня межа	Нижня межа
Холодний період року	Легка Іа	25	21
Теплий період року		28	22

У проектному відділі температура повітря становить 30℃ в теплий період року,що перевищує допустиму на 2 ℃. Забезпечили температуру приміщення 23 ℃,за допомогою механічної вентиляції з вентилятором VORTICE VARIO, повітрообмін якого становить 680 $м^3$ /год.

Недостатня освітленість. В приміщенні встановлені персональні комп'ютери, присутнє природне та штучне освітлення . За вимогами [18], величина коефіцієнта природної освітленості повинна бути не менше 1.5%. В проектному відділі порушенні вимоги, освітленість робочої поверхні складає 370 лк , а коефіцієнт освітленості складає 1.2%. Природне світло проникає у приміщення через бічні світло прорізи. Вікна мають жалюзі. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників, розташованих паралельно лінії зору інженера-проектувальника. Для місцевого освітлення використовувати галогенні лампи розжарювання

Виробничий шум. Шум на робочому місці створюється: комп'ютером та периферійним пристроєм. Допустимі рівні звукового тиску на робочому місці повинні відповідати вимогам [19]:

Таблиця 4.2

Санітарні норми виробничого шуму, ультразвуку та інфразвуку

Вид трудової діяльності, робоче місце	Рівні шуму та еквівалентні рівні шуму, ДБА, дБАекв
Конструювання та проектування.	50

Реальний рівень шуму в проектному відділі становить 54 дБ, що перевищує допустимий рівень.

Для зменшення рівня шуму рекомендується використовувати місцеву та загальну звукоізоляцію, шумопоглинаючі екрани, поглинаючі фільтри.

4.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів

Нормалізація повітря робочої зони. Для створення й автоматичної підтримки в ІТ відділі незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря [20].

Виробниче освітлення. Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення шляхом встановлення 5 додаткових світильників, щоб загальна кількість лам відповідала розрахованому вище значенню, а саме 36 світлодіодних ламп. Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік [21].

Електробезпека. Електробезпечність у приміщенні ІТ відділу пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЭ) для електроустановок з напругою до 1000 В. А також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки [22].

Ергономіка та організація робочого місця. Після проведення аналізу робочого місця програміста в ІТ Відділі було з'ясовано, що воно відповідає встановленим вимогам.

Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви сумарний час яких повинен складати 50 хвилин при 8-ми годинному робочому дні [23].

4.2.1. Розрахунок повітрообміну за надлишком тепла у проектному відділі

Приміщення має розміри 4×8×4, яке розміщується на другому поверсі п’ятиповерхового будинку з південного боку. Площа вікон F = 2,88 м^2. На вікнах розміщенні жалюзі. У приміщенні 5 інженерів-проектувальників, розташовано $N_{пк} = 5$ персональних комп’ютерів та принтер. Для штучного освітлення використовується 4 офісних світлодіодних світильника потужністю 125 Вт.

1. Розраховуємо загальну кількість тепла:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад,}\ \text{Вт} \qquad (4.1)$$

$Q_{над}$ – загальна кількість тепла

$Q_{осв}$ - кількість тепла від джерел штучного освітлення

$Q_{облад}$ - кількість тепла від обладнання

$Q_{ін\text{-}пр.}$ - кількість тепла від інженерів-проектувальників

$Q_{рад,}$ - кількість тепла від сонячної радіації

2. Розраховуємо кількість тепла від джерел штучного освітлення:

$$Q_{осв} = N \cdot \eta\ , \qquad (4.2)$$

де N - сумарна потужність джерел освітлення, Вт; η - коефіцієнт теплових витрат (η = 0,55 – для світлодіодних ламп).

$$Q_{осв.} = 125 \cdot 4 \cdot 0{,}55 = 275\ \text{Вт}$$

2. Розраховуємо кількість тепла при роботі обладнання: 5 комп’ютерів і принтера (в режимі друку):

$$Q_{облад} = n \cdot P_{комп.} + P_{пр.}, \qquad (4.3)$$

де n – кількість комп’ютерів (обладнання);

$P_{комп}$ – встановлена потужність комп'ютерів, $P_{комп}=400$ Вт

$P_{пр.}$ – потужність принтера в режимі друку, $P_{пр}=465$ Вт

$$Q_{облад}=5\cdot 400+465=2.5 \text{ кВт}$$

3. Розраховуємо кількість тепла від інженерів-проектувальників:

$$Q_{ін\text{-}пр.} = n \cdot q \text{ , Вт} \quad (4.4)$$

n – кількість інженерів-проектувальників

q – кількість тепла, що виділяється одним інженером-проектувальником

Кількість тепла, що виділяється одним інженером-проектувальником, який виконує легку фізичну роботу дорівнює 99 Вт.

$$Q_{ін\text{-}пр} = 5 \cdot 99 = 495 \text{ Вт}$$

4. Розраховуємо кількість тепла від сонячної радіації:

$$Q_{рад}=m \cdot S \cdot k \cdot q_{скл} \quad (4.5)$$

де m – число вікон; $S_{вікна}$ – площа одного вікна, $S_{вікна}$ =2,88 $м^2$;

k – коефіцієнт, віконного переплетення: k = 0,6 матові;

$q_{скл.}$ – надходження тепла через 1 $м^2$ вікна при різній орієнтації вікон: $q_{скл.}$ = *150* – південь;

$$Q_{рад}=1 \cdot 2,88 \cdot 0,6 \cdot 150=259,2 \text{ Вт}$$

5. Загальна кількість тепла в проектному відділі:

$$Q_{над}= Q_{осв}+ Q_{облад}+ Q_{ін\text{-}пр.} + Q_{рад}=275+2500+495+259,2 = 3,529 \text{ кВт}$$

6. Потрібний повітрообмін за надлишком тепла:

$$L = \frac{Q}{c \cdot \rho \cdot (t_{вид} - t_{зовн})} \text{ , м}^3/\text{год} \quad (4.6)$$

Q - кількість тепла, яке виділяється в приміщення за годину, Дж:

$$Q=3600 \cdot Q_{надл}=3600 \cdot 3529=12704 \text{ Вт} = 5328 \text{ кДж};$$

c – теплоємність повітря, Дж/кг (в інтервалі температур від 0ºС до 100ºС приймається рівною $1,01 \cdot 10^3$Дж/кг);

ρ – густина повітря, кг/м^3(дорівнює $\rho_{внт}$=1,2 кг/м^3);

$t_{вид}$– температура повітря, що видаляється, $t_{вид}$=*30*℃

$t_{зовн.}$- температура повітря, що подається до робочої зони, $t_{зовн.}$=23℃

$$L = \frac{5328}{1{,}01 \cdot 10^3 \cdot 1{,}2 \cdot (30 - 23)} = 628 \text{ м}^3 \text{/год}$$

Оскільки, в проектному відділі підвищена температура повітря на 2 ℃ від допустимого значення 28℃, встановили механічну вентиляцію з вентилятором VORTICE VARIO , яка забезпечила надходження до приміщення температури повітря 23 ℃, дане значення є оптимальним.

4.3. Пожежна безпека

Відповідно до [24-25] дане приміщення відноситься до категорії В по вибухово-пожежній та пожежній небезпеці із-за використання у ньому твердих горючих матеріалів з температурою спалаху понад 61℃.

Проектний відділ оснащено:

- Двома безпровідними датчиками детектування диму SD-02 (оповіщає при задимленні приміщення; площа обслуговування: до 20 м^2);
- двома порошковими вогнегасниками ВП-5 (для приміщення категорії В за відсутності горючих газів і рідин, площею до 50 м^2 і масою вогнегасної речовини – 5 кг, мінімальна кількість порошкових вогнегасників 2).
- LifeSOS LS-30LR бездротова пожежно-охоронна система (при детектуванні вторгнення, датчики передають на центральний блок сигнал тривоги по радіоканалу без проводів. Централь приймає сигнал від датчиків, включає сирену, відправляє інформацію на пульт централізованого нагляду, дзвонить на зазначені телефонні номери та відправляє SMS повідомлення з повідомленнями про тривогу.)

Для попередження виникнення пожеж проводяться організаційно-технічні заходи пожежної безпеки, які включають:

- включення питань пожежної безпеки у всі інструкції по техніці безпеки;
- виконання встановленого режиму експлуатації електричних мереж та обладнання;
- заборона куріння в недозволеному місці;
- видання необхідних інструктажів, планів евакуації

План евакуації складається з графічної і текстової частин. Графічна частина являє собою схематичний план поверху (рис. 5.1), в якому зеленими суцільними стрілками вказують шляхи евакуації, що ведуть до основних евакуаційних виходів, а пунктирними зеленими стрілками - до аварійних виходів. Двері на шляху евакуації відчиняються назовні у напрямку виходу з будівлі. На плані евакуації умовними знаками показано розміщення вогнегасників, пожежних гідрантів, телефонів, аптечок медичної допомоги, електрощитів, датчиків диму, системи охоронно-пожежної сигналізації.

Рис 5.1. План евакуації 2 поверх

4.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Вимоги безпеки перед початком роботи.

- Перед початком роботи працівник повинен зовнішнім оглядом перевірити цілісність корпусів системного блоку, відео монітора, принтера, клавіатури.
- Перевірити цілісність кабелів живлення, місць їх підключення (розеток електромережі, продовжувачів електромережі, розгалужувальних коробок, штепсельних вилок).
- Підготувати своє робоче місце, прибравши речі, які можуть заважати при виконанні роботи.
- Ввімкнути живлення ПК.
- У випадку, якщо після ввімкнення ПК не проходить загрузка або комп'ютер не виходить на робочий режим, працівник повинен повідомити керівника чи спеціаліста відділу інформаційних технологій.
- При виявленні ушкодження або яких-небудь інших недоліків повідомити безпосереднього керівника. Не приступати до роботи без його вказівки.

Вимоги безпеки під час роботи

- Необхідно стійко розташувати всі складові пристрої на столі, в тому числі і клавіатуру. Разом з тим повинна бути передбачена можливість переміщення клавіатури. ЇЇ розташування і кут нахилу повинні відповідати побажанням користувача ПК. Якщо в конструкції клавіатури не передбачений простір для опору долонь, то її слід розташовувати на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля. При роботі на клавіатурі слід сидіти прямо, не напружуватись.
- Для зменшення несприятливого впливу на користувача пристроїв типу "миша" (вимушена поза, необхідність постійного контролю за якістю дій) слід забезпечити вільною більшу площу поверхні столу для переміщення "миші" і зручного упору ліктьового суглоба.
- Не припустимі сторонні розмови, роздратовуючи шуми тощо.

- Періодично при вимкнутому ПК слід видаляти злегка зволоженою мильним розчином хлопко-паперовою салфеткою пил з поверхонь апаратури. Екран і захисний екран протирають ватою, зволоженою спиртом.
- Не дозволяється використовувати рідинні або аерозольні засоби чистки поверхонь ПК.

Забороняється:

- самостійно ремонтувати апаратуру, в яких кінескоп та інші елементи можуть знаходитись під високою напругою (до 25 кВ0.)
- класти будь-які речі на апаратуру ПК, бутерброди та напої на клавіатуру або поруч з нею. Це може вивести її з ладу;
- затуляти вентиляційні отвори в апаратурі, це може призвести до її перегріву і виходу з ладу.

- Для зменшення негативного впливу на стан здоров'я працівників різних факторів ризику, пов'язаних з роботою на ПК, передбачаються додаткові регламентовані перерви для відпочинку користувачів ПК:

- через кожний час безперервної роботи – 10 хвилин;
- через кожні 2 години – 15 хвилин.

- При можливості слід чергувати зміну діяльності з іншою, не пов'язаною з роботою на ПК.
- З метою зменшення негативного впливу монотонності доцільно застосовувати чергування операцій введення тексту і введення даних (зміна змісту і темпу роботи) і т.п.
- При роботі на лазерних принтерах:
- Розташовувати принтер необхідно поряд з системним блоком так, щоб з'єднувальні шнури не були натягнуті. Забороняється ставити принтер на системний блок.
- Перш, ніж програмувати роботу принтера, впевніться, що він знаходиться в режимі зв'язку з системним блоком.
- Для досягнення високоякісного, чистого, з високою роздільною здатністю зображення щоб не зіпсувати апарат, потрібно використовувати папір, марка якого вказана в інструкції до принтера (найчастіше папір вагою 60-135 г/м^2, типу Canon або Xerox 4024).

- Обрізання країв паперу повинно бути виконаним гострим лезом ножа, без зазусенців – це зменшить вірогідність загинання паперу.
- При виконанні роботи (більше 20 хвилин), коли втручання користувача в роботу програми не потрібне, бажано вимикати живлення відео монітора.
- Для підтримки загального тонусу м'язів, профілактики кістково-м'язових порушень, зорового дискомфорту та інших несприятливих суб'єктивних почуттів під час регламентованих перерв необхідно виконувати комплекси рекомендованих вправ для очей, для хребта, для рук.
- Кількість мікро пауз до 1-2 хвилин слід визначити індивідуально. Форма та зміст перерв можуть бути різними виконання допоміжних робіт, не пов'язаних з роботою ПК , приймання їжі, виконання рекомендованих вправ.
- Виконання фізичних вправ протягом дня рекомендується індивідуально, залежно від почуття втоми. Гімнастика повинна біти на корекцію вимушеної пози покращення кровообігу, часткову компенсацію, дефіциту рухової активності.
- Про виявлені несправності (іскріння, пробоїв, запаху гару, ознак горіння тощо) негайно припинити роботу, відключити все обладнання від електромережі і терміново повідомити безпосереднього керівника або спеціаліста по ремонту ПК.

Вимоги безпеки при закінчення роботи на ПК.

- Закінчити і зберегти в пам'яті ПК файли, які знаходились у роботі. Виконати всі дії для коректного завершення роботи в оперативній системі.
- Вимкнути принтер та інші периферійні пристрої, вимкнути системний блок. При наявності пристрою безперебійного живлення (ПБЖ) вимкнути його живлення.
- Вимкнути ПК кнопкою «POWER" (ЖИВЛЕННЯ) та вийняти штепсельну вилку кабелю живлення з розетки
- Накрити клавіатуру кришкою для попередження попадання в неї пилу.
- Навести порядок на робочому місці.

Вимоги безпеки в аварійних ситуаціях.

- Якщо після ввімкнення ПК відчувається запах горілого або при доторканні до металевих частин ПК відчувається дія електричного струму, потрібно негайно відключити ПК від електромережі та повідомити про це своєму керівникові.
- У випадку виникнення пожежі негайно розпочати гасіння наявними засобами пожежогасіння і повідомити за телефоном 101 (міська пожежна охорона) та начальнику ДПД підприємства. Пам`ятайте, що загашувати електроустановки слід вуглекислотними вогнегасниками, сухим піском, щоб уникнути ураження електричним струмом.

У разі виникнення інших аварійних ситуацій слід припинити роботу і повідомити про це керівника робіт.

Висновки. На підставі виконаного розрахунку повітрообміну за надлишком тепла, значення якого 628 м^3/год, встановили механічну вентиляцію з вентилятором VORTICE VARIO, оскільки використання природної вентиляції є малоефективним. Механічна вентиляція здатна забезпечити виведення з проектного відділу температури 30℃ і підтримувати температуру повітря допустимого та навіть оптимального значення.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день радіотехнічне та електронне виробництво є досить розвинутим і без нього суспільство не уявляє свого життя. Електронна і радіотехнічна промисловість грає провідну роль в науково-технічній революції. Впровадження електронних приладів в різні сфери людської діяльності значною мірою сприяє успішній розробці складних науково-технічних проблем, підвищенню продуктивності фізичної і розумової праці, поліпшенню економічних показників виробництва.

В кваліфікаційній роботі розроблена система захисту з використанням серверного обладнання, що може здійснювати негативний вплив на навколишнє середовище.

5.1. Аналіз впливу техногенних чинників

Широке використання електричного та електронного обладнання дозволило не тільки підвищити якість життя людей, але й призвело до негативних наслідків для навколишнього середовища та здоров’я людини. Можна виділити основні шкідливі та небезпечні чинники, які впливають на навколишнє середовище [26]:

- шумове забруднення;
- вібраційне забруднення;
- електромагнітне забруднення
- теплове забруднення
- радіаційне забруднення

Шумове забруднення. У сучасному світі в умовах науково-технічного прогресу шум став однією з форм фізичного (хвильового) забруднення природного середовища. Шумом прийнято вважати усі неприємні та небажані звуки або їх сукупність, які заважають нормально працювати, сприймати потрібну звукову інформацію та відпочивати.

Адаптація до нього практично неможлива. Фоновий рівень шуму навколишнього середовища становить 30-60 децибел. До цього природного фону за сучасних умов додаються виробничі й транспортні шуми, рівень яких нерідко перевищує 100 децибел. Джерелами шуму є: промислові об’єкти, транспорт, гучномовні пристрої, телевізори, радіоприймачі, музичні інструменти, юрби людей тощо. Шум у виробничих умовах негативно впливає на працівника: послаблює увагу, посилює розвиток втоми, сповільнює реакцію на небезпеку. Внаслідок цього знижується працездатність та підвищується ймовірність нещасних випадків. Допустимі рівні звукового тиску в октавних смугах частот на робочих місцях у виробничих приміщеннях наведені в таблиці 5.1 [26]:

Таблиця 5.1.

Допустимі рівні звукового тиску в октавних смугах частот

Рівні звукового тиску в дБ, в октавних смугах частот, Гц								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

Встановлено, що рослини під впливом шуму знижують енергію до зростання, у них спостерігається надмірне (навіть повне, що призводить до загибелі) виділення вологи через листя, можливі порушення у клітинах. Гинуть листя і квіти рослин, які розташовані близько до джерела інтенсивного шуму (звуку). Відсутність шуму особливо необхідний для тварин, які обмінюються звуковою інформацією, а також аналізуючи звуки навколишнього середовища з метою покращання отримання інформації, в тому числі сигналів тривоги. Аналогічно діє шум на тварин. Від шуму реактивного літака гинуть личинки бджіл, самі

вони втрачають здатність орієнтуватися, у пташиних гніздах дає тріщини шкаралупа яєць. Від коливань повітря, які утворюються звуками переносної радіоапаратури, не можуть піднятися у повітря жуки, джмелі та інші комахи.

Вібраційне забруднення. Вібрація – це механічні коливання твердого тіла. Вібрацію поділяють на природну та штучну. Джерелами природної вібрації є землетруси,

що викликаються природними чинниками. Джерелами штучної вібрації є промисловість, транспорт. Тривалі вібрації завдають великої шкоди здоров'ю людини – від сильної втоми до змін багатьох функцій організму: порушення серцевої діяльності, нервової системи, спазмів судин, деформації м'язів, струсу головного мозку тощо. Особливо небезпечна вібрація з частотою, яка є резонансною з частотою коливання окремих органів чи частин тіла людини, що може призвести до їх пошкодження. Тривала дія вібрації може спричинити професійне захворювання – вібраційну хворобу [26].

Електромагнітне забруднення. У процесі еволюції біосфера постійно знаходилася і знаходиться під впливом електромагнітного поля (ЕМП) природного походження (природний фон): електричного й магнітного поля Землі, космічного електромагнітного випромінювання, насамперед того, що генерується Сонцем. У період науково-технічного прогресу людство створювало і дедалі ширше використовувало штучні (антропогенні) джерела ЕМП. У наш час ЕМП антропогенного походження значно перевищують природний фон і є тим несприятливим чинником, вплив якого на людину та довкілля рік за роком зростає. Ступінь впливу ЕМП на організм людини залежить від діапазону частот, інтенсивності та тривалості дії, характеру випромінювання (неперервного чи модульованого), режиму опромінювання, розміру поверхні тіла, що зазнає опромінювання, індивідуальних особливостей організму. Електромагнітні поля можуть викликати біологічні та функціональні порушення у функціонуванні організму. Функціональні ефекти проявляються у передчасній втомлюваності, частих болях голови, погіршенні сну, порушенні функцій серцево-судинної та центральної нервової систем. Тривалий та інтенсивний вплив ЕМП призводить до стійких порушень та захворювань. Біологічні негативні ефекти впливу ЕМП проявляються у тепловій та нетепловій діях. Теплова дія призводить до підвищення температури тіла та місцевого вибіркового нагрівання органів і тканин організму внаслідок переходу електромагнітної енергії в теплову. Таке нагрівання особливо небезпечне для органів із слабкою терморегуляцією (головний мозок, очі, нирки, шлунок тощо). Наприклад, випромінювання сантиметрового діапазону призводить до появи катаракти, тобто до поступової втрати зору [26].

Теплове забруднення. Теплове забруднення – це результат розсіювання в навколишнє середовище теплоти, яка виділяється у багаточисельних теплових процесах, насамперед пов’язаних зі згоранням палива. Під час згорання палива щорічно витрачається до 23% кисню, що утворюється в процесі фотосинтезу на Землі за рік. За підрахунками під час спалювання вугілля в навколишнє середовище викидається радіоактивних компонентів більше, ніж за той самий час на всіх атомних електростанціях у разі безаварійної роботи. Теплове забруднення гідросфери відбувається переважно внаслідок скидання у водойми підігрітих вод від ТЕС, АЕС та інших енергетичних об’єктів. Тепла вода змінює термічні та біологічні режими водойм і шкідливо впливає на їхніх мешканців [26].

5.2. Вплив приймальних пристроїв на навколишнє середовище

Абонентський приймач – телевізійний приймач (приставка), пристрій, що приймає сигнал цифрового телебачення, декодує його і перетворює в аналоговий сигнал для виведення через роз'єми RCA або SCART або перетворює в цифровий сигнал для виведення через роз'єм HDMI , і передає його далі на телевізор.

Перехід до цифрового телебачення призвів до зростання виробництва цифрових абонентських приймачів, що в свою чергу може негативно впливати на навколишнє середовище. Приймач продукує слабкі електричні і магнітні змінні поля в широкому діапазоні частот. Проте проблема впливу електромагнітних випромінювань, що продукуються заслуговує на особливу увагу. Наукові дослідження показали, що ЕМВ мають у своєму складі чинник, котрий впливає на користувачів при наявності сучасних екранів від ЕМВ. Вчені України ідентифікували цей чинник як торсіонові поля, котрі супроводжують будь-яке електромагнітне випромінювання та являються його інформаційною компонентою [27]. Робоча група Всесвітньої організації охорони здоров’я з гігієнічних аспектів користування моніторами та радіо терміналами виявили порушення стану здоров’я при користуванні пристроями, які мають електромагнітне випромінювання, найсерйозніші з яких:

- погіршення зору;

- порушення імунної системи;
- порушення психоемоційної сфери (стресовий синдром, агресивність)

Для забезпечення безпеки здоров'я користувачів в Україні діють Державні санітарні норми і правила при роботі з джерелами електромагнітних полів «ДСанПіН 3.3.6.096-2002». Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових залежно від тривалості їх дії наведені в таблиці 5.2.

Таблиця 5.2.

Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових

Час перебування персоналу, год	$E_{гд}$, В/м					$H_{гд}$, А/м			
	1-10 кГц	10-60 кГц	0,063 МГц	3-30 МГц	30-300 МГц	1-10 кГц	10-60 кГц	0,06-3 МГц	30-50 МГц
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

У результаті дії на організм людини електромагнітних випромінювань в діапазоні 30 кГц - 300 МГц (НЧ) спостерігається: загальна слабкість, підвищена втома, сонливість, порушення сну, головний біль та біль в ділянці серця. З'являється роздратованість, втрачається увага, сповільнюються рухово-мовні реакції. Виникає ряд симптомів, які свідчать про порушення роботи окремих органів - шлунку, печінки, підшлункової залози.

Для того, щоб зменшити рівень електромагнітного випромінювання потрібно обмежити безперервний час роботи абонентського приймача [27-28].

В Україні норми електромагнітної безпеки регламентуються Державними санітарними нормами і правилами захисту населення від впливу електромагнітного випромінювання, згідно з якими допустимі рівні інтенсивності електромагнітного випромінювання для цивільного населення становлять 2,5 мкВт/см^2.

Абонентський приймач під час роботи створює шум, рівень якого становить 54 дБ. Допустимий рівень звукового тиску повинний відповідати «ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку», а саме 50 дБ.

Велика кількість звукових сигналів, що поступають до кори головного мозку, викликають переживання, страх, передчасну втому. Дія шуму на людину виражається в широкому діапазоні - від суб'єктивного роздратування до об'єктивних змін в ЦНС, органах слуху, серцево-судинних та ендокринній системах, травному акті та інших органів і систем. Першим показником шкідливої дії шуму є скарги на роздратованість, переживання, порушення сну [29].

5.3. Засоби для захисту від електромагнітного випромінювання та шуму, проблема електронних відходів

Захист від електромагнітного випромінювання. Для зменшення впливу ЕМП на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів, потрібно вжити ряд захисних заходів. До їх числа можуть входити організаційні, інженерно-технічні та лікарсько-профілактичні.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають таке розташування джерел ЕМП, яке б зводило до мінімуму їх вплив на працюючих, використання в умовах виробництва

дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання, застосування засобів індивідуального захисту (халатів, комбінезонів із металізованої тканини, з виводом на заземлюючий пристрій). Для захисту очей доцільно використовувати захисні окуляри ЗП5-90. Скло окулярів вкрито напівпровідниковим оловом, що послаблює інтенсивність електромагнітної енергії при світлопропусканні не нижче 75%.

Взагалі, засоби індивідуального захисту необхідно використовувати лише тоді, коли інші захисні засоби неможливі чи недостатньо ефективні: при проходженні через зони опромінення підвищеної інтенсивності, при ремонтних і налагоджувальних роботах в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання трудових операцій, погіршують гігієнічні умови.

У радіочастотному діапазоні засоби індивідуального захисту працюють за принципом екранування людини з використанням відбиття і поглинання ЕМП. Для захисту тіла використовується одяг з металізованих тканин і рідіопоглинаючих матеріалів. Металізовану тканину роблять із бавовняних ниток з розміщеним всередині них тонким проводом, або з бавовняних чи капронових ниток, спірально обвитих металевим дротом. Така тканина, наче металева сітка, при відстані між нитками до 0,5 мм значно послаблює дію випромінювання. При зшиванні деталей захисного одягу треба забезпечити контакт ізольованих проводів. Тому електрогерметизацію швів здійснюють електропровідними масами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок безконтактних проводів.

Лікарсько-профілактичні заходи передбачають проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП, обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань, видачу працюючим безкоштовного лікарсько-профілактичного харчування, перерви санітарно-оздоровчого характеру.

Захист від шуму. Для зменшення і ліквідації шуму застосовується цілий комплекс заходів, що називається шумозахистом. Це застосування звукопоглинаючих ма-

теріалів, раціональне розміщення будівельних об'єктів, створення вздовж вулиць екранів у вигляді земляних валів, стін різних конструкцій, шумовідбиваючих, як правило не житлових будівель - магазинів, складів, гаражів.

Проблема електронних відходів. Згідно Закону України «Про відходи» з метою запобігання або зменшення обсягів утворення відходів потрібно здійснювати системи збирання та утилізації електричного та електронного обладнання [30]. Вирішення проблеми електронних відходів в Україні мав би забезпечити «Технічний регламент з поводження з відходами електричного та електронного обладнання», розробка якого в Україні здійснюється з 2008 року. Згідно з проектами цих законодавчих актів імпортери і виробники можуть як самостійно утилізувати електровідходи, так і підписувати договори на виконання робіт з організації збирання, заготівлі та утилізації відповідних видів техніки з уповноваженими підприємствами. Розроблено також проект Постанови Кабінету Міністрів України «Про затвердження Технічного регламенту з поводження з відходами електронного та електричного устаткування». Цим регламентом передбачається створення пунктів збору відходів електронного та електричного обладнання, які повинні розташовуватися у місцях, зручних для користувачів, та забезпечувати безоплатність послуг, що надаються цими пунктами для користувачів. Наразі обговорюється ще один варіант вирішення проблеми, а саме проект внесення змін до Податкового Кодексу, в якому передбачає централізоване стягнення коштів з імпортерів та виробників різних споживчих товарів з метою забезпечення за рахунок цих коштів належної організації збирання, заготівлі та утилізації відходів від зазначених товарів.

Однак, загалом проблему електронних відходів в Україні необхідно вирішити як в організаційно-правовому аспекті – створення фондів виробників, підтримка держави підприємств з утилізації відходів, так і в соціально-інформаційному: українців треба переконати в тому, що виносити на звичайний смітник поламаний електронний пристрій – не можна.

Висновок. Абонентські приймачі створюють негативний вплив на навколишнє середовище. Вони є джерелами електромагнітного випромінювання та шумового за-

бруднення. Для мінімізації ризику виникнення захворювань, ефективними є інженерно-технічні заходи, які зменшать дію шкідливих чинників. Також були розглянута проблема електронних відходів, одним зі шляхом вирішення якої є створення пунктів збору відходів електронного та електричного обладнання.

ВИСНОВКИ

Завдання полягало в тому, щоб, спираючись на тему дипломної роботи, виділити найбільш важливі активи, що підлягають захисту, та проаналізувати ризикові ситуації для даних активів, а також провести розрахунок максимальних ризиків та залишкових (ризиків, що залишаються після впровадження захисних заходів). Розрахунок максимальних ризиків показав, що всі ризикові ситуації є прийнятними (чисельне значення ризиків склало від 5 до 8 по восьмибальної шкалою), і для них необхідно впроваджувати заходи щодо обробки ризиків. Оскільки кваліфікаційна робота присвячена SIEM – системі, поруч із заходами захисту під час аналізу ризиків SIEM – система впроваджувалася як моніторингова, що використовується у зв'язці з іншими засобами захисту. Повторний перерахунок (розрахунок залишкового ризику) показав, що після застосування цих заходів ризики стали прийнятними. З урахуванням того, наскільки високі були первинні ризики, і яку шкоду могла б зазнати компанія при реалізації загроз, використання заходів захисту, впроваджених для обробки ризиків, є прийнятним та рентабельним. У середньому ризики після вживання вищевказаних заходів обробки зменшилися вчетверо (наприклад, первинний ризик становив 8 за восьмибальною шкалою, а залишковий - 2).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вікіпедія - вільна енциклопедія // Wikipedia.org: "SIEM". URL: https://ua.wikipedia.org/wiki/SIEM.
2. M. Fiedler, "Cyberangriffe: dramatische Zunahme und Rekordschäden", procontra-online.de Alsterspree Verlag GmbH Berlin.
3. Z. Qu and X. Wang, "Study of rough set and clustering algorithm in network security management", Proceedings of the 2019 International Conference on Networks Security Wireless Communications and Trusted Computing, vol. 1, pp. 326-329, 2019.
4. X. Li, X. Zheng, J. Li and S. Wang, "Frequent itemsets mining in network traffic data", Proceedings of the 2020 5th International Conference on Intelligent Computation Technology and Automation ICICTA ‘2020, 2020.
5. M. A. Jabbar, R. Aluvalu and S. S. Reddy, "Cluster based ensemble classification for intrusion detection system", Proceedings of the 9 th International Conference on Machine Learning and Computing ser. ICMLC’2021, pp. 253-257, 2021.
6. C. C. Aggarwal, Outlier Analysis. in Data Mining: The Textbook, Cham:Springer International Publishing, pp. 237-263, 2019.
7. F. Heine et al., "Outlier detection in data streams using OLAP cubes" in New Trends in Databases and Information Systems ADBIS 2021 Communications in Computer and Information Science, Cham:Springer, vol. 767, 2021.
8. Офіційний сайт RSA Witness // Rsa.com: « Rsa NetWitness SIEM». URL: https://www.rsa.com/en-us/products/threat-detection-respon se (дата звернення: 21.10.2022).
9. C. Ordonez, Z. Chen and J. Garcia-Garcia, "Interactive exploration and visualization of olap cubes", Proceedings of the ACM 14 th International Workshop on Data Warehousing and OLAP ser. DOLAP'11 , pp. 83-88, 2021.
10. V. Hamolia, V. Melnyk, P. Zhezhnych and A. Shilinh, "Intrusion detection in computer networks using latent space representation and machine learning", International Journal of Computing, vol. 19, no. 3, pp. 442-448, 2020.

11. 11 Офіційний сайт fortinet // https:// www.fortin et.com URL: https://help.fortinet.com/fsiem/5-1-0/Online-Help/HTML5_Help/Importing_malware_url_information.htm (дата звернення : 21.10.2022).

12. M. Gupta, J. Gao, C. C. Aggarwal and J. Han, "Outlier detection for temporal data", Synthesis Lectures on Data Mining and Knowledge Discovery, vol. 5, no. 1, pp. 1-129, 2021.

13. A. S. Maniatis, P. Vassiliadis, S. Skiadopoulos and Y. Vassiliou, "Advanced visualization for OLAP", Proceedings of the 6th ACM International Workshop on Data Warehousing and OLAP ser. DOLAP'03, pp. 9-16, 2003.

14. V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey", ACM Comput. Surv., vol. 41, 2019.

15. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин.

16. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

17. Державні санітарні норми та правила «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу».

18. «ДСН 3.3.6.042-99 Санітарних норми мікроклімату виробничих приміщень».

19. ДБН 13.2.5-28-2006 «Природне і штучне освітлення».

20. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

21. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

22. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».

23. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».

24. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

25. НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

26. Прогнозування екологічних ризиків з використанням аналізу ієрархів та теорії нечітких множин: міжнародна науково-практична конференція «І-й всеукраїнський з'їзд екологів»: Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. – 2016. – С.25.

27. Антипов В.В, Давыдов Б.И., Тихончук В.С. Біологічна дія, нормування та захист від електромагнітних вилучень. К.: Енер, 2012. - 177 с.

28. Філіппов О.С. Вплив електромагнітних полів на біологічні об'єкти/Є.С. Філіппов, Є.Л. Ткачук // Медичний журнал. - 2018. - №1 - Том: 24. - С. 15-19.

29. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с

30. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с