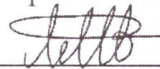


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

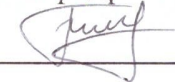
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми моніторингу та аналізу
подій безпеки периметрового захисту комп'ютерної
мережі організації»

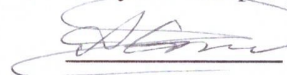
Виконав студент 4-го курсу групи КБ-2
спеціальності 125 «Кібербезпека»

 А. В. Медведенко

Керівник старший викладач кафедри КІ та КБ

 Покотило О. А.

Рецензент к.т.н., доцент, завідувач кафедри КІ та КБ

 А. А. Єфіменко

Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Медведенко Андрій Віталійович

Тема роботи: «Проект підсистеми моніторингу та аналізу подій безпеки периметрового захисту комп'ютерної мережі організації»

затверджена Наказом університету від

Термін здачі студентом закінченої роботи

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єкт дослідження – процес реєстрації, аналізу та візуалізації подій інформаційної безпеки.

Предмет дослідження – методи і засоби використання систем реєстрації, аналізу та візуалізації подій інформаційної безпеки для реагування на події інформаційної безпеки.

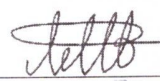
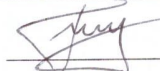
Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco 7200 Series
2. Cisco ASA 5500
3. Комутатори Cisco Catalyst 2960
4. Open Source SIEM AlienVault

5. Персональний комп'ютер на ОС Windows 10 Home
6. Віртуальна машина на ОС Windows XP
7. Віртуальна машина на ОС Windows 7
8. Віртуальна машина на ОС Kali Linux
9. Віртуальна машина на ОС Debian 8.3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

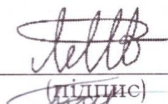
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Студент  Медведенко А. В.
 Керівник  Покотило О. А.

Календарний план

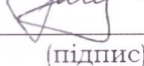
№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка цілей	15 березня 2022	Виконано
2	Визначення завдань, що вирішуються з використанням підсистеми реєстрації.	17 березня 2022 – 22 березня 2022	Виконано
3	Огляд захисту периметра для сучасних мереж	25 березня 2022 – 31 березня 2022	Виконано
4	Визначення ролі брандмауера в захисті мережі периметра	3 квітня 2022 – 10 квітня 2022	Виконано
5	Опис обраного обладнання для будівництва мережі	11 квітня 2022 – 13 квітня 2022	Виконано
6	Огляд найпопулярніших систем для запису, аналізу та візуалізації подій безпеки та вибір однієї з них	15 квітня 2022 – 21 квітня 2022	Виконано
7	Розробка проекту мережі організації з інтегрованою підсистемою реєстрації, аналізу та візуалізації подій безпеки	23 квітня 2022 – 26 квітня 2022	Виконано
8	Огляд обраної системи реєстрації, аналізу та візуалізації подій безпеки	27 квітня 2022 – 30 квітня 2022	Виконано
9	Побудова та адаптація мережі підприємств	5 травня 2022 – 10 травня 2022	Виконано
10	Інтеграція та налаштування підсистеми реєстрації, аналізу та візуалізації подій безпеки	15 травня 2022 – 23 травня 2022	Виконано
11	Тестування продуктивності та безпеки моделі інформаційної системи підприємства	25 травня 2022 – 27 травня 2022	Виконано
12	Аналіз результатів дослідження	29 травня 2022 – 31 травня 2022	Виконано
13	Написання пояснювальної записки	1 червня 2022 – 10 червня 2022	Виконано

Студент _____


(підпис)

Медведенко А. В.

Керівник _____


(підпис)

Покотило О. А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми реєстрації, аналізу та візуалізації подій інформаційної безпеки та пояснювальної записки до нього. Пояснювальна записка до роботи містить 76 сторінок та 26 ілюстрацій.

Метою кваліфікаційної роботи є впровадження підсистеми реєстрації, аналізу та візуалізації подій безпеки в існуючій мережі та адаптування її з підсистемою периметра захисту інформаційної системи підприємства.

Було обрано виробників обладнання для побудови мережі та вибрано підсистему реєстрації, змодельовано проект мережі та підсистеми периметрового захисту організації. Описано функції та можливості підсистеми реєстрації, аналізу та візуалізації подій безпеки. До того ж, був проведений розрахунок для використання апаратних ресурсів для побудови мережі. Було проведено базові налаштування усіх пристроїв у мережі, а також налагодження та тестування підсистеми реєстрації, аналізу та візуалізації подій безпеки.

КЛЮЧОВІ СЛОВА: БЕЗПЕКА, ПОДІЇ БЕЗПЕКИ, РЕЄСТРАЦІЯ, АНАЛІЗ, ВІЗУАЛІЗАЦІЯ, ПЕРИМЕТР МЕРЕЖІ, ПІДСИСТЕМА РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ПОДІЙ БЕЗПЕКИ.

					КІК.КР.Б - 125 - 13 - ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми моніторингу та аналізу подій безпеки периметрового захисту комп'ютерної мережі організації	Літ.	Арк.	Аркуші	
Розроб.		Медведенко А. В.		24.06.22					
Керівник		Покотило О. А.		24.06.22			4	59	
Реценз.		Єршменко А. А.		24.06.22		ФІКТ, Гр. КБ-2			
Н. контр.		Єршменко А. А.		24.06.22					
Залверд.		Єршменко А. А.		24.06.22					

ABSTRACT

Qualification work consists of a project of the subsystem for registration, analysis and visualization of information security events and an explanatory note to it. The explanatory note to the work contains 76 pages and 26 illustrations.

The purpose of the qualification work is to introduce a subsystem for registration, analysis and visualization of security events in the existing network and to adapt it to the subsystem of perimeter protection of the enterprise information system.

The manufacturer of network construction equipment was selected and the registration subsystem was selected, the network design and the perimeter security subsystem of the organization were modeled. The functions and capabilities of the subsystem for registration, analysis and visualization of security events and security events are described. In addition, a calculation was made for the use of hardware resources to build the network. Basic settings of all devices in the network were performed, as well as debugging and testing of the subsystem for registration, analysis and visualization of security approaches.

KEYWORDS: SECURITY, SECURITY EVENTS, REGISTRATION, ANALYSIS, VISUALIZATION, NETWORK PERIMETER, REGISTRATION SUBSYSTEM, ANALYSIS AND VISUAL VISUALS.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ОРГАНІЗАЦІЯ СИСТЕМ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ	10
1.1. ОСНОВА ЗАХИСТУ ПЕРИМЕТРА – БРАНДМАУЕР	10
1.2. ОХОРОНА ПЕРИМЕТРА ТА ЇЇ ОРГАНІЗАЦІЯ В СУЧАСНИХ МЕРЕЖАХ.....	15
1.3. ОХОРОНА ПЕРИМЕТРА ТА ВИБІР ВИРОБНИКІВ ВНУТРІШНЬОГО МЕРЕЖЕВОГО ОБЛАДНАННЯ	21
1.4. ОГЛЯД ТА ВИБІР СИСТЕМ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ІНЦИДЕНТІВ БЕЗПЕКИ	25
РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ РЕЄСТРАЦІЇ ПОДІЙ БЕЗПЕКИ, АНАЛІЗУ, ВІЗУАЛІЗАЦІЇ	33
2.1. ОРГАНІЗАЦІЯ МЕРЕЖІ ПРОЕКТУ	33
2.2. ПРОЕКТ ПІДСИСТЕМИ ЗАХИСТУ ПЕРИМЕТРА.....	39
2.3. ОПИС ПІДСИСТЕМ, ЩО ВИКОРИСТОВУЮТЬСЯ ДЛЯ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ПОДІЙ БЕЗПЕКИ.....	41
2.4. ПРОЕКТ СЦЕНАРІЇВ ДЛЯ ТЕСТУВАННЯ ФУНКЦІОНАЛЬНОСТІ ПІДСИСТЕМИ ..	46
2.5. РОЗРАХУНОК КІЛЬКОСТІ АПАРАТНИХ РЕСУРСІВ, ВИКОРИСТАНИХ ДЛЯ ПОБУДОВИ МЕРЕЖІ	54
РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ПОДІЙ БЕЗПЕКИ.....	57
3.1. БАЗОВЕ ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ МЕРЕЖЕВОГО ОБЛАДНАННЯ	57
3.2. НАЛАШТУВАННЯ ПІДСИСТЕМ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ПОДІЙ БЕЗПЕКИ	58
3.3. ТЕСТУВАННЯ ПІДСИСТЕМИ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ПОДІЙ БЕЗПЕКИ	60
3.4. АНАЛІЗ РЕЗУЛЬТАТІВ ВИПРОБУВАНЬ	62
ВИСНОВКИ.....	65
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	67
ДОДАТКИ.....	70

		Медведевко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SIEM – Security Information and Event Management

ОС – операційна система

МЕ – міжмережний екран

OSI – Open Systems Interconnection

TCP – Transmission Control Protocol

IP – Internet Protocol

VLAN – Virtual Local Area Network

ДМЗ – демілітаризована зона

NAT – Network Address Translation

ASA – Adaptive Security Appliances

ПЗ – програмне забезпечення

АЗ – апаратне забезпечення

VPN – Virtual Private Network

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Обсяг інформації, яку обробляють та передають між ІТ-системами, зростає з кожним днем. Тому, незалежно від того, чи є вони кінцевими користувачами, організаціями чи окремими користувачами, вони все більше і більше залежать від цих процесів та правильності їх реалізації. Щоб реагувати на загрози, ІТ-адміністраторам потрібні інструменти аналізу подій у реальному часі. Одним із рішень цієї проблеми є використання систем керування подіями інформаційної безпеки (Security information and event management – SIEM). Ці системи працюють по принципу збору інформації про ІТ-систему з різних джерел і обміну результатами їх обробки в інтерфейсі, доступному для аналітиків безпеки. Це набагато полегшує дослідження характеристик інцидентів безпеки.

SIEM являє собою пристрої або служби, які зачастих використовуються для запису даних і створення звітів для забезпечення узгодженості з іншими бізнес-даними.

Ця тема є досить актуальною, тому що впровадження системи SIEM сприяє більш швидкому реагуванню на події, які пов'язані з безпекою. Це допоможе зменшити або, можливо, і нейтралізувати злочинний вплив на мережу.

Прийняття рішень до того, як ситуація стане критичною - це і є попереджування інцидентів безпеки та управління ними. Такий контроль найчастіше здійснюється, використовуючи автоматичні механізми розрахунку прогнозу майбутніх подій на основі історичних даних та автоматичного редагування налагодження моніторингу подій в залежності від стану системи.

Основною ціллю систем SIEM є підвищення рівня інформаційної безпеки в існуючій архітектурі. Цього досягають завдяки здатності маніпулювати інформацією про безпеку та керувати інцидентами та подіями безпеки майже в реальному часі.

Мета роботи. Впровадження системи запису, аналізу, а також візуалізації подій, які тісно пов'язані із інформаційною безпекою в існуючій мережі та адаптація її до підсистеми безпеки периметра мережі на базі обладнання Cisco.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Поставлена мета включає себе такі задачі:

- аналіз вже існуючих підсистем охорони периметра підприємства;
- аналіз сучасних систем реєстрації, аналізу та візуалізації подій, пов'язаних з інформаційною безпекою;
- вибір засобів для реалізації підсистеми;
- встановлення необхідного програмного забезпечення (ПЗ) та налагодження систем реєстрації, аналізу та візуалізації подій, пов'язаних з інформаційною безпекою.

Об'єкт дослідження. Процес реєстрації, аналізу та візуалізації подій, пов'язаних з інформаційною безпекою.

Предмет дослідження. Методи та засоби використання систем реєстрації, аналізу та візуалізації подій, пов'язаних з інформаційною безпекою, для реагування на події, пов'язані з інформаційною безпекою.

Методи дослідження. Процес впровадження та адаптації системи реєстрації, аналізу та візуалізації подій інформаційної безпеки в існуючій мережі.

Інформаційна база. Дослідження фахових наукових публікацій, наукових публікацій провідних вітчизняних та зарубіжних вчених, навчально-методичних публікацій, законодавчих та нормативних актів з питань комп'ютеризації і аналітичних даних фахівців у цій галузі.

Практичне значення отриманих результатів. Отримані результати становлять теоретичну основу для дослідження та практичного вирішення проблеми організації системи реєстрації, аналізу та візуалізації подій безпеки мережі. Розроблені пропозиції можуть бути використані в діяльності підприємств, які потребують цієї системи.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОРГАНІЗАЦІЯ СИСТЕМ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

1.1. Основа захисту периметра – брандмауер

В корпоративній мережі одним з найважливіших елементів системи інформаційної безпеки є захист периметра. Захист периметра містить у собі такі поняття як віртуальна приватна мережа (VPN - Virtual Private Network) (рис.1.1), брандмауери, шлюзи безпеки, і система запобігання вторгненням (IPS - Intrusion Prevention System) (рис.1.2). Основою надійної роботи критичних для компанії ІТ-систем та одним з найважливіших завдань інформаційної безпеки являється його правильна реалізація.

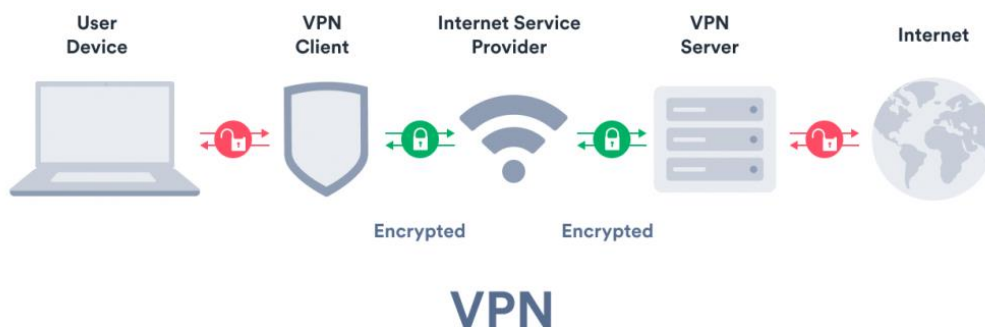


Рисунок 1.1 - Віртуальна приватна мережа

Intrusion Prevention System (IPS)

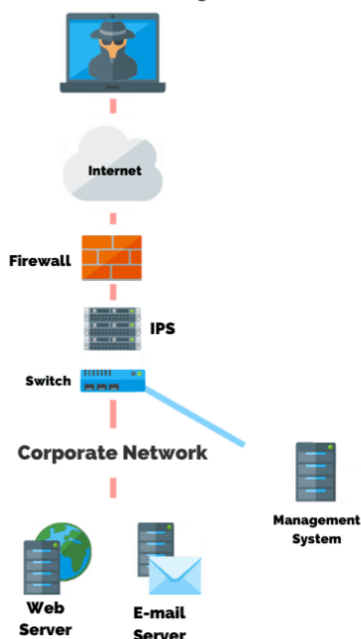


Рисунок 1.2 - Система запобігання вторгненням

		Медведенко А. В.		
		Покотило О. А.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 13 – ПЗ

Арк.

10

Міжмережевий екран (фаєрвол, брандмауер) є апаратно-програмним комплексом засобів, які фільтрують локальний і вхідний трафік, згідно з параметрами, раніше заданими адміністратором. Головна мета використання міжмережевого екрану – захист інформації від зломисників та фільтрація трафіку (рис.1.3) [7].

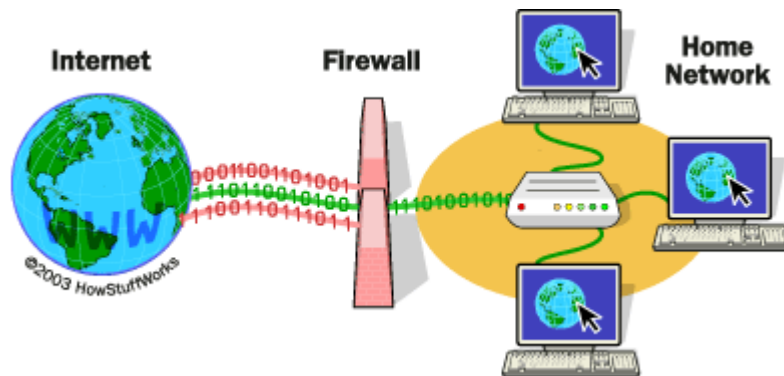


Рисунок 1.3 – Візуалізація роботи міжмережного екрана

Міжмережевий екран - комплексний захист, який вважається обов'язковим для будь-якої корпоративної мережі. Крім фільтрації трафіку, у міжмережевого екрану є ще одна важлива функція — захист конфіденційних даних від витоку, а також захист від несанкціонованого доступу до мережі шкідливого програмного забезпечення.

Більшість загроз використовують уразливості на вищих рівнях, включаючи рівень програми, тому сучасні функції безпеки повинні враховувати це. Охорона периметра є елементом комплексного захисту в рамках забезпечення безпеки персональної інформаційної система, автоматизованої системи управління технологічними процесами тощо.

Підсистема зовнішнього захисту як правило включає в себе два основні механізми:

- засоби міжмережного екранування;
- засоби виявлення та запобігання вторгнень.

Частіше за все ці механізми реалізовані як частина одного продукту, тому що вони вирішують майже схожі проблеми.

Можливості, які спочатку називалися уніфікованим керуванням загрозами (UTM), сьогодні більш відомі як брандмауер наступного покоління (NGFW),

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

надають безліч функцій безпеки та послуг в одному пристрої або службі в мережі, захищаючи користувачів від загроз безпеці спрощеним способом (рис.1.4).

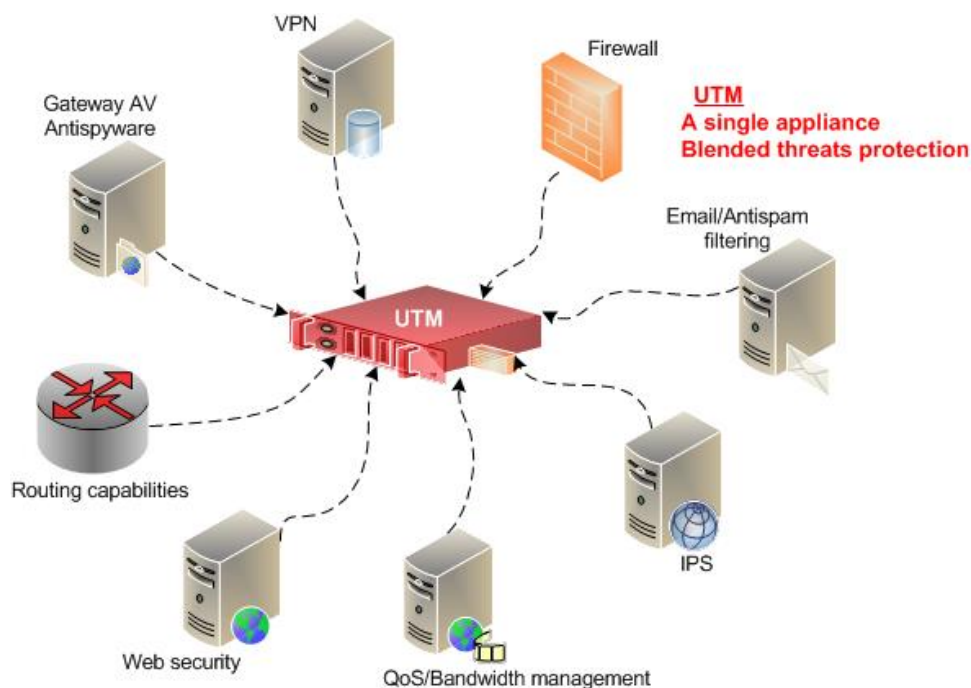


Рисунок 1.4 - Візуалізація уніфікованого керування загрозами

Зараз постійно можна зіткнутися з проблемою захисту продуктивності та цифрових активів своїх компаній від нових і складних загроз, включаючи спам і фішингові атаки, віруси, трояни та заражені файли-шпигуни, несанкціонований доступ до веб-сайтів і несанкціонований вміст. Наявність кількох окремих пристроїв, кожен з яких призначений для виконання спеціальних функцій, таких як фільтрація спаму, фільтрація веб-контенту або антивірусний захист, не полегшує це завдання. Навпаки, це збільшує вартість і складність керування кількома ящиками та кількома операційними системами.

UTM захищають мережу від вірусів, шкідливого програмного забезпечення або шкідливих вкладень, скануючи вхідні дані за допомогою глибокої перевірки пакетів, запобігають атакам до того, як вони увійдуть в мережу, перевіряючи заголовки пакетів, запобігають доступу до небажаних веб-сайтів, встановлюючи розширену веб-фільтрацію та надають можливість автоматично оновлюватися за допомогою останніх оновлень безпеки, антивірусних визначень та нових

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

функцій, так що після початкового налаштування потрібно мінімальне втручання вручну.

Це дозволяє адміністраторам керувати широким спектром функцій безпеки за допомогою єдиної консолі керування.

Багатофункціональні шлюзи безпеки (Unified Threat Management - UTM) включають у себе найбільш популярні функції, такі як: брандмауер, запобігання вторгненням, криптографічний захист каналів зв'язку, безпечний віддалений доступ (VPN), антивірусний захист мережевого трафіку, захист електронної пошти, DLP, фільтрація веб-сайтів, моніторинг трафіку та оптимізація.

Основою будь-якого такого шлюзу є брандмауер, який як правило підтримує більшість механізмів безпеки, що і робить цей пристрій безпечнішим і простішим у керуванні та виконує наступні функції:

- аналіз даних, які проходять через нього;
- контроль середовища, де проходить обмін даними;
- регулювання обміну даними залежно від політики безпеки;
- реєстрація подій безпеки.

Завдяки цьому можна досягти наступного:

- підвищити безпеку внутрішнього середовища;
- керувати інформаційними потоками в зовнішнє середовище;
- забезпечити реєстрації процесів обміну інформацією.

Зазвичай міжмережний екран розташовується на межі глобальної та внутрішньої мереж. Іноді, коли МЕ використовується для захисту від атак з підключеної до локальної мережі підприємства корпоративної мережі, міжмережний екран діє як захисний бар'єр і стає єдиним виходом кожного вузла мережі до потенційно ворожого зовнішньої мережі. МЕ здійснює свій захист, коли він доступний ззовні, але мережа, що стоїть за ним, ні.

Захист МЕ має відповідати суворим вимогам - від фізичного захисту доступу до критичного постійного оновлення операційної системи

За основною відмінною рисою МЕ, якою є рівень його моделі, МЕ поділяються на:

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

- МЕ з пакетною фільтрацією або екрануючі маршрутизатори;
- шлюзи прикладного рівня;
- шлюзи сеансового рівня чи рівня з'єднання;
- МЕ експертного рівня.

Найпростішим класом МЕ є фільтри пакетів, які працюють на мережевому та транспортному рівні OSI, виконуючи фільтрацію за допомогою порівняння параметрів заголовка мережевого пакета з набором правил фільтрації.

Шлюз сеансового рівня виключає пряму взаємодію двох вузлів на рівні сеансу моделі OSI та підключається до обох сторін обміну інформацією, при тому не з'єднуючи їх і не даючи їм проникнути у внутрішню мережу. Передача відбувається завдяки копіюванню пакетів, які передалися за один сеанс. Після завершення сеансу записи видаляються з таблиці з'єднання.

Шлюзи прикладного рівня виконують аналіз пакетів на рівні програми та презентації. Зазвичай це універсальні комп'ютери, які підтримують захисних агентів, які, у свою чергу, інтерпретують протоколи на рівні програми. Ці програми блокують передачу пакетів повідомлень безпосередньо між зовнішньою та внутрішньою мережами. Обмін інформацією між мережами відбувається через проміжне програмне забезпечення, яке фільтрує потік повідомлень.

Експертні МЕ мають можливість стежити за станом мережевих з'єднань під час фільтрації пакетів. Вони прозорі для кінцевого користувача і не вимагають додаткових налаштувань, також вони не змінюють IP-адреси пакетів, які проходять через них, тим самим дозволяють протоколам функціонувати належним чином на рівні програми, що і є їх великою перевагою на іншими.

Частково МЕ може також містити комутаційні пристрої, які дозволяють диверсифікувати доступ до мережі. Комутатори мають можливість фільтрувати трафік на основі MAC-адрес, але на жаль у наш час цей метод вже неефективний.

Однією з особливостей МЕ є простота адміністрування. Це дуже актуально, том що помилка у визначенні правил доступу може легко створити потенційну вразливість. Тому більшість МЕ працює із інструментами, що мають

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

можливість виконувати функції введення, видалення або перегляду набору правил.

Найбезпечнішим варіантом адміністрування МЕ є адміністрування лише з локального терміналу, що не завжди є зручним. Тому частіше за все для цього використовується віддалений доступ, який виконується тільки за умов розширеної аутентифікації.

На МЕ має бути лише два користувачі: адміністратор МЕ та адміністратор архіву, щоб запобігти несанкціонованим змінам у системі.

Необхідно записувати дії, які виконуються МЕ – збої, вхідні та вихідні з'єднання, час з'єднання, зміна конфігурації та інші. Це називається журналюванням. МЕ мають можливість сповіщати про деякі події, такі як: повідомлення консолі, повідомлення електронної пошти або SMS тощо. Негайне та вчасне сповіщення допомагає швидше відреагувати в разі спроби вторгнення.

Призначення МЕ як основного, вторинного або кешуючого DNS-сервера покращує продуктивність мережі та приховує інформацію про внутрішню мережу. Також внутрішні хости можуть забезпечити внутрішню маршрутизацію до серверів.

Основним механізмом будь-якого проксі-сервера є трансляція мережевих адрес (NAT). Він виконує функції безпеки шляхом заміни IP-адрес і портів та зберігає загальнодоступні IP-адреси, перетворюючи багато внутрішніх IP-адрес на менш загальнодоступні (до однієї). Це використовується майже всіх мережах світу, тому що це запобігає або обмежує доступ до внутрішніх хостів ззовні, в той час як можливість доступу зсередини назовні залишається.

1.2. Охорона периметра та її організація в сучасних мережах

Більшість людей у сучасних містах постійно надсилають або отримують величезні обсяги інформації. У наш час люди винайшли велику кількість методів для передачі інформації. Звичайні технології, які мали б ледь неповністю задовольняти усі потреби людини, замінюються ні більш досконалі та нові.

		Медведев А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Для високошвидкісної передачі інформації створюються спеціальні канали передачі даних. Тут, як правило, використовують програмно-технічне забезпечення, яке з'єднує мережі і абонентів між собою та забезпечує швидку й безпечну передачу різної інформації.

Для системних адміністраторів завжди стоїть питання захисту мережі від крадіжки конфіденційної інформації. Провідні аналітичні центри підтверджують, що кількість інцидентів інформаційної безпеки зростає з кожним роком.

Зараз технології електронних платежів і документообігу швидко розвиваються, тому будь-який збій мережі може призвести до збоїв у роботі банків або цілих корпорацій і призвести до величезних матеріальних втрат. Щоб цьому запобігти, потрібно організувати захист інформації в мережі.

Питання, чи вибрати для підприємства хмарні обчислення (хмара), чи локальні рішення – вже не таке болюче, як було раніше. Не так давно експерти розглядали хмарні та локальні рішення як дві абсолютно різні між собою області, але сьогодні відмінності між ними все більше стираються.

Колись локальна інфраструктура як правило потребувала немалих початкових інвестицій, коли ж хмарні оцінювали лише за фактичною вартістю. У той час хмарні середовища також мали складні схеми оплати, додаткові витрати на передачу даних та платежі за контрактом API. Нині існують постачальники фізичного обладнання, «хостери», які пропонують подібний метод оцінки своїх ресурсів. Тут слід розуміти, що якщо компанія не в змозі негайно інвестувати значні суми в придбання всієї IT-інфраструктури, можна знайти спосіб розподілити витрати в часі без використання загальнодоступної хмари.

Також часто зустрічається така думка, що хмара може бути менше захищеною, тому що одна інфраструктура використовується кількома користувачами. В теорії хмара має меншу ізоляцію даних і є більша ймовірність витоку з одного хмарного клієнта до іншого. Але з часом така думка зникла. Через неадекватно побудовану хмарну архітектуру серйозних кібератак майже

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

не було. Тепер можна навіть сказати, що хмара стає набагато більш безпечною, аніж локальна мережа. Хмарні інфраструктури керування обліковими даними ISP надають жорсткіший контроль доступу, ніж локальні середовища.

З початку розвитку хмарних сервісів відчувалося, що дотримання в хмарі правил складніше через те, що компанії мають менше контролю над своєю хмарною інфраструктурою, а постачальники хмарних послуг не надають регуляторних послуг. Всі основні постачальники хмарних послуг дотримуються дуже складних правил і стандартів, тому твердження про те, що більшість компаній не можуть працювати на хмарних платформах, звучить майже абсурдно.

Безсумнівною перевагою хмарних ресурсів була можливість їх масштабування без обмежень. Ресурси зазвичай важче додати локально, оскільки потрібно встановити нове обладнання, що означає витрати на його придбання та час на налаштування. Зараз починають з'являтися все більше і більше так званих гібридних хмарних платформ наступного покоління, наприклад таких як AWS Outposts (рис.1.5) і Azure Stack (рис.1.6). За їх допомогою можна створювати локальні середовища.

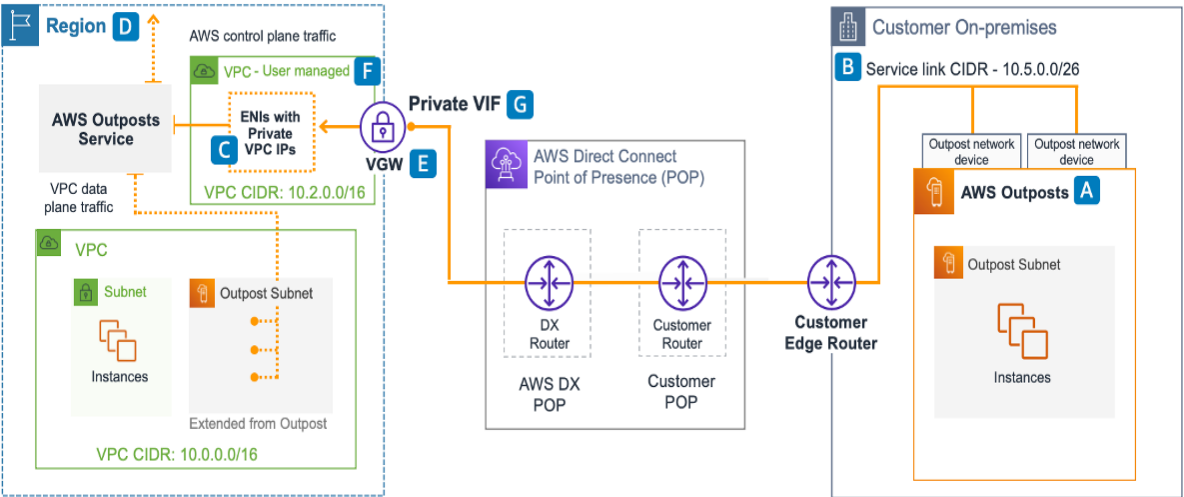


Рисунок 1.5 – Приклад роботи AWS Outposts

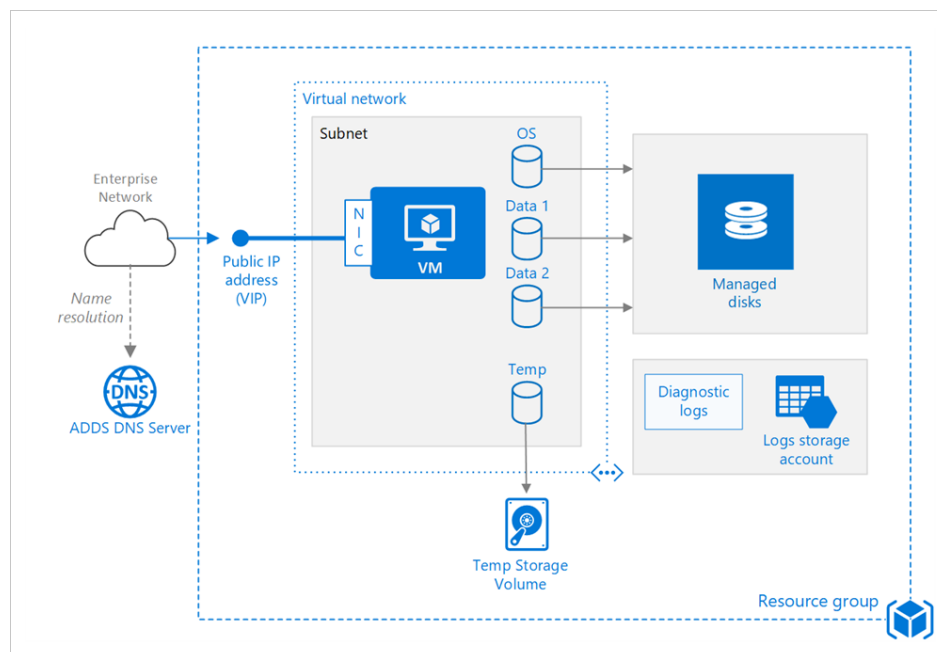


Рисунок 1.6 – Приклад роботи Azure Stack

Ще одна кардинальна відмінність полягала в тому, що керування хмарними сервісами здійснювалося за допомогою спеціальних інструментів, які сильно відрізнялися від тих, які використовуються в локальному середовищі. Сьогодні розгортання та керування декількома робочими процесами однаково незалежно від того, де вони працюють: локально, у хмарі чи в гібридній моделі. Це пов'язано з поширенням таких платформ, як Kubernetes, які абстрагуються від базової інфраструктури та забезпечують рівномірне розгортання незалежно від того, де використовуються програми. Вона об'єднує процес розгортання та керування та виглядає однаково, незалежно від того, чи складається інфраструктура з локальних серверів, або є загальнодоступною хмарою.

Звичайно, між цими середовищами досі є відмінності, які відображаються в деяких типах робочих навантажень. Але зараз обирати між хмарним або локальним середовищем стало вже неактуально. Подібно до того, як відмінності між операційними системами стали менш істотними, сьогодні вибору між хмарою та локальним середовищем приділяється все менше уваги.

Ще з десятирок років тому захист периметра корпоративної мережі був обов'язковим компонентом системи інформаційної безпеки організації. У наш же час, коли співробітник компанії може працювати будь-коли та будь-де, а

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

обчислення переносяться в хмарне середовище - важко встановити чіткий периметр корпоративної мережі.

Через те ще дуже довго структура локальних мереж буде класичною і схожою на фортецю. Дивлячись на локальну мережу, можна помітити, що існує внутрішня частина зі своїми точковими підключеннями, які здійснюють доступ до глобальної мережі, утворюючи зовнішній периметр. Вони повинні бути добре захищеними від проникнення у мережу. Щоб цього запобігти, реалізують багаторівневу систему захисту інформації на зовнішньому кордоні мережі.

Існує декілька потенційних загроз порушення прав доступу та мережі:

- порушення роботи обладнання;
- втрата інформації через некоректну роботи ПЗ;
- втрата інформації, що пов'язана з несанкціонованим доступом;
- втрата інформації, що пов'язана з неправильним зберіганням архівних даних;
- помилки обслуговуючого персоналу і користувачів.

Існує два види несанкціонованого доступу: з фізичним доступом до елементів мережі і без нього.

Маючи фізичний доступ, будь-який зловмисник має можливість використовувати пряме підключення до пристроїв. А вже потім, залежно від того, що він хоче, має можливість отримати бдь-яку інформацію. Якщо фізичного доступу немає, описані вище дії виконуються віддалено через Інтернет.

Зараз створюють спеціальні технічні рішення та інструменти через те, що кількість атак на мережу зростає з кожним днем, які ґрунтуються на таких принципах інформаційної безпеки як конфіденційність, цілісність, доступність.

Інформаційна безпека поділяється на два типи:

- технічні (апаратні) заходи;
- програмне забезпечення.

Технічні заходи захисту включають у себе різні фізичні, електричні, електромеханічні або електронні пристрої, які підключаються безпосередньо в

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

пристрої локальної мережі. Також до цього списку можна віднести такі пристрої як охоронна сигналізація, дверні замки, віконні решітки та інші.

Такі інструменти надійні і не залежать від суб'єктивних факторів. Недоліком цих засобів є досить мала адаптивність, яка обмежує область їх застосування. Окрім цього, зачасту вони мають великий розмір і вагу, через це ускладнюється їх транспортування. Також до мінусів також можна віднести і їх ціну

Якщо потрібно захистити окремих комп'ютер, набагато краще буде використати програмний засіб безпеки. Його досить легко адаптувати до певних змін, вони досить прості та зручні в монтажі і користуються великою популярністю.

Програмні засоби захисту поділяють на:

- засоби архівації даних;
- антивірусні програми;
- криптографічні програми;
- засоби ідентифікації і автентифікації користувачів;
- засоби керування доступом;
- протоколювання та аудит.

Сьогодні більшість сучасних операційних систем вже мають вбудоване програмне забезпечення безпеки. Але вони можуть забезпечити захист лише на базовому рівні, тому краще встановлювати додаткове спеціалізоване програмне забезпечення.

Програмні та апаратні засоби безпеки також мають умовний розподіл. В даний час розвиток даних технологій спрямований на поєднання цих засобів і підвищення захисту. Такі гібридні інструменти зараз найбільш поширені в сферах контролю доступу. Гібридні рішення поєднують переваги та недоліки апаратного та програмного забезпечення.

Також є й організаційні заходи протидії. Основні переваги – необмежені можливості модифікації та розвитку, недоліки – висока залежність від відповідальності користувачів, дотримання ними норм і правил.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Експерти вже довели, що навіть використовуючи будь-який з цих заходів, не можна забезпечити сто відсотків збереження інформації. Тому рекомендується поєднувати всі перераховані вище засоби для захисту інформації.

1.3. Охорона периметра та вибір виробників внутрішнього мережевого обладнання

Вибір буде базуватися на дослідженнях консалтингової компанії Gartner, яка використовує власні високоякісні методи аналізу даних (рис.1.7).



Рисунок 1.7 – Рейтинг виробників МЕ від Gartner

Дана компанія кожного року публікує звітність маркетингових досліджень. Ці документи показують як позитивні та негативні риси і враховуючи це все формують власний рейтинг.

МЕ розвивається, щоб захистити нові мережеві програми, включаючи хмари, і значно збільшити кількість віддалених працівників. Провайдери МЕ Неохоче реагують на розвиток гібридних мереж, тому що вони користуються значною популярністю та підтримкою. Але перспективи розвитку досить позитивні.

Так, припускається, що до 2025 року 30% нових розгортань МЕ розподіленого офісу перейде на МЕ як послугу, порівняно з менш ніж 5% у 2020 році.

Gartner визначає ринок МЕ як переважно МЕ, які мають двонаправлену фільтрацію для захисту мережі. Ці мережі можуть бути локальними, гібридними, загальнодоступними або приватними хмарами.

Цей ринок тепер також включає постачальників, що пропонують віртуальні версії та МЕ як послугу (FWaaS) (рис.1.8).

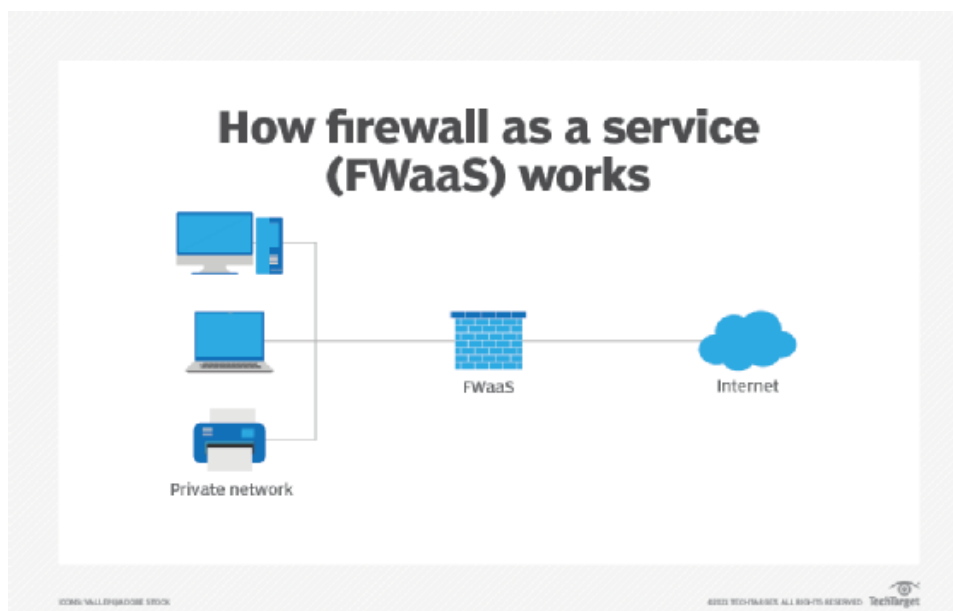


Рисунок 1.8 - Як брандмауер як послуга працює

МЕ також можуть запропонувати додаткові можливості, такі як розпізнавання програм і керування ними, виявлення та запобігання вторгненням,

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

покращене виявлення шкідливих програм, а також ведення журналів і звітування.

Таким чином, виходячи з вищесказаного, стає зрозумілим, що тенденцією останніх років є програмно-апаратні рішення, які поступово змінюють виключно програмні чи апаратні системи.

Одним з провідних виробників обладнання є Cisco Systems. Cisco - американська транснаціональна корпорація, найбільший у світі виробник мережевого обладнання для мереж віддаленого доступу, служб безпеки, мереж зберігання даних, маршрутизації та комутації, а також для комерційного IP-зв'язку та корпоративних ринків.

Cisco Systems була заснована в грудні 1984 року Леонардом Бозаком і Сенді Лернером, двома вченими-комп'ютерниками Стенфордського університету, які відігравали важливу роль у підключенні комп'ютерів у Стенфорді. Вони започаткували концепцію локальної мережі (LAN), яка використовується для підключення віддалених комп'ютерів через систему багатопрокольних маршрутизаторів.

Cisco має досить широкий вибір рішень безпеки для того, щоб захистити будь-який пристрій і будь-яке середовище, від локальної мережі до хмари, в залежності від того, що потрібно. Передові рішення в цій галузі наявні в серіях програмно-апаратних середовищ безпеки цієї компанії, які можна повністю конфігурувати та інтегрувати.

Cisco пропонує широкий асортимент продуктів і успішно спрямовує клієнтів до корпоративних ліцензійних угод, які часто включають підписку та підтримку ME.

Лінійка пристроїв адаптивної безпеки Cisco (ASA) активно працює з 2005 року. Сімейство пристроїв безпеки Cisco ASA захищає корпоративні мережі та центри обробки даних усіх розмірів. Він надає користувачам високобезпечний доступ до даних і мережевих ресурсів — у будь-який час, у будь-якому місці, за допомогою будь-якого пристрою.

		Медведевко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

В даний час Cisco пропонує декілька серій ME, головними з яких є Cisco Firepower Threat Defense, Next Generation Firewall (NGFW) і серія Meraki MX.

Також Cisco може запропонувати FWaaS як частину свого захищеного інтернет-шлюзу Umbrella та Industrial ME (серія ISA).

Асортимент обладнання від цього виробника ледь не найбільший, має широкий діапазон цін і опцій, які зможуть задовольнити будь-якого клієнта, незалежно від його вимог.

Особливий інтерес на ринку представляє рішення Cisco Meraki MX (рис.1.9), яке надає клієнтам невеликих офісів прості в налаштуванні, розгортанні та управлінні рішеннями безпеки та мереж.



Рисунок 1.9 – Міжмережний екран Cisco Meraki MX

Cisco Meraki MX - це багатофункціональні корпоративні пристрої безпеки та SD-WAN з широким набором можливостей для вирішення різних завдань - від пристрою "все в одному". Організації будь-якого розміру та у всіх галузях покладаються на MX для забезпечення безпечного підключення до вузлових точок або багатохмарних середовищ. MX на 100% керується хмарою, тому встановлення та віддалене управління дійсно не вимагають участі користувача. Люди відзначають високоякісну VPN від Cisco і повідомляють, що VPN типу Site-to-Site є стабільною та нескладною в налаштуванні.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Але все ж таки у цієї корпорації є ряд недоліків, які заважають їй досягти лідерської позиції. Тому Cisco пропонує кілька різних порталів управління безпекою, що викликає багато одноманітної інформації та плутанини в спільноті кінцевих користувачів. Постачальник пропонує Cisco DefenseOrchestrator як централізованого хмарного менеджера, Cisco Threat Response Cloud Threat Correlation (CTR), Cloud Reporting Portal for Security Analytics and Logging (SAL), а також останнє доповнення, SecureX Improved Detection and Response Platform.

Хоча існує кілька продуктів хмарної безпеки, постачальник пропонує лише підтримку AWS та Azure для Cisco NGFWv, ASA v та ASA для Cisco Meraki vMX. Натомість вони не інтегруються з платформою захисту хмарного навантаження Cisco Tetration.

Якщо подивитися на інфраструктуру мережевого обладнання підприємства в загальному плані, то ці недоліки можна не є вже такими суттєвими через те, що є потужних серії маршрутизаторів та комутаторів, які досить легко підключаються один до одного та з ME від одного виробника. Кількість моделей маршрутизаторів виробництва Cisco дуже велика, що дозволяє задовольнити будь-які побажання та потреби замовника. Значною перевагою більшості роутерів є можливість змінювати та додавати модулі, що робить моделі ще більш гнучкими.

1.4. Огляд та вибір систем реєстрації, аналізу та візуалізації інцидентів безпеки

Управління інформацією та подіями безпеки (SIEM) — це галузь у сфері комп'ютерної безпеки, де програмні продукти та послуги поєднують управління інформацією про безпеку (SIM) та керування подіями безпеки (SEM) (рис.1.10). Вони забезпечують аналіз у режимі реального часу сповіщень безпеки, які генеруються програмами та мережевим обладнанням. Постачальники продають SIEM як програмне забезпечення.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.10 - Управління інформацією та подіями безпеки

Система управління інформацією та подіями безпеки є фундаментальним елементом кібербезпеки. Керування журналами, виявлення вторгнень, кореляції подій, збору інформації про загрози, управління інцидентами, забезпечення виконання стандартів реагування та оцінки вразливості – з усім цим допомагає впоратися програмне забезпечення SIEM.

В інфраструктурі компаній часто відбуваються порушення користувацьких політик або вторгнення зловмисника в локальну мережу. Рішення класу SIEM використовуються для аналізу інформації про події та централізованого збору. Головною метою таких систем є автоматизація процесу виявлення інцидентів, своєчасне інформування спеціалістів із безпеки, збір інформації про події з різних джерел – мережевих пристроїв, програм, журналів операційної системи, засобів безпеки.

Незалежно від того, які системи SIEM ви розглядаєте, у них є декілька важливих факторів, на які потрібно звернути увагу.

Одним з перших і найважливіших факторів є виявлення вторгнень, тому що ефективний підхід до цієї функції має вагомий вплив. Важливим аспектом є аналіз усіх даних у реальному часі, тому інструмент повинен відрізняти нешкідливі невдалі спроби входу та інтенсивні атаки.

Автоматичні сповіщення також є надзвичайно важливою функцією, адже після виявлення вторгнення потрібно якомога швидше повідомити про це адміністратора.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Також використовують журнал подій, щоб бачити всю хронологію подій у реальному часі.

Ще однією з важливих функцій є функція зберігання та фільтрації даних. Дані мають зберігатися в архіві для того, щоб до їх можна було переглянути в будь який момент і попередити подальші ризики.

Багато щоб була функція візуалізації даних, оскільки допомагає у сприйнятті інформації людиною. Графіки, лічильники та кольорове кодування дозволяють користувачеві в найкоротші терміни отримати уявлення про те, що відбувається в системі.

За останні десять років інструменти SIEM значно покращилися, розширили свої функціональні можливості у відповідь на інциденти. У наш час більшість інструментів SIEM використовують алгоритми машинного навчання, щоб мати змогу аналізувати більше даних за менший час. Ці інструменти спрощують адміністрування IT-інфраструктури, пропонуючи не тільки детальний огляд корпоративних середовищ, але й забезпечуючи ефективні інтелектуальні дані замість нескінченного потоку журналів і сповіщень.

Фахівці з усього світу діляться з усіма досвідом налаштування, а це свідчить про те, що інструмент постійно розвивається. Але на жаль безкоштовні інструменти просто не мають змоги запропонувати повноцінне рішення SIEM корпоративного класу.

Основна проблема відкритих систем SIEM полягає в тому, що вони зазвичай вразливі до атак і не спроможні виявляти шахрайські дії. Ці програми, як правило, мають обмежений бюджет, і тому менш зручні у використанні, ніж їхні платні аналоги.

Тому аналіз, яку систему вибрати, слід проводити з урахуванням як безкоштовної, так і платної версії. Далі розглянемо кілька прикладів популярних систем SIEM:

1. Splunk Enterprise Security. Це передове рішення SIEM, відоме своїми можливостями моніторингу безпеки в реальному часі та аналізу даних. Система заснована на алгоритмах машинного навчання, які виявляють аномалії з меншою

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

кількістю помилкових спрацьовувань. Це дозволяє підвищити безпеку за рахунок покращеного виявлення загроз (рис.1.11).

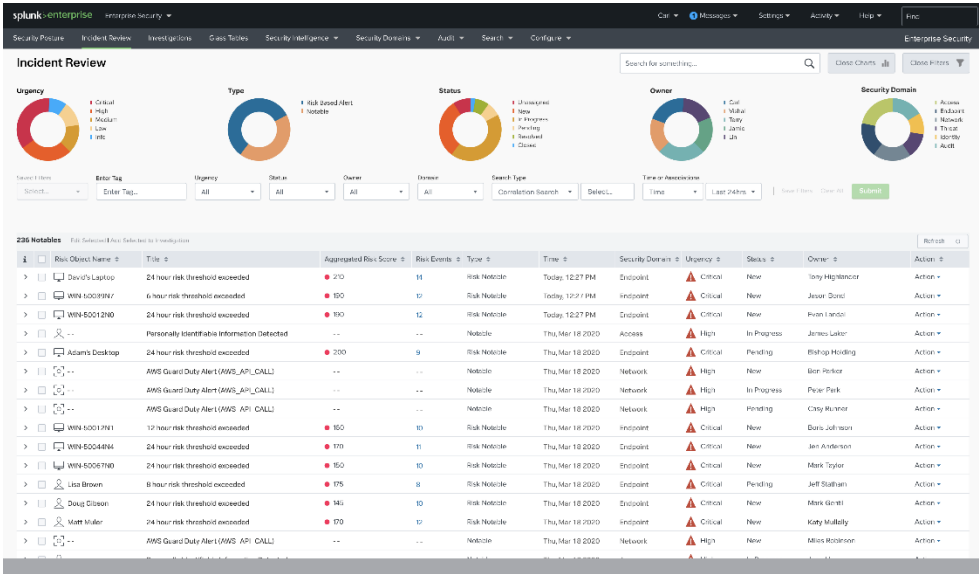


Рисунок 1.11 – Інтерфейс Splunk Enterprise Security

Splunk Enterprise Security вирішує широкий спектр випадків аналітики безпеки та операцій, включаючи безперервний моніторинг безпеки, розширене виявлення загроз, відповідність вимогам, розслідування інцидентів, криміналістичну експертизу та реагування на інциденти. Splunk ES забезпечує наскрізне уявлення про положення безпеки організацій з гнучкими дослідженнями, продуктивністю та гнучкими варіантами розгортання, які пропонуються в хмарних, локальних або гібридних моделях розгортання. Але через те, що це рішення безпеки преміум-класа, воно вимагає платної ліцензії.

2. SolarWinds Threat Monitor. Використовується для постачальників керованих послуг, які пропонують послуги операційного центру безпеки (SOC) для бізнесу. Один з кращих варіантів для моніторингу активів у гібридних хмарних середовищах. Також він збирає велику кількість даних про загрози з багатьох зовнішніх джерел, щоб бути в курсі останніх загроз (рис.1.12).

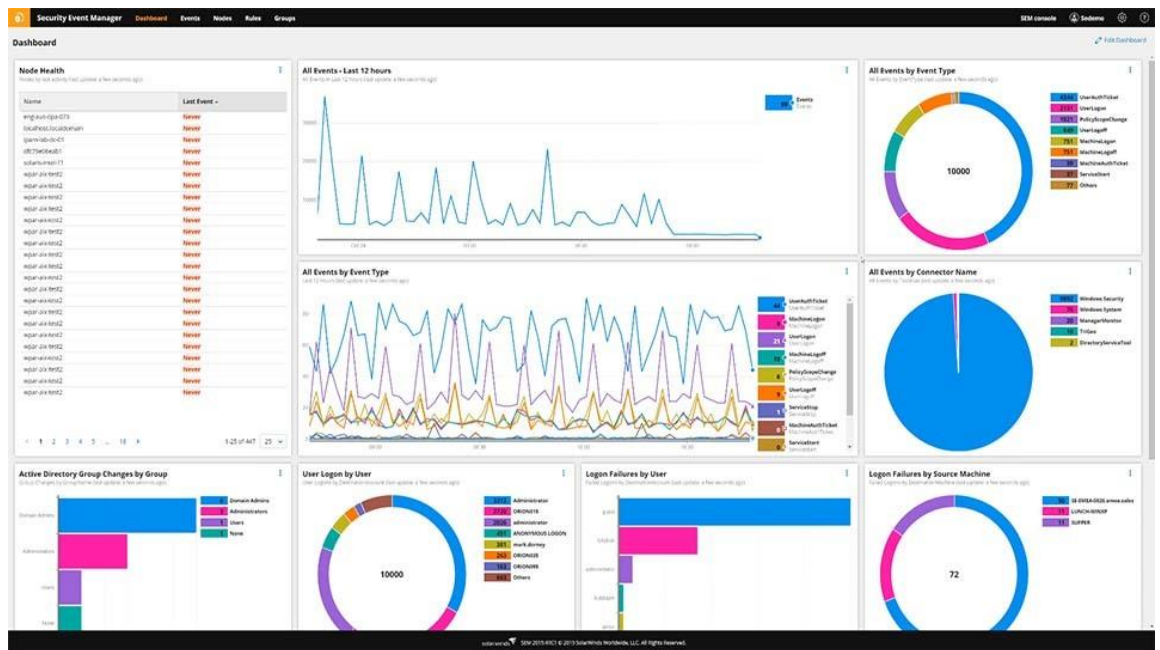


Рисунок 1.12 – Інтерфейс SolarWinds Threat Monitor

3. ManageEngine EventLog Analyzer. Комплексний інструмент SIEM, що охоплює всі аспекти управління та аналізу журналів, доступу користувачів і аудиту продуктивності, моніторингу цілісності програм і файлів, а також звітів про відповідність. Він звіряє журнали у реальному часі з визначеними правилами, що допомагають запобігти множинним кібератакам і багатьом порушенням (рис.1.13).

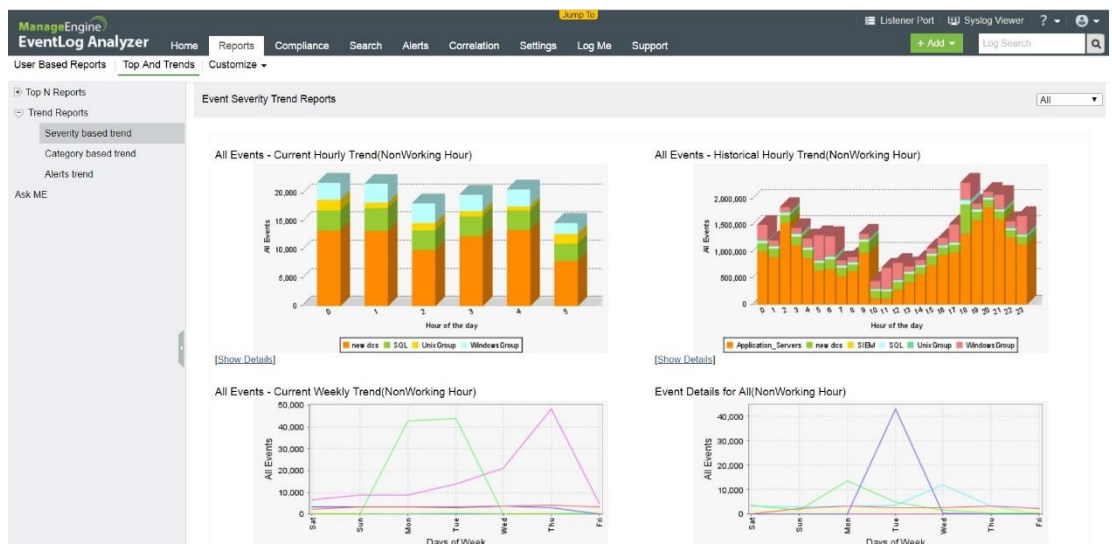


Рисунок 1.13 – Інтерфейс ManageEngine EventLog Analyzer

Коли справа доходить до пристроїв Windows, працювати з терабайтами даних журналу подій, які вони створюють, може бути складно. Завдяки EventLog Analyzer, потужному інструменту керування журналом подій, який забезпечує

		Медведенко А. В.							Арк.
		Покотило О. А.							29
Змн.	Арк.	№ докум.	Підпис	Дата					

наскрізне керування журналами подій, адміністратори безпеки можуть автоматизувати процеси, включаючи збір журналів у мережі та архівування цих журналів у заздалегідь визначений час. Важливою функцією інструмента керування журналом подій є збір журналів подій з усіх можливих джерел. Можливості збирання журналів подій у EventLog Analyzer є винятковими завдяки підтримці як безагентних, так і методів збору журналів на основі агентів.

4. ArcSight Enterprise Security Manager. Потужне рішення SIEM, яке має змогу зібрати та співвіднести до 100 000 подій в секунду. Він має досить просте налаштування та дозволяє збирати дані про події з 500 різних пристроїв, включаючи кінцеві точки, IPS, сервери, хмари тощо (рис.1.14).

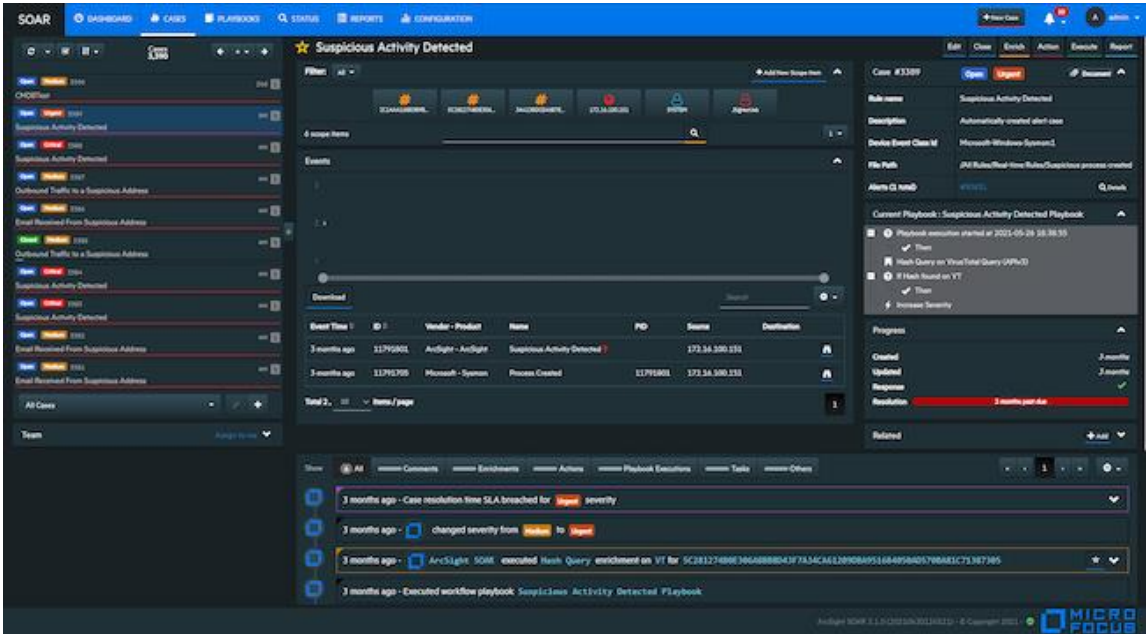


Рисунок 1.14 – Інтерфейс ArcSight Enterprise Security Manager

ArcSight ESM аналізує та співвідносить кожну подію, що відбувається в організації — кожен вхід, вихід із системи, доступ до файлу, запит до бази даних — для точного визначення пріоритетів ризиків безпеки та порушень відповідності. ArcSight Enterprise Security Manager (ESM) надає підхід аналітики великих даних до безпеки підприємства, перетворюючи великі дані в практичний інтелект.

Виходячи з усього вищесказаного, можна проаналізувати дані систем SIEM і вибрати одну з них для цього проекту. Спочатку потрібно перевірити чи містить

система необхідні функції, розглянути простоту налаштування та введення в експлуатацію, фінансові критерії.

Найкращим рішенням для операційної системи Windows буде SolarWinds Security Event Manager. Він досить простий та доступний у користуванні, дозволяє користувачу швидко розпочати роботу та отримати корисні інтелектуальні дані, не витрачаючи багато часу на його налаштування.

Крім того до переваг цього рішення можна віднести пробний період, що дає змогу протестувати дане ПЗ та прийняти рішення про його подальше використання.

Для Linux-серверів можна використати на AlienVault Unified Security Management.

AlienVault Unified Security Management (USM) – платформа All-In-One, розроблена для забезпечення малих та середніх організацій можливостями ефективно захищати себе від сучасних передових загроз (рис.1.15).

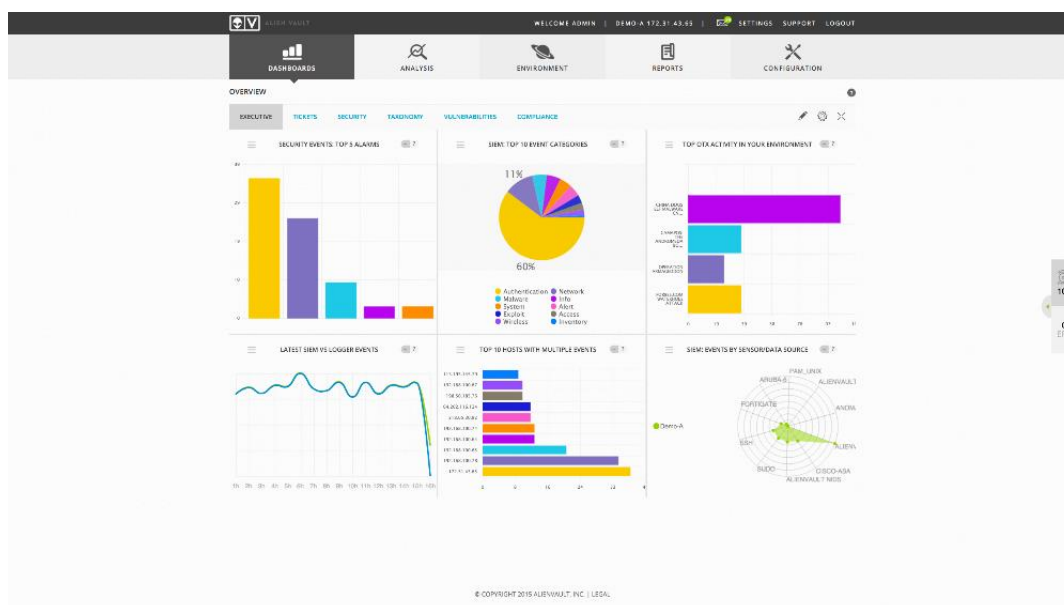


Рисунок 1.15 – Інтерфейс AlienVault Unified Security Management

USM включає 5 найважливіших функцій безпеки для спільного управління загрозами та відповідності нормативним вимогам. Розуміючи, що сучасні IT-інфраструктури є дуже чутливими до впровадження рішень, розробник використовує активні, пасивні та хост-технології так, щоб не порушити відповідність існуючим вимогам.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Порівнюючи SolarWinds Security Event Manager та AlienVault Unified Security Management, функціонально між собою вони майже однакові. Також вони досить прості у налаштуванні, що дозволяє швидко включати їх в існуючу мережу. Але у AlienVault USM є один вагомий плюс, він потребує майже вдвічі менше ресурсів процесора і оперативної пам'яті, тому цей продукт був обраний для цієї мережі.

Висновки до розділу 1

Отже, в результаті аналізу було визначено основні принципи захисту внутрішніх мереж та обрано захист периметра на основі ME.

Розглянуто 4 існуючі види ME та проаналізовано всі їх плюси та мінуси. Дослідження цих типів ME показали, що пристрої, що використовуються в цій топології, є екрануючими маршрутизаторами та ІЕ експертного рівня.

Проведено аналіз мережевого обладнання від Cisco Corporation. Аналіз проводився на основі дослідження компанії Gartner.

Розглянуто концепцію інформаційної безпеки та системи управління подіями. Проаналізовано найпопулярніші рішення на ринку та вибрана система SIEM, яка буде використовуватися в цьому проекті.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ РЕЄСТРАЦІЇ ПОДІЙ БЕЗПЕКИ, АНАЛІЗУ, ВІЗУАЛІЗАЦІЇ

2.1. Організація мережі проекту

У цій роботі було розглянуто організаційну мережу, яка представлена шістьма офісами подібної структури. Вони складаються з офісних комутаторів, серверів, робочих станцій, периметральних мережевих пристроїв і принтерів. Також є можливість збільшити кількість кінцевих пристроїв у мережі.

Для з'єднання мережевих пристроїв між собою використовуються порти FastEthernet і GigabitEthernet, які мають пропускну здатність 100 Мб / с та 1000 Мб / с відповідно.

Операційна мережа організації була побудована на комутаторах Cisco, ME та маршрутизаторах.

Нижче наведено серію пристроїв, які використовуються для побудови даної мережі.

Одним з найпопулярніших та найбільш універсальних рішень є маршрутизатор Cisco серії 7200 (рис.2.1-2.2), який є одним з основних пристроїв у цій мережі. Серія підтримує досить велику кількість інтерфейсів, через це є можливість розвивати мережу активно [19].



Рисунок 2.1 – Cisco series 7200

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33



Рисунок 2.2 – Cisco series 7200

Маршрутизатори серії 7200 стали відомими по всьому світу, безліч компаній довірили свій мережевий інтерфейс цим пристроям. Володіючи високою продуктивністю, маршрутизатори здатні відправляти дані кількома потоками, тим самим, такий прийом передачі інформації сприяє розширенню можливостей обчислювального центру. При створенні локальної мережі важливо впроваджувати у середовище лише найкращі конфігурації.

Таке широке поширення пояснюється тим, що компанії необхідні маршрутизатори, що підтримують велику кількість інтерфейсів. Маючи таку здатність, сімейство маршрутизаторів Series 7200 активно використовується не тільки великими компаніями, а й підприємствами-початківцями, адже від цього повною мірою залежатиме майбутній розвиток обчислювального центру. Швидкість виконання завдань залежить від того, який центр управління має пристрій. Маршрутизатори серії 7200 оснащені процесорами, розробленими безпосередньо розробниками цієї компанії.

Маршрутизатори можуть надсилати дані кількома потоками, оскільки вони мають високу продуктивність. Таким чином можна збільшити швидкість обміну інформацією, чому в свою чергу сильно сприяють мікросхеми Cisco 7200 NPE-G2 (рис.2.3). Завдяки цьому процесору можна створити мережеву платформу, яка не тільки зможе досить швидко передавати дані, але і впорається з

		Медведев А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

перевантаженістю каналів передачі. Значною перевагою даних маршрутизаторів є простота в управлінні та обслуговуванні та підвищена гнучкість.



Рисунок 2.3 - Мікросхема Cisco 7200 NPE-G2

Також ці маршрутизатори мають до 5000 віртуальних мереж на IPsec.

Крім того, серед основних пристроїв є ще одна серія пристроїв Cisco Systems - Cisco ASA 5500 (рис.2.4). Ця серія модульних багатофункціональних захисних пристроїв є продовженням лінійки Cisco PIX, яка колись була достатньо популярним рішенням для захисту периметра мережі.



Рисунок 2.4 – Міжмережні екрани лінійки Cisco ASA 5500

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

Багатофункціональні пристрої захисту серії Cisco ASA 5500 дозволяють налаштувати безпеку відповідно до специфічних вимог компанії у доступі та бізнес-політиками, мають можливість поповнювати набір функцій та проводити оновлення систем. Вони включають в себе новітні технології забезпечення безпеки контенту, шифрування, автентифікації, авторизації та запобігання вторгненням.

Серія ASA 5500 дозволяє активно реагувати на мережеві атаки та запобігати їм ще на ранній стадії, а також забезпечує комплексний захист мережі.

Якщо розглядати на прикладі інфраструктури підприємства, то класичний ME тут замінений на ASA 5500. Це дозволяє захистити або окремі сегменти, або всю мережу, а ще функціонал цього рішення набагато ширше [1].

В додаток до того, ASA 5500 підтримує функцію резервування каналів доступу до Інтернету, протоколи динамічної маршрутизації OSPF і RIP, а також механізми якості обслуговування (QoS).

Для взаємодії з мережевими пристроями краще використовувати комутатори Cisco Catalyst 2960 (рис.2.5), які мають великий спектр моделей для організації рівня доступу до локальної мережі.



Рисунок 2.5 – Комутатор Cisco Catalyst 2960

Комутатори Cisco Catalyst 2960 – лінійка провідних продуктів серед комутаторів другого рівня. Ці комутатори дозволяють знизити сукупну вартість володіння при розгортанні з використанням IP-телефонів Cisco, точок доступу до бездротової мережі (WLAN) Cisco Aironet або інших пристроїв, сумісних з

IEEE 802.3af. Їхнє використання дозволяє спростити експлуатацію IT-інфраструктури, підвищити рівень безпеки бізнес-процесів, забезпечити стійку роботу мережі, а також надати користувачам можливість роботи в "мережах без кордонів"

Комутатори Cisco Catalyst серії 2960 – це комутатори доступу з фіксованою конфігурацією, призначені для мереж великих та середніх підприємств, а також їхніх філій, що дозволяють знизити сукупну вартість володіння.

Лінійка включає у себе моделі з 8, 24 або 48 портами 10/100 Ethernet + 2-4 портами Gigabit Ethernet, а також моделі з усіма портами 1 Gigabit. Порти комутатора мають технологію PoE (Power over Ethernet) для живлення IP-телефонів або бездротових точок доступу. Існує також підтримка резервного модуля живлення Cisco Redundant Power System 2300.

Більшість Cisco Catalyst 2960 Series не підтримують маршрутизацію, але можуть фільтрувати трафік.

Розробкою цієї серії є комутатори Cisco Catalyst 2960 X / XR (рис.2.6), які мають чудові технічні параметри, є ще більш розумними та продуктивними рішеннями.



Рисунок 2.6 – Комутатор Cisco Catalyst 2960 X

Cisco Catalyst 2960-X – лінійка коммутаторів, що стекуються з підтримкою технології доступу Gigabit Ethernet. Моделі Cisco Catalyst 2960-X забезпечують

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

комутацію другого рівня (L2 layer) та оснащені одним основним блоком живлення з можливістю встановлення додаткового, резервного джерела живлення. Дані комутатори забезпечені 24 або 48 портами Gigabit Ethernet, підтримують технології Power over Ethernet/Power over Ethernet Plus (PoE/PoE+) і чотири канали Gigabit Ethernet Small Form-Factor Pluggable (SFP) або два канали 10 Gigabit Ethernet Small Form-Factor (SFP+). Комутатори працюють на базі двох ядерних процесорів 600МГц. Технологія FlexStack-Plus дозволяє зібрати стек з 8 комутаторів та забезпечує пропускну здатність 80 Гбіт/сек. Для забезпечення візуалізації та контролю трафіку різних програм у мережі, Cisco додали функцію NetFlow Lite, яка дозволяє інженерам моніторити та керувати потоками даних на всіх сегментах мережі [4].

В даний час однією з найбільш використовуваних і поширених серій комутаторів Cisco у світі є серія Catalyst 2960-S / SF, яку фактично замінила згадана серія - Catalyst 2960 X / XR. Використовуючи технологію FlexStack, апаратна платформа комутатора Catalyst 2960-S / SF здатна організувати стек комутаторів зі швидкістю до 40 Гбіт/с, чого достатньо для з'єднання чотирьох комутаторів разом.

Комутатори Cisco Catalyst 2960-S - це потужні функціональні пристрої, що дозволяють організувати надійну локальну мережу, досягти максимальної продуктивності обміну інформацією та високої швидкості комунікацій. Пристрої Cisco Catalyst 2960-S – це гігабітні комутатори фіксованої конфігурації, які можуть об'єднуватись у стек (stack). Призначені для організації рівня доступу до локальної мережі (безпосереднє підключення комп'ютерів/ робочих станцій/ мережевих принтерів).

Через обмежені ресурси комп'ютера, розроблену топологію мережі було дещо спрощено, кількість кінцевих пристроїв зменшено, кількість серверів також зменшено, до того ж, вони є віртуальним і виконують роль кластера серверів. Спочатку були налаштовані параметри IP-адресації для того, щоб усе почало працювати. Протокол динамічної конфігурації хосту (DHCP) використовується для налаштування адресації внутрішньої мережі. Внутрішні

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

мережі поділяються на кілька віртуальних локальних мереж - VLAN, що підвищує рівень безпеки та полегшує налаштування.

2.2. Проект підсистеми захисту периметра

У цьому дослідженні було вибрано три офіси, оскільки це дозволяло аналізувати різні підсистеми захисту периметра. Усі підсистеми показали однаковий результат за результатами первинної перевірки.

Для захисту периметра першої офісної мережі використовуються два пристрої Cisco ASA серії 5500, які мають досить велику кількість технологій для забезпечення інформаційної безпеки.

Крім того, ME, які мають механізми для перевірки пакетів, дають змогу контролювати з'єднання вузлів мережі один з одним і враховувати стан протоколу на 2-7 рівнях. Завдяки цьому можна контролювати стан комунікацій і уникнути несанкціонованого доступу. Механізми аналізу протоколів на рівні програми забезпечують захист від несанкціонованого використання дозволених портів, таких як HTTP-TCP 80, для різних програм.

Cisco ASA 5500 дає змогу налагодити безпечний віддалений доступ до VPN, якщо використовувати технології SSL та IPSec. Їх можна назвати найефективнішими для захисту критичної інформації, під час коли вона передається через ненадійні або загальнодоступні мережі.

Cisco ASA 5500 може працювати в прозорому режимі, що у свою чергу означає, що трафік прозорий для користувача.

Для того, щоб фінансові інвестиції в захист мережевої інфраструктури не були такими високими, а гнучкість при використанні ASA 5500 залишалася на досить високому рівні, Cisco на основі одного фізичного пристрою впровадила кілька віртуальних.

Можна розширити функціональні можливості Cisco ASA 5500 для мережевих атак та роботи за допомогою спеціалізованого програмного забезпечення, якщо установити апаратні модулі захисту контенту та захисту від

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

вторгнень (можна другий модуль, CSC-SSM, який призначається для захисту від шкідливих програм і широкого спектру атак).

Можна використати вбудовані механізми дублювання для того, щоб забезпечити високонадійний доступ до найважливіших ресурсів з двома пристроями Cisco ASA 5500. Якщо один з пристроїв раптом зламається, то другий рівень візьме на себе абсолютно все навантаження, і зробить це так, що користувач можливо навіть і не помітить. Цей процес також ще називають безпечний режим. Він дає можливість двом фізичним пристроям працювати так, ніби це один логічний.

Аварійний режим може працювати в двох варіантах: Активний / Очікування або Активний / Активний.

Перший варіант - Активний / Очікування, означає, що один з пристроїв знаходиться в активному режимі, а інший - в режимі очікування. Якщо у одного пристроя трапляється раптовий збій, тоді інший пристрій переходить в активний режим і продовжує так працювати. У такому випадку одночасно і перевагою, і недоліком є використання ресурсів ME в режимі очікування.

Другий варіант режиму - Активний / Активний. Це означає, що обидва пристрої завжди знаходяться в активному режимі і повністю розділяють навантаження між собою. При збої тільки один блок буде активним і основним, поки другий внутрішній блок не відновить роботу.

Топологія першого офісу досить мала, тому для нормального функціонування внутрішньої мережі потрібно небагато ресурсів. Тому краще буде використати режим Активний / Очікування.

Третій офіс використовує лише граничний маршрутизатор Cisco 7200 як захист. Цей пристрій надає величезний набір сервісів для захисту як маршрутизатора, так і локальної мережі.

Перш за все, цього можна досягти завдяки вбудованим службам безпеки, розширеним функціям AAA (Authentication, Authorization, Accounting) і локальній системі аутентифікації.

		Медведевко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Крім того, маршрутизатори цієї серії забезпечують інтегрований набір рішень IPsec / IU / IPS.

Список контролю доступу - технології ACL і NAT є основою захисту внутрішньої мережі, що дозволяє отримати надійний захист на третьому рівні моделі OSI [2].

Технологія AutoSecure, зовнішній контроль, а також доступ до командної строки, частіше за все використовуються для захисту самого маршрутизатора .

Для забезпечення захисту внутрішньої мережі периметра у другому офісі організації використано двухрівневий захист із застосуванням експертного МЕ та маршрутизатора граничного екранування. Це дозволить відфільтрувати трафік до експертного і захистити внутрішню мережу й пристрій експертного МЕ.

2.3. Опис підсистем, що використовуються для реєстрації, аналізу та візуалізації подій безпеки

Кількість атак на внутрішні мережі постійно зростає, тому системним адміністраторам потрібно створювати максимально захищене інформаційне середовище. Це дуже складне завдання, оскільки воно потребує спеціалізованих інструментів для постійного запобігання будь-якої несанкціонованої діяльності із зовнішнього та внутрішнього середовища мережі, контролю за її використанням та реалізації політики організації щодо захисту її інформації та мережевих ресурсів.

Потрібно також переглянути й інші компоненти, щоб забезпечити ефективний захист мережі:

- 1) політику інформаційної безпеки організації;
- 2) систему захисту хоста внутрішньої мережі;
- 3) систему захисту каналів зв'язку внутрішньої мережі;
- 4) моніторинг та аудит мережі з використанням систем аналізу безпеки та систем виявлення вторгнень;
- 5) план реагування на виявлені атаки.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Перші три компоненти захисту вже реалізовані в корпоративній мережі, тому потрібно реалізувати решту.

Як було написано вище, для цієї роботи було обрано продукт AlienVault. Продукт створений у 2003 році і активно використовується майже у 170 країнах світу. Через це його можна назвати найбільш використовуваним SIEM. AlienVault розробила рішення Unified Security Management (USM) для більш повного рівня безпеки.

Пристрій USM включає ключові функції безпеки та розвідки загроз, які надаються постійно. Через це можна швидко та без проблем виявити загрозу та реагувати на них. USM має вбудовані можливості моніторингу безпеки мережі та візуалізації, що сильно спрощує та збільшує швидкість, з якою інформація сприймається аналітиками корпоративної безпеки.

До того ж це рішення надає наступні функції:

пошук активів у мережі до здійснення шкідливих дій (активне та пасивне мережеве сканування, контроль активів мережі);

визначення підозрілих дій та потенційно зламаних систем (аналіз Netflow, сервіс доступності моніторингу, повне перехоплення пакетів);

визначення вразливих місць мережі (тестування мережі на вразливості та їх безперервний моніторинг);

кореляція та аналіз даних про події безпеки в мережі (log management, кореляція подій, реагування на інциденти, звітність та оповіщення);

виявлення шкідливого трафіку в мережі (мережна та локальна IDS, контроль цілісності файлів).

AlienVault Labs використовує можливості Open Threat Exchange (OTX), першої у світі спільноти розвідки загроз, щоб надати глибше і обширніше розуміння атак і тенденцій зловмисників. Ця спільнота співпрацює та обмінюється мільйонами артефактів загроз як тільки вони виникають. Тим самим вони надають користувачеві глобальне уявлення про тенденції атак і зловмисників, які можуть вплинути на їхню діяльність.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Усі ці функції вже заздалегідь вбудовані та готові до керування через веб-інтерфейс.

Також можна звернути увагу, що USM має декілька версій - All-in-One, Standard, Enterprise, Anywhere і Central. У кожної є свої особливості призначення.

USM All-in-One версія є першим рішенням безпеки в цій лінійці. Вона має три основні компоненти, які необхідні для цієї системи - датчик USM, реєстратор USM і сервер USM. All-in-One можна назвати універсальним рішенням для невеликих мереж. Його легко інтегрувати, оскільки є однокомпонентним, тобто один фізичний або віртуальний сервер забезпечує повну функціональність цієї системи. Максимальна пропускна здатність системи виявлення вторгнень становить 100 Мбіт/с. До того ж якщо порівнювати цю систему з іншими, то вона може працювати навіть на невеликій. Це рішення ідеально підходить для реалізації підсистеми реєстрації, аналізу та візуалізації подій безпеки в цьому корпоративному мережевому проекті.

Якщо мережа зростає, то компоненти завжди можна без проблем розширити за допомогою USM Standard або USM Enterprise, які призначені для середніх і великих мереж відповідно. USM Anywhere трохи спрощує систему, оскільки це сервіс як послуга. Мається на увазі, що компонент Server вже реалізований у хмарному середовищі AlienVault, тому для інтеграції можна лише встановити компоненти Sensor і Logger і підключити їх до Інтернету (рис.2.7).

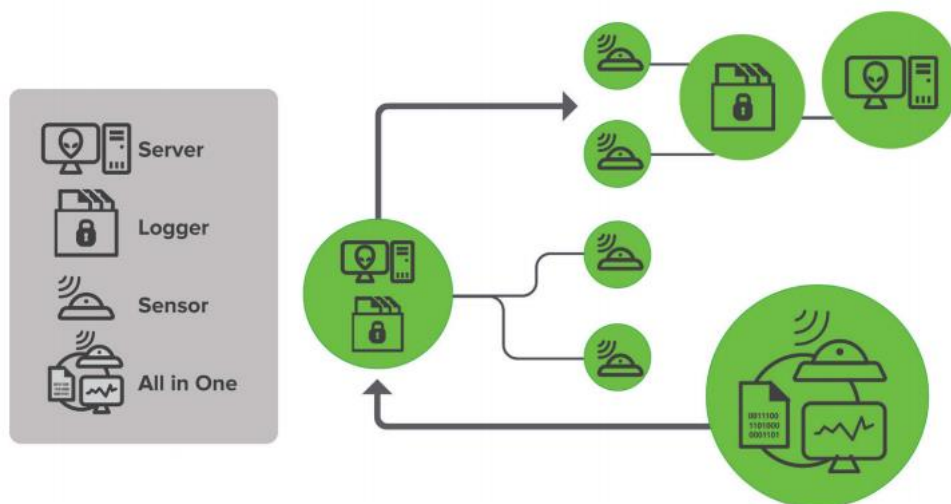


Рисунок 2.7 – Відмінність між USM Standard та USM Enterprise

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Перше розгортання USM Anywhere зазвичай займає приблизно годину, що особливо корисно якщо ресурси та час обмежені. Оскільки USM Anywhere є продуктом SaaS, про розгортання дорогого обладнання можна не перейматися. Все, що потрібно зробити, це впровадити перший датчик USM Anywhere в середовищі, яке потрібно контролювати. Потім датчик подбає про всі потреби моніторингу, включаючи зв'язування та аналіз ресурсів у цьому середовищі, використовуючи власні API та вбудовані інструменти моніторингу безпеки для перевірки мережевого трафіку, збору даних про події системного журналу або збору ваших власних даних у хмарі, а потім забезпечує безпеку трансляції подій, розміщених у захищеній хмарі AlienVault, на USM Anywhere (рис.2.8) [18].

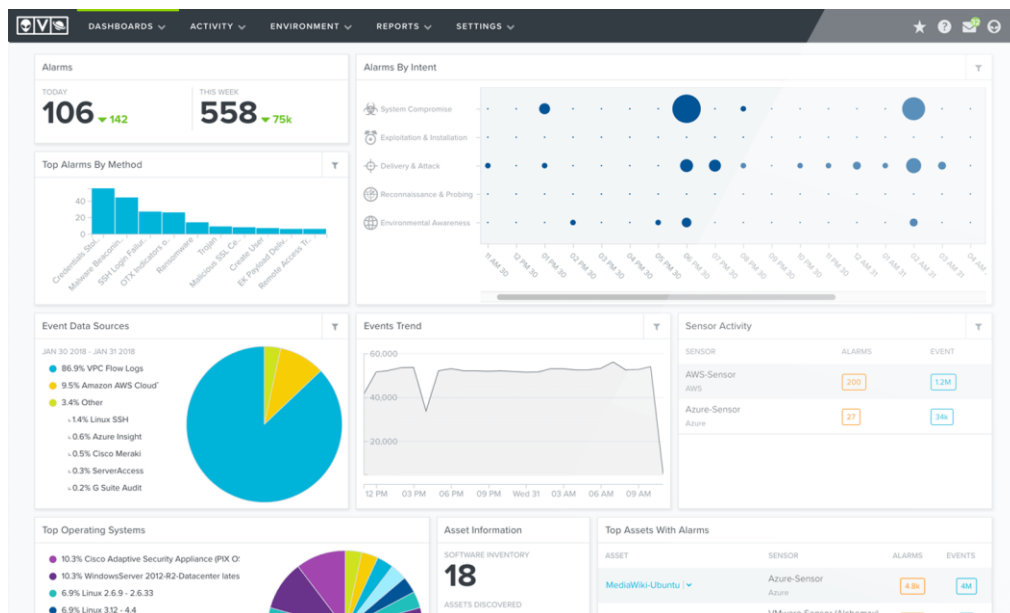


Рисунок 2.8 – Зовнішній вигляд USM Anywhere

Датчики USM Anywhere можна встановити для моніторингу хмарних середовищ Amazon Web Services (AWS) або Microsoft Azure, а також таких хмарних сервісів, як Microsoft Office 365 і G Suite (рис.2.9). Фізичними та гостьовими операційними системами, включаючи Windows і Linux, також можна керувати за допомогою інтегрованого агента, такого як osquery, або пересилаючи події на датчик USM Anywhere.



Рисунок 2.9 – Приклад роботи датчиків USM Anywhere

Після початкової конфігурації всіх компонентів система буде вести себе як апаратний або віртуалізований аналог. Таке рішення зменшує значущість впливу на бюджет компанії за рахунок розподілу витрат на термін корисного використання. Крім того, це розгортання спрощує розгортання розширень у міру зростання ваших потреб.

Якщо потрібно об'єднати кілька систем в одну, потрібно використовувати USM Central (рис.2.10), що дасть змогу централізовано контролювати розгортання кількох USM Anywhere та USM Appliance з однієї веб-консолі. Його використання заощадить багато ресурсів і часу під час керування кількома середовищами безпеки.

		Медведенко А. В.			KIK.KP.B – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.10 – Приклад роботи USM Central

USM Central використовується для централізації абсолютно всього, від повідомлення до відповіді. Це рішення може бути дуже зручним для компаній, які є постачальниками керованих послуг (MSP) або постачальниками послуг з управління безпекою (MSSP).

2.4. Проект сценаріїв для тестування функціональності підсистеми

Немає гарантії, що при використанні засобів інформаційної безпеки, таких як системи контролю доступу, антивірусу відкрита система буде стійка до несанкціонованих дій зловмисників, які порушують встановлений порядок використання ресурсів. Будь-яке програмне або апаратне забезпечення не ідеальне і, скоріше за все, буде вразливим до цього. Тому під час проектування та експлуатації відкритих ІТ-систем колись, але виникне питання про захист від загроз інформаційної безпеки. Поки що немає точного і єдиного визначення безпеки, але, наприклад, твердження, що безпека визначається як обернене значення вразливості.

Але як же все таки визначити рівень безпеки? Аналіз безпеки з різним рівнем деталізації є одним із елементів аудиту інформаційної безпеки відкритих

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

ІТ-систем. Під цим зазвичай мають на увазі незалежний і документований систематичний процес отримання та оцінки відповідності політиці безпеки за конкретними об'єктивними критеріями даних про поточний стан безпеки, у тому числі про події, що відбуваються в системі, що перевіряється. Його цілеспрямований контроль процесів безпеки при реалізації відкритих систем, основною метою яких є інформаційна підтримка користувачів.

Виходячи з цього, ми можемо вивести перелік професійних якостей, якими повинні володіти спеціалісти, що займаються аналізом безпеки та щоденним адмініструванням. В цей перелік можна віднести такі якості, як здатність оцінювати ризики, знання поширених загроз та вразливостей, критерії та підходи до аналізу безпеки, методи аналізу та спеціальні інструменти та інші.

Потрібно також розглянути таке поняття як моніторинг інформаційної безпеки, або тобто моніторинг пов'язаних подій. Він здійснюється на основі постійного моніторингу зафіксованих подій, пов'язаних з інформаційною безпекою, контролює дотримання основних вимог безпеки та запропонованих нормативних документів. Під час цього процесу, події піддаються ретельному аналізу, і виходячи з отриманих результатів робиться висновок про можливість інциденту безпеки.

Аналітика безпеки — це комбінація програмного забезпечення, алгоритмів та аналітичних процесів, які використовуються для виявлення потенційних загроз для ІТ-систем. Потреба в технологіях аналітики безпеки зростає завдяки швидкому розвитку зловмисного програмного забезпечення та інших кіберподвигів.

На основі звіту Verizon про розслідування зловмисного доступу до даних, кіберзлочинцю потрібні лише хвилини, навіть секунди, щоб вкрати конфіденційні дані. Але ІТ-відділи можуть не виявляти це порушення годинами, іноді навіть днями чи тижнями. У багатьох випадках порушення виявляє стороння сторона, наприклад, правоохоронні органи або клієнт.

Хакери використовують інноваційні тактики, щоб проникнути в ІТ-системи. Вони використовують уразливості в додатках без виправлень, створюють

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

резидентні скрипти, які не можуть бути виявлені сканерами шкідливих програм, і використовують фішинг та інші види соціальної інженерії, щоб уникнути систем ІТ-безпеки.

Звіт Verizon показав, що майже три чверті (73%) кібератак були сторонніми особами, половина з яких були членами організованих злочинних груп, а 12% — ворожими державами або державними установами. Ці творчі підходи ускладнюють для середнього ІТ-відділу виявлення та блокування потенційного зловмисника до того, як він здобуде дані. За словами аналітиків, буде тільки гірше. Дослідники Trellix передбачають, що злочинні організації об'єднаються у більші, сильніші підприємства з використанням шкідливих програм як послуг, які мають ресурси для розробки більш складних експлойтів.

Щоб випередити ці професійні злочинні угруповання, традиційні рішення безпеки — антивірусне програмне забезпечення, брандмауери та системи виявлення та запобігання вторгненням — потребують автоматизації та аналізу в режимі реального часу для виявлення та запобігання кібератакам. Для цього знадобиться аналітика безпеки.

Спеціалізовані інструменти, які при цьому використовуються мають у собі технічні заходи та рішення, інтегровані з регламентом їх експлуатації. Також потрібно відмітити, що велике значення надається комплексу організаційно-правових заходів у цій сфері.

Системи аналізу захищеності (САЗ) і сканери безпеки зазвичай використовуються щоб оцінити рівень реальної захищеності інформаційних ресурсів і перевірити ефективність застосовуваних механізмів захисту (рис.2.11).

САЗ діють на етапі попередження і виявляють та усувають вразливі місця, тим самим усуваючи саму можливість атаки, що зменшує витрати на дію заходів безпеки. Технологія аналізу безпеки є ефективним методом, який дозволяє аналізувати та впроваджувати політику безпеки, перш ніж намагатися її зламати за межами або всередині організації.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

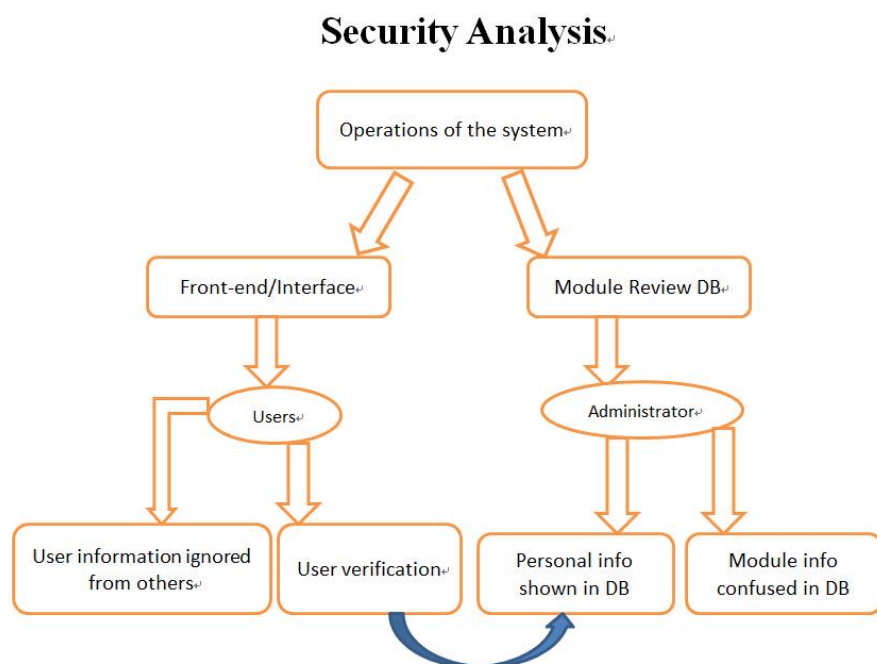


Рисунок 2.11 – Схема роботи систем аналізу захищеності

Сканування необхідне для підтвердження стану безпеки та впровадження відкритої системи превентивного захисту, але для якісного аудиту цього замало, так як сканери зазвичай шукають раніше відомі вразливості, які містяться в їхній базі знань. До того ж при скануванні часто може бути негативний вплив на компоненти системи. Наприклад, значне збільшення трафіку в аналізованому сегменті або навіть вихід з ладу відсканованого вузла чи окремого сервісу. До того ж можна відмітити, що сканером може користуватися і адміністратор мережі, і зловмисник, який намагається визначити чутливі частини системи для подальшого вторгнення.

Тому САЗ можна визначити як систему пошуку вразливостей при проектуванні та експлуатації, що виконує превентивний пошук уразливостей у внутрішніх мережах шляхом аналізу налаштувань своєї АЗ і програмного забезпечення.

САЗ проводить серію тестів на уразливість, подібних до тих, які використовуються зловмисниками під час підготовки та проведення атак. Пошук уразливостей базується на використанні бази даних, яка містить більшість відомих програмних і апаратних вразливостей. Сканування починається з початкової системної інформації, такої як дозволені протоколи та відкриті порти,

версії операційної системи тощо, і може закінчитися спробою імітації вторгнень за допомогою відомих атак. САЗ дає змогу досить швидко ідентифікувати більшість вузлів внутрішньої мережі, які доступні на момент сканування, ідентифікувати всі послуги та протоколи, їх налаштування та можливість несанкціонованого впливу.

В даний час впроваджено велику кількість САЗ. Серед них не так багато, які однозначно визначалися б за типом. Дуже часто це інтегровані реалізації кількох підходів до аналізу безпеки, наприклад, поєднання активного аналізу на рівні мережі з методами пасивного аналізу на системному рівні. Інтеграція часто здійснюється за допомогою централізованих функцій управління.

Найбільшого поширення набули мережеві САЗ, головним чином тому, що вони є універсальними, вони працюють на мережевому рівні і є засобом віддаленого пошуку прогалин у мережевій взаємодії.

Вивчення та широке використання таких мережевих протоколів, як IP, TCP, HTTP, FTP, SMTP та інших, істотно впливає на безпеку внутрішніх мереж. Перевірка його реалізації в конкретному середовищі з використанням мережевих САЗ дозволяє з високим ступенем ефективності оцінити безпеку цього середовища.

Мережні САЗ також аналізують уразливості в системі та програмах, що відповідають за роботу з мережею, наприклад, веб-сервер, FTP та електронна пошта, ІЕ, браузері тощо. На додаток до аналізу програмного забезпечення, деякі комерційно доступні інструменти виконують сканування та сканування обладнання. Як правило, це комутаційне і маршрутизаційне обладнання.

Ще слід звернути увагу, що мережеві САЗ проводять перевірки мережі дистанційно. Вони можуть використовувати різні методи виявлення однієї і тієї ж уразливості та різні облікові записи для підключення до сканованих об'єктів.

Зовні можна аналізувати лише периметр інтрамережі або всю інтранет в цілому: від мережі філій з досить широкими правами доступу, від партнерів - з більш обмеженими правами доступу.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Зсередини можна проаналізувати внутрішню частину інтрамережі з ДМЗ або з інших внутрішніх частин тієї самої інтрамережі. Також можна провести аналіз ДМЗ з внутрішньої мережі.

В даний час є два основних механізми, використовуючи які мережевий сканер перевіряє мережеві вразливості: сканування та зондування.

Сканування та зондування сайту є основними техніками, яку зловмисники використовують, щоб зібрати якомога більше інформації про веб-додаток та допоміжну інфраструктуру. Стандартне сканування сайту складається з кількох кроків. Спочатку зловмисник виявляє операційну систему, встановлену на сервері. Це можна зробити за допомогою таких автоматичних інструментів, як nmap, шляхом визначення типу веб-сервера в HTTP-запиті (наприклад, IIS працює на сайтах під керуванням Windows) або шляхом вгадування за розширеннями файлів. (Зазвичай сайти на базі Windows використовують файли «.htm» і «.jpg», тоді як сайти UNIX використовують файли .html і .jpeg).

Визначення того, який веб-сервер працює на цільовій машині, дуже корисно для зловмисника. Знаючи конкретний тип веб-сервера (і, відповідно, його конфігурацію за замовчуванням), зловмисник може спробувати використати відомі вразливості, отримати доступ до файлів зразків і спробувати облікові записи користувачів за замовчуванням. Існує три поширені способи виявлення веб-сервера: за допомогою автоматичних інструментів, таких як Nikto, шляхом визначення типу веб-сервера в запиті HTTP або шляхом вгадування за суфіксами файлів (сторінки ASP зазвичай вказують на сервер IIS, тоді як сторінки PHP зазвичай вказують сервер Apache).

Додаткову важливу інформацію про інфраструктуру цільового сервера можна зібрати за допомогою методів дослідження, таких як виявлення шляху, обхід каталогу та віддалене виконання (може дозволити зіставити весь сайт і його джерело). Зловмисник може заповнити базу знань інфраструктури, визначивши типи серверів баз даних, типи інфраструктури вмісту (WebSphere, BroadVision і Vignette) тощо.

		Медведевко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Після того, як зловмисник проаналізує інфраструктуру, можна просканувати всю програму. Сканування програми надає карту всього сайту, включаючи: усі сторінки, параметри, які використовуються динамічними сторінками, файли cookie, які використовує сайт, і потік транзакцій. Ця інформація приводить зловмисника до розуміння аутентифікації, авторизації, логіки та механізмів транзакцій програми. Ця інформація є основою для стратегії атаки на цільовий сайт.

Найшвидшим і найпростішим методом перевірки наявності вразливості є сканування. На основі непрямих причин сканер намагається визначити наявність. Також цей метод ще називається «логічним міркуванням». З цією метою дослідження Cisco визначає відкриті порти, а також збирає та аналізує банери доступних служб, які знайшлися під час сканування кожного порту. Кожен отриманий заголовок порівнюється з базою даних, щоб визначити мережеві пристрої, операційні системи та потенційні вразливості безпеки. На основі цього виконується висновок чи наявна, чи відсутня уразливість безпеки. Сканування не заважає службам чи вузлам мережі.

Але на жаль тут присутній ряд серйозних недоліків. По-перше, ефективність перевірки заголовків достатньо мала. По-друге, часто версія, зазначена в заголовку відповіді на запит, не завжди свідчить про наявність невирішених програмних уразливостей. Нарешті, усунення вразливості в одному випуску програмного забезпечення не означає, що вразливість буде відсутня в наступних випусках.

Другий тип аналізу називається зондування. Це аналіз, при якому перевіряється, чи присутня вразливість в аналізованому об'єкті. Цей процес використовує інформацію, яку отримали в результаті сканування, для детального аналізу кожного мережевого пристрою. Він ніяким чином не перевіряє версію програмного забезпечення в заголовках, а порівнює «відбиток пальця» його фрагмента з «формою» відомої уразливості. Можна сказати, що це подібно до антивірусних програм, які порівнюють фрагменти відсканованого програмного забезпечення з вірусними сигнатурами у своїй базі даних. З цією метою система

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

піддається ключовим впливам, які використовують тестування на вразливість із чітким посиленням на систему та проаналізованим зворотним зв'язком. Також цей процес має ще дві назви: «етичний злом» або «тестування на проникнення». Якщо сканер відповідає на командний рядок, у системі є вразливість. Метою тесту є пошук шляхів отримання доступу до системи за допомогою інструментів і прийомів, які використовує зловмисник. Іншими словами, тест на проникнення має на меті оцінити, наскільки легко тестувальник може отримати несанкціонований доступ до інформації компанії та мережевих ресурсів.

Зондування рекомендується для особливо критичних систем. Крім того, тестування найкраще проводити як зовнішньо, так і внутрішньо.

Буває що при зондуванні випадково можна виявити й інші вразливості, які неможливо виявити пасивними методами. Тестова робота також може мати другорядні цілі, такі як тестування процедури ідентифікації інциденту та реагування, перевірка поінформованості користувачів, відповідність політикам безпеки тощо.

Цей метод повільніший і більш трудомісткий, ніж пасивне сканування, але майже завжди точніший і надійніший. Зондування також може створити велике навантаження на мережу. Іншим недоліком є те, що перевірка деяких вразливостей, які викликають реальні атаки, призводить до збою служби або комп'ютера. У цьому проекті, через недостатню кількість ресурсів, тестування функціональності мережі доведеться здійснювати шляхом легшої реалізації. Таким чином, для перевірки продуктивності мережі будуть використовуватися 3 віртуальні машини на базі Windows XP і Windows 7, по одній у кожному офісі зі спрощеною топологією. З їх допомогою стане можливою як наявність відповідних мереж, так і наявність візуальної складової веб-сервера. До того ж, у першому офісі буде використовуватися рішення AlienVault USM All-in-One, яке дозволить побачити вплив атаки на мережу на візуальному дисплеї (графіки, графіки тощо).

Як САЗ буде використовуватися віртуальна машина на базі ОС Kali Linux. Ця операційна система була розроблена спеціально для атаки як на мережеве

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

обладнання, так і на кінцеві пристрої. Ще одна перевага Kali Linux для цих дій полягає в тому, що більшість популярних додатків зловмисників вже встановлено в операційній системі за замовчуванням [14].

2.5. Розрахунок кількості апаратних ресурсів, використаних для побудови мережі

Через обмежену кількість апаратних ресурсів, потрібно спочатку проаналізувати мережу та визначити, чи є можливість виконувати ці дії на наявному обладнанні.

Завантаження ЦП відбувається лише під час навантаження, тому можна припустити, що цей ресурс актуальний лише під час завантаження симулятора та обладнання в ньому, оскільки це найбільш ресурсозатратний процес. Тому обсяг оперативної пам'яті, необхідний для модуляції, має вирішальне значення для обчислень.

Перш за все, необхідно розрахувати обсяг оперативної пам'яті, яку буде використовувати віртуальна машина. Переглянувши технічні характеристики потрібного обладнання, можна побачити наступне:

Cisco ASA v.9.12.2.9 – 2048 Мб;

Cisco c7200 – 512 Мб;

Cisco c2960 – 160 Мб.

Враховуючи ці значення і знаючи кількість використовуваних пристроїв, можна розрахувати максимальний обсяг оперативної пам'яті, який вони споживатимуть:

$$\sum_{k=1}^n ASA_k \times R_{ASA} + R_{RAM} \times R_{c7200} + S_k \times R_{c2960}, \# \quad (21)$$

де ASA_k – кількість пристроїв Cisco ASA;

ASA_{RAM} – кількість оперативної пам'яті для одного пристроя Cisco ASA;

R_k – кількість пристроїв Cisco c7200;

R_{RAM} – кількість оперативної пам'яті для одного пристроя Cisco c7200;

S_k – кількість пристроїв Cisco c2960;

		Медведев А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

S_{RAM} – кількість оперативної пам'яті для одного пристрою Cisco c2960.

Це означає, що максимальний обсяг оперативної пам'яті, який можуть споживати мережеві пристрої, становить 9184 МБ. Однак варто відзначити, що великого навантаження на змодельовану мережу не буде, тому можна зменшити розраховану суму приблизно вдвічі - до 4,5 ГБ. Єдине правило якого слід буде дотримуватися, намагатися не завантажувати всі пристрої одночасно. Тому потрібно все проводити поетапно – після завантаження пристрою дочекатися зменшення навантаження ресурсу, а потім завантажити наступний.

Також розраховується загальне використання оперативної пам'яті комп'ютера. Симулятор віртуальної машини використовуватиме приблизно 4,5 ГБ, також 2 ГБ потрібно для роботи Windows [10].

Звертаючись до документації AlienVault можна помітити, що мінімальні системні вимоги для USM All-in-one вимагають 16 ГБ оперативної пам'яті. Очевидно, що цей обсяг не може бути забезпечений доступними ресурсами, тому ми перевіримо роботу цієї системи на максимальному обсязі оперативної пам'яті, який можна надати для решти.

Також потрібно визначити обсяг оперативної пам'яті, який споживають віртуальні машини:

Windows XP - не менше 128 МБ [12];

дві 32-розрядні Windows 7 - не менше 1 Гб кожна [11];

Kali Linux - не менше 2 Гб;

три 32-розрядні версії Debian 8.3 – щонайменше 135 МБ кожна.

Для кращої продуктивності Windows XP і Debian 8.3 ми надамо їм 256 МБ кожному. Тому обсяг оперативної пам'яті, що споживається всіма кінцевими віртуальними машинами, розраховується наступним чином:

$$\Sigma = \quad + 7 \times 7 \quad + \quad + \quad \times \quad , \quad (22)$$

де XPRAM – обсяг оперативної пам'яті для Windows XP;

W7k - кількість віртуальних машин під керуванням Windows 7;

W7RAM - обсяг оперативної пам'яті для Windows 7;

KLRAM - обсяг оперативної пам'яті для Kali Linux;

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

LDk - кількість віртуальних машин з Linux Debian 8.3;

LDRAM - обсяг оперативної пам'яті для Linux Debian 8.3.

Таким чином, кінцеві віртуальні машини потребують 5 ГБ оперативної пам'яті. Також потрібно залишити невелику кількість пам'яті у резерві для операційної системи, оскільки існує велика ймовірність того, що фонові процеси в якийсь момент можуть трохи збільшити споживання. Це призведе до виснаження всіх ресурсів і аварійного відключення операційної системи.

Висновки до розділу 2

Описано організаційну мережу, яка складається з шести офісів. Дослідження трьома офісами є виправданими.

Описано пристрої, на яких базується мережа. Описано можливості обладнання, яке буде використовуватися для виконання завдання.

Описано обрану підсистему запису, аналізу та візуалізації подій безпеки – AlienVault USM All-in-One. Ще коротко описана вся продуктова лінійка компанії, яка може бути використана для розширення мережі.

Були проаналізовані різні САЗ. Віртуальна машина на базі Kali Linux була обрана в якості САЗ. Розроблено сценарій тестування працездатності підсистеми.

Розрахунки обсягу використання апаратних ресурсів для моделювання мережі. Тут описуються особливості пристроїв, які можуть знадобитися для реалізації цього проекту на реальному обладнанні.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ РЕЄСТРАЦІЇ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ПОДІЙ БЕЗПЕКИ

3.1. Базове введення в експлуатацію мережевого обладнання

У цьому розділі описано основні налаштування спрощених мережевих пристроїв, які налаштовані на корпоративному обладнанні. Ці конфігурації забезпечують повну продуктивність мережі та відповідають політикам безпеки організації. Надалі буде описано основні етапи налагодження.

Спочатку потрібно налагодити адресацію мережевих пристроїв, використовуючи статичну адресацію та адресацію за допомогою DHCP.

На комутаторах потрібно внутрішню мережу розділити на підмережі. Це дозволить диверсифікувати трафік різних підрозділів підприємства. Завдяки цьому можливо буде підвищити рівень безпеки мережі всередині кожного офісу. Для цього були налагоджені мережі VLAN.

Статичні маршрути або протоколи динамічної маршрутизації були налаштовані, щоб дозволити різним мережам взаємодіяти: статичні маршрути були налаштовані за замовчуванням між мережевими пристроями та Інтернетом, а BGP Border Dynamic Routing Protocol був налаштований для Інтернет-маршрутизації.

Додатково потрібно встановити захист консолі та віддаленого підключення до мережевого обладнання, що знизить ризик того, що зловмисник змінить конфігурацію.

Для того, щоб відбувався обмін трафіку із глобальною мережею, на додаток до «шлюзу останньої надії», пристрої маршрутизатора були налаштовані на передачу мережевих адрес NAT. Трансляція виконує дві важливі функції:

1. Забезпечити взаємодію внутрішньої та зовнішньої підмереж.
2. «Приховує» внутрішню мережу ззовні.

Щоб реалізувати частину політики безпеки ДМЗ, слід адаптувати мережеві об'єкти на ME, додавши іншу статичну трансляцію адреси. У цей момент зовнішня адреса перекладається в адресу сервера, розташованого в офісі. Це

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

потрібно для того, щоб Інтернет мав доступ до внутрішніх серверів, які містять дані, які повинні бути доступні у всесвітній мережі. Однак, щоб сервер був у безпеці, передача повинна відбуватися лише на необхідні порти. Цей параметр називається переадресацією портів.

Для безпеки також створено різні списки доступу. Це правила, за допомогою яких відбувається фільтрування мережевого трафіку, яке дозволяє або забороняє проходження певного трафіку. Для ізоляції небезпечного трафіку від внутрішньої мережі налаштовано фільтрацію на інтерфейсах, який знаходиться на сервері та на зовнішньому.

Приватні віртуальні мережі - VPN - призначені для взаємодії в офісі. Завдяки ним можна безпечно обмінюватися усією потрібною інформацією між офісами. У цій роботі використовувався найпопулярніший тип VPN - IPSec Site-to-Site VPN. Налагодження відбувається в два етапи: створення тунелю і налагодження передачі зашифрованого трафіку [5].

Щоб створити тунель потрібно спочатку створити політику і ключ аутентифікації.

Надалі встановлюються правила шифрування трафіку, що проходить через створені тунелі, яку було створено раніше і створюється криптографічна карта, яка «збирає» всі задані налаштування разом. Щоб використовувати криптографічну карту, вам потрібно визначити, з яким інтерфейсом діяти.

Налагодження подій мережевого пристрою також є обов'язковим. Для цього потрібно ввімкнути журналювання та налаштувати сервер збору.

3.2. Налаштування підсистем реєстрації, аналізу та візуалізації подій безпеки

Після налаштування мережі для тестування потрібно перейти до конфігурації підсистеми для реєстрації, аналізу та візуалізації подій безпеки. Перед цим потрібно було загрузити образ цього продукту.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Після цього була утворена віртуальна машина з усіма потрібними параметрами, щоб інтегрувати підсистему у мережу

Після того як мова інсталятора обрана, пароль адміністратора створений, а мережева карта налаштована, потрібно установити операційну систему та програмні додатки.

Після того, як завершиться інсталяція, з'являється можливість перейти до налаштувань сервера цієї підсистеми.

Перелік усіх налаштування є досить невеликим, але включає у себе все необхідне. Під час налаштування найбільш цікавими є такі пункти: «Властивості системи» та «Конфігурація компонента датчика».

У вікні «Властивості системи» присутня можливість змінювати такі параметри як властивості мережевого адаптера, назву пристрою, параметри електронної пошти та системний пароль.

Але зараз цей пункт не є дуже важливим, так як все що потрібно було налаштовано ще під час встановлення системи

Що стосується «Конфігурації компонентів датчика», то тут є можливість налаштувати скановані мережі, роз'єми джерел даних та моніторинг.

Додатково ще можна змінити інтерфейс, який буде використовуватися для сканування трафіку, але виходячи з того, що у цьому проєкті він тільки один, то і змінювати нічого не потрібно. Оскільки рішення All-in-One інтегроване, тобто всі компоненти системи знаходяться на одному сервері, IP-адресу сервера, який оброблятиме інформацію, не слід змінювати.

Потім того, як попередні пункти будуть виконані, можна перейти до налаштувань, які наявні у веб-інтерфейсі. Для цього потрібно використати вже іншу віртуальну машину, яка знаходиться в тому ж офісі. Після введення в адресний рядок IP-адреси інтерфейсу віртуальної машини, потрапимо на сторінку помилки, яка виникає у Internet Explorer і Google Chrome через те, що це рішення використовує самопідписаний сертифікат.

Якщо все ж таки перейти далі, то з'явиться сторінка профілю реєстрації адміністратора підсистеми. Після створення аккаунту можливо буде продовжити

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

працювати далі і використовувати саме цей аккаунт для подальшої авторизації у веб-інтерфейсі.

Після того, як увійти в обліковий запис з цими даними, можна буде побачити сторінку з налаштуваннями сервера

Спочатку, буде запропоновано конфігурацію мережевих інтерфейсів. Але оскільки використовується рішення «All-in-One», ця функція буде вимкнена

На другій сторінці конфігурації потрібно налаштувати пристрої, які будуть перевірятися (сканування трафіку пристрою, збір журналів, сканування конфігурації пристрою на випадок уразливості). Такі пристрої можна додавати вручну використовуючи сканування мережі та за допомогою табличного файлу даних (файл csv).

Після цього потрібно буде ввести логіни та паролі для розпізнаних у мережі пристроїв. Це в першу чергу потрібно для того, щоб програмне забезпечення могло читати та аналізувати конфігурації пристрою.

Далі потрібно налаштувати колекції журналів для аналізу безпеки. Для цього потрібно обрати виробника обладнання, його модель та версію.

Після того, як ці дані будуть налаштовані, потрібно натиснути на кнопку «Увімкнути»

Зрештою, пропонується приєднатися до AlienVault - Open Threat Exchange (OTX), який підтримуватиме безпеку цієї мережі в актуальному стані, оскільки він інформуватиме про останні новини загрози та допомагатиме унакати їх.

Тепер залишилося лише налаштувати окремі мережі для сканування наявності вразливостей і активно сканувати мережу на предмет додавання нових пристроїв.

3.3. Тестування підсистеми реєстрації, аналізу та візуалізації подій безпеки

Для того щоб перевірити налаштування з точки зору відповідності можливостям виробника підсистеми, потрібно буде випробувати підсистеми реєстрації, аналізу та візуалізації подій безпеки.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Щоб це зробити, перш за все потрібно переконатися, що підсистема встановила з'єднання з пристроями.

Якщо для кожного пристрою відображається кількість подій, це означає, що з'єднання було встановлено коректно.

Для початку має сенс переглянути доступність ДМЗ з імітованої мережі Інтернет. Таким чином, якщо стартова сторінка веб-сервера, розташованого в ДМЗ, відкривається за зовнішньою адресою граничного обладнання маршрутизації, а за допомогою внутрішньої IP-адреси – ні, то NAT працює належним чином.

Зараз потрібно перевірити віддалений доступ до обладнання. Краще всього використати програму Putty, яку потрібно інстальувати на віртуальну машину. Перед тим, як виконувати будь-які дії з ним, потрібно ввести пароль та увійти.

Надалі тестування буде проводитися шляхом моделювання зовнішніх атак. Це дозволяє побачити, як підсистема реагує на спроби вторгнення або атаки збою. Як вже було сказано раніше, всі атаки будуть проводитися за допомогою Kali Linux.

Спочатку спробуємо атакувати з використанням програми Cisco Audit Tool або CAT.

Ця атака використовується для брутфорса пароля, коли режим aaa вимкнено, SNMP community-рядків, а також для перевірки історії IOS із можливістю помилок.

Тепер спробуємо використати Cisco Global Exploiter або CGE, який використовує відомі вразливості

Ще одним багатофункціональним сканером уразливостей апаратного забезпечення Cisco є cisco-torch. Цей сканер має можливість сканувати декілька IP-адрес одночасно, завантажуючи їх із текстового файлу.

І під кінець також проведемо атаку за допомогою програми cory-router-config.pl, який завантажуватиме поточну конфігурацію маршрутизатора Cisco з відомим community-рядком на сервер TFTP, після чого з'являється можливість

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

змінити конфігурацію та перезавантажити її на сервер за допомогою програми merge-copy-config.pl.

Після проведення цих атак, потрібно переглянути чи є зміни у інформації про пристрої в підсистемі для запису, аналізу та візуалізації подій безпеки.

Справді, кількість вразливостей і повідомлень змінилася, а у аналізаторі подій можна помітити атаки, які було зафіксовано.

Також з кожною проблемою автоматично створюються записи, які прийнято називати тікет (від англ. Ticket-білет). Це дозволяє керувати кроками усунення несправностей незалежно від кількості адміністраторів. Кожен такий запис має пріоритет, що дозволяє судити про серйозність проблеми, не аналізуючи всю інформацію.

3.4. Аналіз результатів випробувань

Якщо аналізувати все вищесказане, можна прийти до висновка, що інтеграція підсистеми запису, аналізу та візуалізації подій безпеки пройшла успішно.

Така система дає можливість реєструвати та аналізувати події у реальному часі. При чому така система буде відображати статистику у візуальному та текстовому вигляді. Ця підсистема має досить просту конфігурацію, яка дозволяє інтегрувати її з реальним обладнанням за відносно короткий проміжок часу. Також потрібно відмітити ще один не менш важливий пункт – можливість підключення до спільноти професіоналів з усього світу, що допоможе розвинути безпеку мережі.

Але є і не дуже приємний момент, такий як кількість необхідних для нормальної роботи ресурсів. Але в порівнянні з аналогами ці дані приблизно рівні. Операційна система відіграє тут важливу роль, оскільки різні операційні системи споживають різну кількість ресурсів. Цю ситуацію рятує AlienVault USM, оскільки він є досить економічним, черех те що базується на Debian Linux.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

У рамках цього проекту підсистема реєстрації подій безпеки, аналізу та візуалізації AlienVault USM All-in-One була встановлена та працювала на обмеженій кількості ресурсів, навіть менше мінімального. Як можна здогадатися, це не найкращим чином впливає на продуктивність. Апаратних ресурсів у такій ситуації критично мало, оскільки підсистема веде себе досить нестабільно, а завантаження інформації може займати до кількох хвилин.

Але не дивлячись на такі наче б то серйозні недоліки, переваги цієї системи все одно переважають недоліки. Цей продукт містить повну документацію, яка до того ж знаходиться на офіційному сайті, а це набагато полугтуше використання. Також досить простою є функція масштабування, яка дозволяє легко збільшити кількість мережевих пристроїв або навіть об'єднати дві або більше схожих підсистем. Також потрібно відмітити, що базова версія даного продукту є абсолютно безкоштовною.

Крім підсистеми реєстрації, аналізу та візуалізації подій безпеки, варто згадати підсистему захисту периметра, який також відповідає всім вимогам політики інформаційної безпеки, про що свідчать результати атак у попередньому параграфі. У майбутньому ця політика може бути оновлена, щоб відповідати більш конкретним потребам кожного офісу.

За результатами масштабних атак можна зробити висновок, що в результаті подібних досліджень усі три опитані офісні мережі виявилися однаково захищеними. Для спрощення налаштування сервера використовувався небезпечний протокол HTTP, так як цей проект безпосередньо не стосувалося безпеки веб-сервера, тому він є досить вразливим.

Усі інші атаки не принесли ніяких результатів. Це означає, що дана ІТ-система підприємства має достатній захист від шкідливих дій ззовні, а отже, буде мати високу стабільність.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновок до розділу 3

У цьому розділі було описано статичну та динамічну адресацію, статичну та BGP-маршрутизацію, транкінгові канали. Було увімкнено реєстрацію подій та налаштовано її. На мережевих пристроях налаштовано віддалений доступ. Також було створено трансляцію внутрішніх адрес, віртуальні приватні мережі між офісами та списки доступу до мережі.

Встановлено підсистему реєстрації, аналізу та візуалізації подій безпеки, виконано базову конфігурацію серверної частини під конкретний проект. Зареєстровано обліковий запис адміністратора веб-інтерфейсу. Налаштована поведінка підсистеми, налаштовані функції сканування мережі.

Перевірено функціонування мережі: обмін трафіком у підмережах, обмін трафіком із глобальною мережею. Атаки на підмережу з метою перевірки коректності та стабільності підсистеми безпеки також були поширеними. Виявлено реакцію на них підсистеми реєстрації, аналізу та візуалізації подій безпеки.

Проаналізовано результати дослідження та зроблено висновки щодо модернізації та можливостей покращення роботи ІТ-системи компанії.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

ВИСНОВКИ

Отже, в результаті аналізу було визначено основні принципи захисту внутрішніх мереж та обрано захист периметра на основі МЕ.

Розглянуто 4 існуючі види МЕ та проаналізовано всі їх плюси та мінуси. Дослідження цих типів МЕ показали, що пристрої, що використовуються в цій топології, є екрануючими маршрутизаторами та ІЕ експертного рівня.

Проведено аналіз мережевого обладнання від Cisco Corporation. Аналіз проводився на основі дослідження компанії Gartner.

Розглянуто концепцію інформаційної безпеки та системи управління подіями. Проаналізовано найпопулярніші рішення на ринку та вибрана система SIEM, яка буде використовуватися в цьому проекті.

Описано організаційну мережу, яка складається з шести офісів. Дослідження трьома офісами є виправданими.

Описано пристрої, на яких базується мережа. Описано можливості обладнання, яке буде використовуватися для виконання завдання.

Описано обрану підсистему запису, аналізу та візуалізації подій безпеки – AlienVault USM All-in-One. Ще коротко описана вся продуктова лінійка компанії, яка може бути використана для розширення мережі.

Були проаналізовані різні САЗ. Віртуальна машина на базі Kali Linux була обрана в якості САЗ. Розроблено сценарій тестування працездатності підсистеми.

Проведено розрахунки обсягу використання апаратних ресурсів для моделювання мережі та описано особливості пристроїв, які можуть знадобитися для реалізації цього проекту на реальному обладнанні.

Було описано статичну та динамічну адресацію, статичну та BGP-маршрутизацію, транкінгові канали. Було увімкнено реєстрацію подій та налаштовано її. На мережевих пристроях налаштовано віддалений доступ. Також було створено трансляцію внутрішніх адрес, віртуальні приватні мережі між офісами та списки доступу до мережі.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Встановлено підсистему реєстрації, аналізу та візуалізації подій безпеки, виконано базову конфігурацію серверної частини під конкретний проект. Зареєстровано обліковий запис адміністратора веб-інтерфейсу. Налаштована поведінка підсистеми, налаштовані функції сканування мережі.

Перевірено функціонування мережі: обмін трафіком у підмережах, обмін трафіком із глобальною мережею. Атаки на підмережу з метою перевірки коректності та стабільності підсистеми безпеки також були поширеними. Виявлено реакцію на них підсистеми реєстрації, аналізу та візуалізації подій безпеки.

Проаналізовано результати дослідження та зроблено висновки щодо модернізації та можливостей покращення роботи ІТ-системи компанії.

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco ASA 5500-X з FirePOWER Services [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html#~models>
2. Cisco ASA. Управління вхідним та вихідним трафіком за допомогою списків ACL [Електронний ресурс] // Скарбничка знань. – 2021. – Режим доступу до ресурсу: <http://teacherbox.ru/kompseti/cisco-asa-upravlenie-vhodyashhim-i-ishodyashhim-trafikom-s-pomoshhyu-spiskov-acl/.html>
3. Cisco ASA/ Джазіб Фрахім, Омар Сантос, Ендрю Осіпов, 2014. - 1248 с. – ("Cisco Press").
4. Cisco Catalyst 2960-X - можливості та переваги [Електронний ресурс] - Режим доступу до ресурсу: http://stornet.ru/articles/cisco_catalyst_2960x_vozmojnosti_i_preimushhestva/
5. IPsec VPN Повний посібник/ Герардус Блокдик, 2019. - 308 с. – ("5STARCooks").
6. IPsec Ясний і стислий довідник/ Герардус Блокдик, 2018. - 224 с. – ("5STARCooks").
7. Апаратні міжмережеві екрани [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: http://www.infobezpeka.com/products/apatnye/Cisco_ASA_5500_Series/
8. Безпека брандмауера маршрутизатора Cisco/ Річард А. Діл, 2004. - 870 с. – ("Cisco Systems").
9. Безпека в обчислювальній техніці/ Чарльз Пфлігер, Шарі Пфлігер, Джонатан Маргуліс., 2015. - 944 с. – ("Пірсон").
10. Вимоги до windows 10 [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715>
11. Вимоги до windows 7 [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://support.microsoft.com/en-us/windows/windows-7-system-requirements-df0900f2-3513-a851-13e7-0d50bc24e15f>

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

12. Вимоги до windows xp [Електронний ресурс]. – Режим доступу до ресурсу:

<https://kb.iu.edu/d/akma#:~:text=Requirements,poorly%20or%20not%20at%20all>.

13.Захист від загроз Cisco Firepower/ Назмул Раджіб, 2017. - 800 с. – ("Cisco Press").

14. Злом за допомогою Kali Linux: покроковий посібник/ Рамон Настасе., 2018. - 129 с. – (Незалежне видавництво).

15.Кібероперації/ Майк О'Лірі, 2019. - 1165 с. – ("Apress").

16. Коммутатор Cisco Catalyst 2960-X [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: <https://lantorg.com/products/kommutator-cisco-catalyst-2960-x-ws-c2960x-48lps-l>

17.Короткий огляд найкращих інструментів SIEM [Електронний ресурс] // Tek-Tools. – 2020. – Режим доступу до ресурсу: <https://www.tek-tools.com/security/top-siem-tools>.

18. Короткий посібник користувача AlienVault USM Anywhere [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: <https://desk.cyflare.cloud/portal/en/kb/articles/alienvault-usm-anywhere-customer-quick-start-guide>

19. Маршрутизатор Cisco 7201 [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: <https://stack-systems.com.ua/marshrutizator-cisco-7201>

20. Мережі Cisco/ Кріс Картерн, Вільям Вілсон, Ноель Рівера, 2021. - 1104 с. – ("Apress").

21. Мережі нульової довіри/ Еван Гілман, Даг Барт, 2017. - 240 с. – ("O'Reilly Media").

22. Міжмережеві екрани [Електронний ресурс] – Режим доступу до ресурсу: https://ua.kursoviks.com.ua/metodychni_vkazivky/article_post/830-tema-mizhmerezhevi-yekrani-navchalniy-posibnik-internet-dlya-koristuvacha-chastina-2-nudpsu

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

23. Мілінський М. ACL: списки контролю доступу в Cisco IOS [Електронний ресурс] / Микола Мілінський. – 2011. – Режим доступу до ресурсу: <https://habr.com/en/post/121806/?mobile=no>.

24. Налаштвання тунель Site-to-Site IPSec IKEv1 між ASA і маршрутизатором Cisco IOS [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html#anc14>

25. Налаштування тунелю Site-to-Site IPSec IKEv1 між ASA і маршрутизатором Cisco IOS [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html#anc14>

26. Основи організації мереж Cisco/Віто Амато., 2004. - 464 с. – ("Вільямс").

27. Порівняння продуктів AlienVault [Електронний ресурс] // AT&T Cybersecurity – Режим доступу до ресурсу: <https://cybersecurity.att.com/products/ossim/compare>.

28. Приклад конфігурації системного журналу ASA [Електронний ресурс] // Cisco. – 2014. – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ua/support/docs/security/pix-500-series-security-appliances/63884-config-asa-00.html.

29. Приклад конфігурації системного журналу ASA [Електронний ресурс] // Cisco. – 2014. – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/security/pix-500-series-security-appliances/63884-config-asa-00.html

30. Режим failover на Cisco ASA [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: <https://deltaconfig.ru/failover-on-cisco-asa/>

31. Системні вимоги Kali Linux [Електронний ресурс] // Системні вимоги. – 2017. – Режим доступу до ресурсу: <https://systemrequirements.ru/kali-linux-sistemnyie-trebovaniya/>

		Медведев А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Медведевко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики маршрутизатора Cisco 7200

Процесор	1.67-GHz Motorola Freescale 7448 processor
Продуктивність	2000000 pps або більше
Порти	4 Gigabit Ethernet, підтримка IEEE 802.1Q
Gigabit Ethernet оптика	SFP Short wave (SX) Long wave/long haul (LX/LH) Extended wavelength (ZX) RJ-45 мідний SFP
DRAM	1 GB за замовчуванням (2 GB максимум)
Compact Flash	64 Мб за замовчуванням (256 Мб максимум)
Cisco IOS Software Release	12.2(31)SB4, 12.4XD7 та 12.4PI6
Вбудовані інтерфейси	Ні
Пропускна спроможність шини	1,2 Гбіт/с
Живлення	AC/DC. 2 слоти. Можливість встановлення запасного БП
Робоча температура	0–40°C
Температура зберігання	-20 до 65°C
Робоча вологість	10-90% (без конденсації)
Висота	13,34 см
Ширина	42,67 см
Глибина	43,18 см

Технічні характеристики міжмережного екрана Cisco ASA5500

Види захисту мережі	Від зовнішніх загроз (Internet)
Технологія доступу	Ethernet
Тип інтерфейсів	10/100Base-TX (100 Мбіт/с)
Модулі	1 шт
Power over Ethernet (PoE)	Є
Кількість PoE портів	2 шт
Слоти розширення	SSC
Порти USB 2.0	3 шт
Протоколи Ethernet	IEEE 802.3, IEEE 802.3u
Пропускна спроможність міжмережевого екрану	150 Мбіт/с
Продуктивність маршрутизації	75 mpps
Підтримка Auto-MDI/MDI-X	Є
Максимальна кількість одночасних сесій	25000
Пропускна спроможність 3DES/AES VPN	100
Користувачі IPsec VPN	25
Користувачі SSL VPN	2
Одночасні сесії	10000
Віртуальні інтерфейси (VLANs)	20
HTTP	Є
SMTP	Є
FTP	Є
DNS	Є
VPN	Є
UDP	Є

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єм системної флеш-пам'яті	128 МБ
Пам'ять	512 МБ
Вхідна напруга	220 В
Споживана потужність	96 Вт
Робоча температура	від 0°C до +40°C
Вологість при експлуатації	від 5% до 95%, без конденсації
Габарити	200.4 x 44.5 x 174.5 мм

Додаток В

Технічні характеристики комутатора Cisco c2960

Кількість LAN портів	24 x RJ-45
Швидкість LAN портів (Мбіт/Гбіт)	10/100/1000 Мбіт
Кількість Uplink портів	4
Швидкість Uplink портів (Мбіт/Гбіт)	1 Гбіт
Тип uplink портів	4 x SFP
Кількість SFP портів	4
Кількість USB-портів	2
Консольний порт	Так
Порт MGMT	Так
Наявність портів XFP	Ні
Наявність портів Xenpak	Ні
Наявність портів X2	Ні
Підтримка PoE	Так
Підтримка PoE+	Так
Підтримка UPoE	Ні
Потужність PoE на порт (Вт) 24 x 15,4 Вт	Потужність PoE+ на порт (Вт) 12 x 30 Вт
Внутрішня пропускна здатність	216 Гбіт/сек
Продуктивність маршрутизації	71,4 Мбіт/сек

		Медведев А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єм оперативної пам'яті	512 Мб
Об'єм Flash пам'яті	128 Мб
Розмір таблиці MAC-адрес	16000
Стекування	Так
Максимальна кількість комутаторів у стеку	8
Web-інтерфейс	Так
Telnet	Так
Міжмережевий екран (Firewall)	Так
DHCP-клієнт	Так
Підтримка IGMP (Multicast)	Так
Підтримка SNMP	Так
Підтримка MGMT	Так
Підтримка Bluetooth	Так
Діапазон робочих температур (°C)	-5 ~ 45
Діапазон температури зберігання (°C)	-25 ~ 70
Вологість при експлуатації (%)	10 ~ 95

Додаток Г

Мінімальні системні вимоги Windows 10, 7, XP

	Windows 10	Windows 7	Windows XP
Процесор	не менше 1 ГГц	не менше 1 ГГц	не менше 233 МГц
Оперативна пам'ять	мінімум 2 ГБ ОЗУ для 64-розрядного та 1 ГБ ОЗУ для 32-	мінімум 2 ГБ ОЗУ для 64-розрядного та 1 ГБ ОЗУ для 32-	мінімум 64 МБ ОЗУ

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

	розрядного комп'ютера	розрядного комп'ютера	
Накопичувач	20 ГБ вільного простору для 64-розрядних та 16 ГБ вільного простору для 32-розрядних систем	20 ГБ вільного простору для 64- розрядних та 16 ГБ вільного простору для 32- розрядних систем	1.5 ГБ вільного простору
Роздільна здатність дисплея	мінімум 800 x 600 пікселів	мінімум 800 x 600 пікселів	мінімум 800 x 600 пікселів
Графіка	Microsoft DirectX 9 та вище	Microsoft DirectX 9 та вище	

Додаток Д

Рекомендовані системні вимоги Kali Linux

Kali Linux
32- або 64-розрядний ЦП (одноядерний) з тактовою частотою 2 ГГц або краще
2 ГБ оперативної пам'яті
20 ГБ дискового простору
Відеокарта та монітор високої чіткості
Широкополосне підключення до Інтернету

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

Мінімальні системні вимоги AlienVault USM

Тип процесора	Intel Xeon E5620 і вище
Тип оперативної пам'яті	DDR3 1333 МГц
Тип диска	SAS 10000 RPM (204 МБ/с)
Продуктивність пам'яті	3310,32 МБ/с
Продуктивність диска (випадкове читання/запис)	15,97 МБ/с (120 МБ/с)
Всього ядер	8
RAM (GB)	16
Пам'ять (ТБ)	1

		Медведенко А. В.			КІК.КР.Б – 125 – 13 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76