Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
*Факультет комп'ютерно-інформаційних систем і програмної інженерії*
(назва факультету )
*Кафедра кібербезпеки*
(повна назва кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *«Аналіз логів з використанням фаєрволу FortiGate»*

Виконав: студент (ка)
Спеціальності:
*125 «Кібербезпека»*
(шифр і назва напряму підготовки, спеціальності)
*Маланчук М.І.*
підпис (прізвище та ініціали)

Керівник *Козак Р.О.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«19» __червня__ 2023 р.

# ЗАВДАННЯ
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)
за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)
Студенту Маланчуку Максиму Ігоровичу
(прізвище, ім'я, по батькові)
1. Тема роботи Аналіз логів з використанням фаєрволу FortiGate

Керівник роботи Козак Руслан Орестович, д.т.н., доцент.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від «03» 04 2023 року № 4/7-349
2. Термін подання студентом завершеної роботи 17.06.2023
3. Вихідні дані до роботи Фаєрвол FortiGate, персональний комп'ютер з ОС Windows, ELK Stack

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз вимог до системи захисту інформації
Використання фаєрволів для організації системи захисту
Розробка узагальненої структури системи захисту інформації в комп'ютерній мережі
Виявлення та нейтралізація загроз фаєрволами
Необхідність використання фаєрволів, огляд фаєрволів
Перегляд інструментів для аналізу логів фаєрволу FortiGate
Практичні результати аналізу логів
Безпека життєдіяльності, основи охорони праці
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Безпека життєдіяльності, основи охорони праці | Пилипець.М.І., проф. кафедри МТ | | |

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Ознайомлення з завданням до кваліфікаційної роботи | 16.01 – 19.01 | *Виконано* |
| 2. | Підбір джерел про аналіз логів за допомогою фаєрволів | 20.01 – 05.02 | *Виконано* |
| 3. | Опрацювання джерел в галузі дослідження | 06.02 – 20.03 | *Виконано* |
| 4. | Дослідження протидії зовнішнім загрозам за допомогою фаєрволу FortiGate | 21.03-05.03 | *Виконано* |
| 5. | Оформлення розділу «Аналіз технічного завдання використання фаєрволу в системах захисту інформації» | 06.03 – 17.04 | *Виконано* |
| 6. | Оформлення розділу «Теоретична частина» | 18.04 – 29.04 | *Виконано* |
| 7. | Оформлення розділу «Практична частина» | 30.04 – 13.05 | *Виконано* |
| 8. | Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці» | 14.05 – 21.05 | *Виконано* |
| 9. | Оформлення кваліфікаційної роботи | 22.05 – 05.06 | *Виконано* |
| 10. | Нормоконтроль | 06.06 – 11.06 | *Виконано* |
| 11. | Перевірка на плагіат | 12.06 – 15.06 | *Виконано* |
| 12. | Попередній захист кваліфікаційної роботи | 16.06 – 19.06 | *Виконано* |
| 13. | Захист кваліфікаційної роботи | 22.06.2023 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Студент _____ *Маланчук М.І.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Козак Р.О.*
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

Аналіз логів з використанням фаєрволу FortiGate // Кваліфікаційна робота ОР «Бакалавр» // Маланчук Максим Ігорович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. __ , рис. – __, табл. – ___, кресл. – , додат. –

Ключові слова: ФАЄРВОЛ, БЕЗПЕКА, ІКС, ЛОГ, АНАЛІЗ, ВРАЗЛИВІСТЬ, КІБЕРБЕЗПЕКА, ЗАХИСТ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ.

Кваліфікаційна робота присвячена підвищенню рівня кібербезпеки підприємств шляхом аналізу логів за допомогою фаєрволу FortiGate.

Об'єкт дослідження – процес управління кібербезпекою та протидії зовнішнім загрозам за допомогою фаєрволу.

Предмет дослідження – методи та методики забезпечення кібербезпеки підприємства шляхом аналізу логів за допопомогою фаєрволу.

У роботі розглядаються питання аналізу безпеки систем. Розглянуто вимоги до системи захисту інформації, а також тенденції розвитку та можливі ризики. Зокрема, здійснено аналіз логів для отримання даних про необхідність використання фаєрволу.

В якості інформаційної бази дослідження були використані публікації, наукові видання, навчальні посібники.

Для реалізації даної роботи були використані програмні продукти: Firewall FortiGate, ELK Stack.

# ABSTRACT

Log analysis using FortiGate firewall // Qualification work for the Bachelor's degree // Malanchuk Maxim Igorovich // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, Group СБС-41 // Ternopil, 2023 // P. ___ , fig. -____, table. - __ , chair. - ___ , added. -___.

Keywords: FIREWALL, SECURITY, IDS, LOG, ANALYSIS, VULNERABILITY, CYBERSECURITY, PROTECTION, INFORMATION TECHNOLOGIES.

The qualification work is dedicated to enhancing the level of cybersecurity for enterprises through log analysis using the FortiGate firewall.

The research object is the process of cybersecurity management and countering external threats using a firewall.

The research subject is the methods and techniques of ensuring enterprise cybersecurity through log analysis using a firewall.

The work discusses security analysis issues for systems. The requirements for information security systems, as well as trends in development and possible risks, are considered. In particular, log analysis is performed to obtain data on the necessity of using a firewall.

Publications, scientific articles, and educational manuals were used as the information base for the research.

The following software products were used for the implementation of this work: Firewall FortiGate, ELK Stack.

ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ПК – Персональний комп’ютер

ІКТ - Інформаційно-комунікаційні технології

СБУ – Служба безпеки України

ІКС – Інформаційно-комунікаційна система

WAN – Wide Area Network ( мережа широкого охоплення)

DDoS – Distributed Denial of Service (розподілена відмова в обслуговуванні)

СЗІ – Система захисту інформації

CIA – Confidentiality, integrity, availability

# ВСТУП

У сучасному світі, де інформаційні технології відіграють ключову роль у багатьох сферах діяльності, захист інформації стає все більш актуальною проблемою. В контексті комп'ютерних мереж, забезпечення безпеки інформації вимагає використання спеціальних інструментів та технологій. Один з таких інструментів - фаєрвол, є ефективним засобом захисту мережі від небажаних зовнішніх втручань та загроз.

Розділ 1 кваліфікаційної роботи присвячений аналізу технічного завдання по використанню фаєрволу в системах захисту інформації. Перший підрозділ цього розділу зосереджена на аналізі вимог до системи захисту інформації. Будуть розглянуті основні принципи та вимоги, які мають бути враховані при розробці системи захисту інформації з використанням фаєрволу. Також будуть проаналізовані можливі рішення поставленого завдання з використанням фаєрволів.

Другий розділ моєї кваліфікаційної роботи присвячений теоретичній частині дослідження. У підрозділі 2.1 розглядається розробка узагальненої структури системи захисту інформації в комп'ютерній мережі. Будуть розглянуті основні компоненти системи захисту, їх взаємодія та важливі аспекти, що необхідно враховувати при їх проектуванні.

У підрозділі 2.2 буде досліджено виявлення та нейтралізацію загроз фаєрволами. Будуть розглянуті основні види загроз, які можуть виникати у комп'ютерних мережах, а також методи їх виявлення та захисту з використанням фаєрволів.

У підглаві 2.3 буде розглянуто важливість використання фаєрволів та їх огляд. Будуть проаналізовані переваги та недоліки використання фаєрволів у системах захисту інформації, а також розглянуті основні типи фаєрволів, їх функціональні можливості та принципи роботи.

У підрозділі 2.4 буде надане обгрунтування обраного фаєрволу. Будуть визначені критерії вибору фаєрволу для даної роботи, проведений аналіз доступних варіантів та обґрунтовано рішення щодо обраного фаєрволу.

Третій розділ кваліфікаційної роботи є практичною частиною дослідження. У підрозділі 3.1 будуть переглянуті інструменти для аналізу логів фаєрволу FortiGate. Будуть розглянуті основні можливості цих інструментів та їх застосування для аналізу логів фаєрволу.

У підрозділі 3.2 проводитиметься аналіз логів фаєрволу. Будуть розглянуті методи аналізу логів, виявлення потенційно небезпечних дій та аномалій у мережі з використанням фаєрволу.

У четвертому розділі кваліфікаційної роботи будуть розглянуті аспекти безпеки життєдіяльності та основи охорони праці. Будуть розглянуті питання ергономіки та безпеки робочого місця. Будуть досліджені основні принципи організації робочого простору з метою забезпечення безпеки та комфорту працівників.

Таким чином, кваліфікаційна робота присвячена аналізу технічного завдання по використанню фаєрволу в системах захисту інформації. Вона включає аналіз вимог до системи захисту, розгляд можливих рішень з використанням фаєрволів, теоретичну частину щодо структури системи та важливості використання фаєрволів, практичну частину з аналізу логів фаєрволу та безпеки життєдіяльності.

# РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ ВИКОРИСТАННЯ ФАЄРВОЛУ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

## 1.1 Аналіз вимог до системи захисту інформації

Одним із комплексних заходів протидії загрозі втрати інформаційних ресурсів є система захисту інформації (система кібербезпеки), яка має забезпечити фізичний та програмний захист інформації в телекомунікаційній системі підприємства.

Система кібербезпеки – це сукупність спеціальних засобів кібербезпеки, методів та інструментів, які ними використовуються, і сукупність відповідних технічних заходів, що використовуються для її забезпечення. Для ефективної побудови системи кібербезпеки необхідно чітко визначити політику безпеки та активно реагувати на зміни в сфері кібербезпеки, що відбуваються у світі. При цьому вибір конкретних заходів і методів для забезпечення кібербезпеки залежить від необхідності прийняття своєчасних заходів, які відповідають реальним і потенційним кіберзагрозам, які можуть негативно вплинути на важливі інтереси компанії, її власників і працівників.

Політика безпеки визначається адміністратором відповідних даних. Однак рішення щодо захисту даних не повинні обмежуватися рамками системи електронного документообігу. Абсолютний захист даних практично не реалізується, тому зазвичай зупиняються на відносному захисті інформації – її захист гарантується вчасно тоді, коли доступ до неї сторонніх осіб пов'язаний з усіма наслідками. Контроль доступу також описується в базі даних обмеженнями, і інформація про це зберігається в її системному каталозі. Іноді може знадобитися додаткова інформація від операційних систем, на яких працює сервер бази даних, і від клієнта, який отримує доступ до сервера бази даних.

Сучасні автоматизовані системи мають досить прогресивні інструменти контролю доступу з дискреційними функціями.

Дискреційний контроль доступу (discreet access control) – розмежування доступу між іменованими сутностями та іменованими об'єктами. Організація з певним правом доступу може передати це право будь-якій іншій організації.

Дискреційний захист – це багаторівневий логічний захист.

Логічний захист в операційній системі – це набір дозволів або ролей по відношенню до об'єкта захисту. Наявність таблиці (вид) також можна віднести до логічного захисту. Власник таблиці може змінювати (розширювати, скасовувати, обмежувати доступ) набір дозволів (логічний захист). Логічні дані безпеки знаходяться в системних таблицях бази даних і відокремлені від захищених об’єктів (таблиць або представлень).

На загальнотеоретичному рівні ми виділимо наступні ключові конкретні проблеми інформаційної безпеки, пов’язані з організаційним аспектом інформаційної безпеки в автоматизованих системах.

Мета організації інформаційної безпеки полягає в забезпеченні захисту інформації, що знаходиться в автоматизованих системах, протиставляючи йому ризики безпеки. Одним із важливих аспектів при впровадженні заходів є визначення та перевірка рівня безпеки. Теоретично та практично  ця концепція відображається через "метрологію". Метрологічна діяльність оцінює розвиток і наявність необхідних засобів, стандартів і методів для оцінки якості СЗІ, зокрема відповідність системи безпеки діючим стандартам.

У відповідних положеннях, що у теорії права відомі як "юрисдикційно-технічні" стандарти, норми та методи метрології стану інформаційної безпеки об'єкта проходять процес формалізації. Ці стандарти можуть включати технічні стандарти, інструкції та інші рекомендації.

Застосовуючи викладені в них нормативи, важливо враховувати природну характеристику або властивість, яка з часом втрачає своє значення. Це стається

через прогрес науково-технічної діяльності за відповідних умов можуть змінюватися принципи та методи моніторингу інформаційної безпеки. Практика показує, що, як правило, вдосконалюються стандарти та методи контролю. Існуючі стандарти є настановами, вказівками для створення нових стандартів. Сам термін «стандарт» вказує на наявність фундаментальних обмежень щодо можливих існуючих фізичних метрологічних пристроїв на певному етапі вивчення людиною законів природи [13].

У процесі організації, у тому числі створення алгоритмів (методів) захисту інформації за допомогою технічних засобів, завданням суб'єкта є не лише збільшення наявних технічних засобів захисту інформації, а й врахування можливих інновацій. При цьому має бути реалізований принцип агрегування інновацій до існуючої системи захисту. Краще, якщо є можливість інтегрувати заходи захисту за рахунок інновацій та виведення із системи захисту застарілого обладнання. Однак не варто забувати, що старі засоби захисту, які можуть самостійно функціонувати в системі оборони, не можна бездумно знімати з «озброєння».

При організації захисту інформації в автоматизованих системах важливо враховувати, що хоча технічний пристрій, який обробляє інформацію, є основою автоматизованої системи, присутній також людський фактор в його використанні. Особа може бути користувачем цих систем або розробником.

Таким чином, безпека і надійність автоматизованої системи залежать від двох взаємопов'язаних факторів: людського фактора та інженерно-технологічного фактора.

Забезпечення безпеки інформації в Інтернеті відбувається шляхом:

- дотримання суб'єктами відповідних правових норм, вимог і принципів, які стосуються організаційно-технічного захисту відповідної інформації;

- використання засобів зв’язку, ПЗ, комп'ютерної техніки та автоматизованих систем, які відповідають вимогам безпеки інформації та мають відповідні сертифікати безпеки;
- перевірка відповідності комп'ютерної техніки, програмного забезпечення, засобів зв'язку та автоматизованих систем вимогам щодо захисту інформації шляхом їх сертифікації;
- здійснення контролю за захистом інформації.

Організаційні (адміністративні) заходи захисту включають заходи, спрямовані на регулювання процесів функціонування комплексу обробки даних, використання ресурсів, дії персоналу та взаємодію користувачів з системою з метою ускладнення або усунення можливих загроз безпеці. Ці заходи включають:

- роботи, що проводяться під час проектування, будівництва та оснащення центрів і решти важливих засобів систем;
- встановленням процедур управління доступом користувачів до ресурсів системи;
- заходи, пов'язані з підбором та підготовкою працівників;
- встановлення системи охорони та строгого режиму проходу;
- управління обліком, зберіганням, використанням та знищенням документів та носіїв інформації;
- розмежування реквізитів розподіленого доступу, таких як паролі, ключі шифрування та інші;
- діяльність, пов'язана з проектуванням, розробкою, ремонтом та модифікацією апаратного та програмного забезпечення та іншими аспектами.

Організаційна діяльність, прямо або опосередковано пов'язана з адміністративним управлінням підприємства і спрямована на зменшення його вразливості перед загрозами. Адміністрація підприємства має компетенцію створювати оптимальні умови для забезпечення безпеки підприємства.

У зусиллях запобігання витоку інформації, основні організаційні заходи можна умовно розділити на два типи. Перший тип включає встановлення кадрової політики, критеріїв та концепції підприємства, що включає підбір персоналу та забезпечення їх соціального захисту. Другий тип включає заходи, спрямовані на забезпечення конфіденційності інформації, такі як класифікація документів за їх важливістю та рівнем секретності, встановлення правил зберігання, контролю доступу та обліку цих документів.

Для вирішення цих завдань надзвичайно важливим є правильне застосування юридичних принципів, що регулюють захист комерційної таємниці та конфіденційної інформації. Ці принципи є найпоширенішими і використовуються для захисту конфіденційної інформації, що обмінюється між різними суб'єктами господарювання.

У контексті організаційної діяльності необхідно забезпечити кадрову безпеку організації, оскільки основним суб’єктом загроз кадровій безпеці в цьому секторі економіки є конкуренти, зацікавлені в конфіденційній інформації технологічного та комерційного характеру.

Тому найпоширенішою формою реалізації цієї загрози є одноразовий комерційний підкуп або пряме залучення до роботи співробітників конкурентної організації, допущених до вищезазначених видів діяльності. інформації.

Необхідно забезпечити фізичний захист обладнання від порушень безпеки та загроз навколишнього середовища. Захист апаратного забезпечення інформаційних систем (включаючи апаратне забезпечення, яке використовується за межами організації) має важливе значення як для зменшення ризику несанкціонованого доступу до даних, так і для запобігання втраті або пошкодженню даних. Також варто звернути увагу на проблеми з розміщенням обладнання та його утилізацією. Можуть знадобитися спеціальні заходи для захисту від несанкціонованого доступу та інших небезпек, а також для захисту допоміжного обладнання, такого як живлення та проводка.

Обладнання інформаційних систем має бути розташоване та захищене для зменшення ризику впливу на навколишнє середовище та несанкціонованого доступу. Тому пропонуються такі заходи:

- обладнання повинно бути розміщене таким чином, щоб максимально обмежити непотрібний доступ до робочих приміщень. Робочі станції, на яких зберігаються конфіденційні дані, повинні бути розташовані таким чином, щоб вони постійно перебували під візуальним контролем;

- слід розглянути можливість відокремлення зон, які потребують спеціальний захист для зниження вимог загального рівня безпеки;

- забороняти приймати їжу та палити в місцях розміщення комп’ютерної техніки;

- розглянути можливість застосування спеціального захисту, наприклад клавіатурні мембрани для промислового обладнання [10].

Актуальною проблемою є забезпечення надійності передачі інформації в мережах. У порівнянні з традиційними способами комунікації, такими як телеграми чи телефонні розмови, передача даних в мережах потенційно стикається з більшим ризиком помилок і спотворень. Навіть одна помилка у передачі може серйозно вплинути на якість інформації, особливо коли ми маємо справу з великою кількістю переданих сигналів.

У термінології, використаній Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ, цілісність інформації означає, що інформація не може бути змінена несанкціонованими користувачами або процесами. Доступність інформації, з свого боку, відноситься до можливості користувача отримати необхідну інформацію у потрібному форматі, місці та часі. Якщо цілісність порушується, це може призвести до порушення доступності інформації.

Порушення цілісності інформації, тобто спотворення її, можливе на будь-якому етапі обігу в комп'ютерних мережах, такому як зберігання, передача або

обробка. Причини таких спотворень можуть бути як випадковими, так і навмисними. Випадкові спотворення можуть бути спричинені природними факторами, такими як електромагнітні розряди, іскріння контактів, несправні електронні компоненти або пошкодження носіїв інформації. Випадкові помилки персоналу також можуть спричинити ненавмисні спотворення. Умисні спотворення завжди пов'язані з навмисними діями винних осіб, наприклад, створенням перешкод у лініях зв'язку.

Серед основних методів (механізмів) забезпечення цілісності (а у визначеному раніше значенні – доступності) інформації для каналів телекомунікаційних мереж (далі – ТКМ) (для мереж передачі даних у цілому) слід виділити [3; с. 67]:

Для підвищення співвідношення сигнал/перешкода можна вжити такі заходи, як збільшення енергії сигналу шляхом використання високої початкової потужності, регенерації в точках посилення з обслуговуванням або без нього. Це може потребувати значних витрат енергії або матеріальних ресурсів. Також для обмеження рівня перешкод можна використовувати спеціальні лінії зв'язку, такі як волоконно-оптичні, які мають низький рівень власного шуму. Проте цей підхід вимагає значних фінансових витрат.

Також корисним є використання групових (мажоритарних) методів захисту, які базуються на використанні кількох роз'єднаних каналів зв'язку (зазвичай 3-5), що передають однакову інформацію. Ці підходи можуть також включати повторну передачу однакової інформації в межах одного каналу зв'язку. Перший варіант вимагає значних фінансових затрат, а другий варіант призводить до зниження пропускної здатності каналу зв'язку в 3-5 разів. Отже, використання цих методів у системах (DTS) не завжди є доцільним через ці фактори.

Необхідний і контроль цілісності інформації та програмного забезпечення під час їх обробки та передачі, у тому числі відновлення у випадку її

пошкодження, шляхом двох підходів. Один підхід полягає у використанні різних типів завадостійких кодів, які здатні виявити помилки в отриманій інформації. Ці коди можуть бути реалізовані як програмні, апаратні або програмно-апаратні засоби, спрямовані на виявлення спотворень. Інший підхід полягає у використанні різних типів завадостійких кодів корекції (ЗКК), які дозволяють виявляти та усувати спотворення. Ці коди також можуть бути реалізовані як програмні, апаратні або програмно-апаратні засоби.

Додатково, для збереження недоторканості інформаційних об'єктів, реконструкції пошкодженої інформації, надлишкова інформація додається до інформації, що захищається – позначка цілісності або контрольна позначка (залежно від термінології, прийнятої в завданнях перевірки цілісності або захищеного кодування) – своєрідне зображення, що відображає цю інформацію, порядок її створення відома та яка з великою ймовірністю відповідає захищеній інформації [6, с. 104].

Серед різних способів захисту від помилок можна виділити три основні групи: групові методи, коригувальне кодування, що забезпечує стійкість до завад, і методи, що захищають від помилок у системах передачі зворотного зв'язку.

Для забезпечення спостережуваності інформації в ІКТ-системах (далі – ІКС) використовуються спеціальні моніторингові програми. Програмне забезпечення для моніторингу – це програмне забезпечення (модулі), призначене для забезпечення спостережуваності комп’ютерних систем, а також для запису активності користувачів і процесів, використання пасивних об’єктів, а також однозначного визначення ідентифікаторів користувачів і залучених процесів у конкретних випадках – з метою запобігання порушенням політики безпеки та/або забезпечення відповідальності за певну діяльність [7, с. 101].

Для реалізації заходів захисту інформації використовуються універсальні механізми захисту, які базуються на ідентифікації особи, яка здійснює доступ до IT-системи.

Для забезпечення безпеки інформації використовуються універсальні методи захисту, що базуються на ідентифікації особи, що отримує доступ до IT-системи. До таких методів входять:

- визначення і розпізнавання особи, автентифікація (підтвердження правдивості) та авторизація (передача прав) суб'єктів;
- контроль та обмеження доступу до мобільного додатка;
- реєстрація та аналіз подій, що відбуваються в додатку;
- моніторинг цілісності системи безпеки.

Для підтвердження законності суб'єкта і забезпечення його нормальної роботи в системі, а також для визначення прав суб'єкта на об'єкт або певну діяльність, необхідні механізми ідентифікації, автентифікації та авторизації.

Ідентифікація - це процес визначення захищеного об'єкта або сутності шляхом використання унікального ідентифікатора або спеціально визначеної інформації; кожен елемент або об'єкт у системі повинен мати свою унікальну ідентифікацію.

Автентифікація - це процес перевірки правомірності користувача, процесу, пристрою або іншого елемента системи перед наданням авторизації. Вона також включає перевірку цілісності та автентичності даних під час їх зберігання або передачі, щоб запобігти несанкціонованій модифікації.

Авторизація - це процес контролю та надання прав доступу суб'єкту до певного об'єкта, ресурсу або функції в системі. Це підтвердження, що суб'єкт має дозвіл на виконання конкретних операцій або отримання певної інформації.

Ідентифікація здійснюється за окремим секретним кодом, доступним як суб'єкту, так і системі безпеки об'єкта мобільного середовища. Цей елемент називається ідентифікатором. Як засіб підтвердження унікальності користувача,

роль ідентифікатора може виконувати певний код, пароль або інший механізм, який відрізняє даного користувача від інших. Цей ідентифікатор використовується для ідентифікації та перевірки правомірності користувача при доступі до системи або ресурсів.

Система безпеки об'єкта, як правило, не зберігає сам секретний ключ, але має певну інформацію про нього, на основі якої приймаються рішення щодо відповідності суб'єкта його ідентифікатору. Наприклад, багато програм перед початком інтерактивної сесії запитують у користувача ім'я користувача та пароль. Введене ім'я є ідентифікатором користувача, а пароль - засобом автентифікації. Операційна система, що забезпечує технічну підтримку безпеки об'єкта, зазвичай зберігає не тільки пароль, але й його хеш (криптографічне перетворення).

Сучасні методи безпеки використовують різні способи для ідентифікації та аутентифікації, включаючи:

- одностороння аутентифікація, де клієнт системи підтверджує свою достовірність ;
- двостороння аутентифікація, де як клієнт, так і система (наприклад, банк) підтверджують непідробність;
- тристороння автентифікація використовується для підтвердження автентичності кожного партнера за допомогою нотаріального обслуговування або автентифікації третьої сторони. Це означає, що на процес автентифікації впливають три незалежні сторони, які перевіряють і підтверджують ідентичність один одного.

Методи аутентифікації також можна розділити на однофакторні та двофакторні. Перші включають:

- логічні методи, такі як використання паролів, ключових фраз тощо, які вводяться з клавіатури комп'ютера або спеціалізованого пристрою;

- методи на основі ідентифікації, де фізичні об'єкти, такі як дискети, магнітні карти, смарт-карти тощо, використовуються як носії ключової інформації. Однак, ці методи мають свої недоліки, такі як потреба у спеціальних зчитувачах та можливість втрати, пошкодження, крадіжки або копіювання фізичних носіїв;
- біометричні методи, що ґрунтуються на унікальних особливостях людини, таких як відбитки пальців, райдужна оболонка ока, голос, обличчя. Однак, ці методи також мають свої обмеження, такі як високі витрати, складність в обслуговуванні, чутливість до змін параметрів та обмеження використання тільки для ідентифікації людини, а не програм або пристроїв. Для підвищення рівня безпеки використовується двофакторна аутентифікація. Зазвичай використовується додаткове підтвердження, наприклад, окрім введення пароля, потрібно також ввести секретний код, надісланий у SMS, або окрім PIN-коду, потрібно ввести відповідь на секретне запитання тощо.

Проте доступ до інформаційних ресурсів може здійснюватись не тільки зсередини, і зовні, тому в системі безпеки має бути передбачена підсистема захисту від зовнішніх атак за допомогою спеціальних програмних чи апаратних засобів, що ми і розглянемо в наступному підрозділі.

Отже виконання цих вимог є необхідним для забезпечення захищенності будь якої системи, адже в сучасному світі вона може стати ціллю для зловмисників.

## 1.2 Використання фаєрволів для організації системи захисту

Зовнішні атаки найкраще відстежувати та блокувати досить рано, перш ніж зловмисник зможе отримати повний контроль над системою. Найефективніший спосіб виявлення вразливостей через ін’єкції – це впровадження автоматичного сканера вразливостей у локальній мережі з можливістю перехоплення потенційно небезпечних запитів. Використання автоматизованого програмного або апаратного сканера дозволяє швидше реагувати на сигнали загрози та допомагає ініціювати захисну відповідь для протидії кібератакам.

Мережевий щит, фаєрвол або брандмауер – це апаратний або програмний інструмент, який контролює інформацію, що надходить або виходить з інформаційної системи. Залежно від налаштувань брандмауер може дозволяти або блокувати трафік, шифрувати дані, діяти як інтерпретатор мережевих адрес (NAT). Існує два типи фаєрволів: апаратні та програмні.

Апаратний брандмауер – це спеціальний пристрій, фізично підключений до комп'ютерної мережі. Щоб налаштувати цей тип брандмауера, використовуйте консольний порт на самому пристрої або використовуйте спеціальний інтерфейс командного рядка (CLI) з віддаленого комп’ютера через Telnet або SSH. Прикладами таких пристроїв є: Cisco PIX, Cisco ASA, Firewall ZL1, Watchguard Firebox та інші;

Програмний фаєрвол – це програма, яка працює на окремих кінцевих пристроях: персональних комп’ютерах, серверах і маршрутизаторах. Робота брандмауера полягає в аналізі вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і виконанні відповідних дій відповідно до поточної конфігурації. Діє як захисний бар'єр між внутрішньою мережею компанії та зовнішньою комп'ютерною мережею (WAN) [12]

Загалом існує три покоління фаєрволів з різними типами фільтрації трафіку. Брандмауери першого покоління діють як фільтр пакетів, порівнюючи

основну інформацію, таку як вихідне джерело, адресат, порт або протокол пакета, із визначеним списком правил. Брандмауери другого покоління містять додатковий параметр налаштування фільтра - статус підключення. Використовуючи цю інформацію, технологія може відстежувати дані про поточні дзвінки, їх початок і закінчення. Брандмауери третього покоління призначені для контролю та фільтрації інформації на всіх рівнях моделі OSI, включаючи рівень додатків. Шляхом аналізу цієї інформації брандмауер може виявляти атаки, спрямовані на обхід захисту через використання дозволених портів або несанкціоноване використання протоколів.

Ідентифікувати кодову атаку можна за допомогою аналізу змін трафіку та відхилень від основного режиму використання. Для реалізації даного рішення в мережі необхідно мати два додаткові пристрої. Один з них відповідає за моніторинг вхідного трафіку та виявлення атак, тоді як другий пристрій відповідає за фільтрацію або очищення зовнішнього трафіку. Протягом звичайної роботи ці пристрої мають працювати без перешкод для передачі даних. У випадку загрози скрабер перехоплює трафік, визначений як зловмисний, запобігаючи його проникненню, проте продовжує працювати у нормальному режимі надаючи основні послуги клієнту. Моніторинговий пристрій серверу виконує 4 етапи, щоб виявити саму атаку та джерело атаки. Ці етапи проводяться по порядку, саме так, як вони перелічені. Подібним чином здійснюється моніторинг у випадку DDoS-атак [**17**; с. 10]:

- фіксування входу в систему на основі аналізу незвичайної трафікової активності;
- ідентифікація походження зловмисних дій, таких як веб-додатки, сервери, електронна пошта та інші;
- зупинка трафіку джерела атаки, якщо ця активність відбувається з-за меж локальної мережі та не є допустимою;

- перевірка на те, що атаку було успішно припинено або нормальний трафік відновлено.

Метод виявлення атак за допомогою використання ентропії мережевого трафіку базується на порівнянні локальної міри невизначеності (середнього значення невизначеності за певний час) з глобальною мірою невизначеності (виміряною без наявності атаки). Якщо значення локальної міри надто відмінне з відповідним глобальним, це свідчить про велику ймовірність мережевої атаки.

Для запобігання подібним атакам рекомендується обмежити програмний доступ до даних сервера шляхом розробки та впровадження додатків, які працюють лише з параметризованими запитами. Це дозволяє уникнути незаконного доступу зловмисників до локальних даних або баз даних. Крім того, важливо дотримуватися рекомендацій щодо безпеки при розробці компонентів баз даних та створенні веб-систем з використанням серверів баз даних. [14; с. 25].

Один з методів полягає у необхідності фільтрувати та перевіряти дані, що надходять на сервер, шляхом перевірки спеціальних символів та відповідності числових даних введеному типу. Також важливо обмежити вхідні дані, наприклад, обмежити кількість інформації, яка може бути введена після перевірки на сервері, та відхилити запити, які перевищують певну межу.

Додатково, важливим аспектом у захисті від таких атак є забезпечення безпеки процесу конфіденційності. Наприклад, база даних, яку ви використовуєте, не може містити такі дані у вигляді звичайного тексту чи таблиць (паролі мають бути хешованими, а також містити випадково згенерований рядок, доданий перед шифруванням тощо) [15].

Другим способом забезпечення безпеки є використання серверами баз даних параметричних запитів.

Третій метод полягає у обмеженні відображення повідомлень про помилки користувача, що включають загальні повідомлення про помилки, які можуть відповідати різним збоям. Проте, всі невдачні запити на стороні сервера повинні

бути відстежені, щоб їх можна було переглядати та аналізувати у разі атаки, що відбувається (аудит інцидентів).

Системи виявлення можуть бути поділені на дві категорії: виявлення ознак або виявлення аномалій. Недоліками систем виявлення ознак є їх спрямованість на конкретні типи атак, які були відомі на час розробки.

Коли з’являються нові атаки або змінюються умови трафіку необхідно переглядати задачу виявлення. Виявлення аномалій, через складність моделювання нормального трафіку в Інтернеті, ґрунтується на припущеннях щодо функціонування системи, наприклад, статистичної однорідності трафіку. Однак вони не враховують груп комп'ютерних систем, до яких застосовуються ці припущення, або умови, за яких вони виконуються. Це призводить до необхідності перенавчання алгоритму виявлення навіть при незначних змінах у трафіку або наданому сервісу. Інтеграція моніторингу системи, історії транзакцій, спеціального сховища для інтелектуального аналізу зловмисників та стратегії протидії може бути потенційним рішенням для ефективної системи боротьби з атаками. Тому використання фаєрволів може стати в нагоді для організації системи захисту від зовнішніх атак. З цією метою доцільно більш детально дослідити сучасні пропозиції щодо фаєрволів та проаналізувати їх можливе застосування у якості елемента комплексної системи захисту інформації на підприємстві.

# РОЗДІЛ 2 ТЕОРЕТИЧНА ЧАСТИНА

## 2.1 Розробка узагальненої структури системи захисту інформації в комп’ютерній мережі

Для забезпечення збереження інформації в системах обміну інформацією використовуються спеціальні моніторингові програми. Програмний моніторинг – це програмне забезпечення (модулі), призначене для забезпечення спостережуваності систем зв'язку, а також для реєстрації активності цих процесів, які беруть участь у конкретній події, щоб запобігти порушенню відповідальності [7, с. 101].

Застосування моніторингу забезпечує для адміністратора безпеки системи автоматичного зв’язку:

- виявлення (пошук) усіх випадків нелегітимного доступу до конфіденційних даних;
- локалізувати можливі спроби знищення інформації;
- встановити факти небгрунтованого встановлення ПЗ;
- контролювати використання ПК у робочий та неробочий час (переконатись в потребі такого використання) ;
- виявляти випадки введення спеціальних слів і фраз на клавіатурі чи іншому пристрої кодованого набору, інші випадки спроб несанкціонованої авторизації в системі;
- виявляти факти неправомірного використання засобів зв'язку;
- отримання достовірної інформації, на основі якої буде розроблено політику безпеки компанії;
- контроль доступу до серверів, ПК , інших пристроїв зв'язку;
- провести інформаційний аудит;
- проводити розслідування виявлених інцидентів;

- проведення досліджень, пов'язаних з визначенням точності, ефективності та адекватності реакцій працівників на зовнішню діяльність;
- визначити завантаженість станції зв'язку;
- розробка механізмів відновлення критичної інформації після системних збоїв;
- забезпечити спостережуваність системи. Саме дана властивість, залежно точності її виконання, дозволяє певною мірою контролювати дотримання працівниками компанії встановленої політики безпечної роботи за комп’ютерами та політики безпеки [10, с. 102].

Існують базові принципи захисту від атак: програмні, апаратні та хмарні.

На ринку найбільш популярні програмні рішення, що складаються з інструментів для фільтрації трафіку, розроблених розробниками на основі власного досвіду. Ці рішення є простими у використанні, але ефективними лише проти незначних атак, наприклад, вандалізму.

Апаратні рішення передбачають створення розподіленого мережевого устрою з резервом пропускної здатності. Вони використовуються в широкомасштабних мережевих структурах [18,с . 230].

Хмарні рішення складаються з мережевих структур, які мають високу пропускну здатність і включають сервери для виявлення та блокування небезпечного трафіку. Отже, ця мережа поступово просіює шкідливий трафік, що допомагає зменшити число недозволених пакетів, що досягають кінцевого користувача. [18,с . 231].

## 2.2 Виявлення та нейтралізація загроз фаєрволами

### 2.2.1 Загальні інформація про кіберзагрози

Функціонування ІТ-систем у світі протягом останніх 10 років виявило проблему недостатнього захисту від вірусів. В 2017 році BadRabbit, WannaCry, Petya та інші атакували несподівано, паралізувавши комп'ютерні системи різних установ і підприємств. Хоча їх творці подекуди мали різні цілі та способи впровадження вірусних програм, вони базувалися на спільній основі – недоліках і слабких місцях системи кібербезпеки. Досить показовим у цьому питанні виглядає механізм дії вірусу Petya, який завдав багатомільйонних збитків українським підприємствам і державним установам. Вірус тихо заразив популярну бухгалтерську програму M.E.Doc, отримав доступ до адміністративних привілеїв для керування комп’ютерною системою та вільно поширював свої копії. Не є винятком і банківські установи, які мають бути захищені сучасним технічним та системним забезпеченням. Світовий досвід вірусних атак і значних фінансових втрат повинен був передусім стимулювати фінансові установи шукати вразливості у власних системах кіберзахисту та постійно їх оновлювати. Однак 2017 рік показав реальне небажання підприємств захищатися від такого роду втручань у роботу своїх ІТ-систем [21, с. 10].

Для забезпечення безпеки та захисту інформаційного простору підприємств ІКТ та ІТС від зовнішніх та внутрішніх загроз, необхідно прийняти конкретні нормативно-правові акти та розробити стратегію для впровадження діяльності, спрямованої на виявлення інформаційних загроз в ІТС і підтримка їх безпеки. Основними цілями цих заходів є захист цілісності, конфіденційності, доступності та спостережуваності інформації. [12, с.10].

Враховуючи вище сказане, під поняттям інформаційної безпеки є здатність системи протистояти спробам порушення принципів CIA та спостережуваності інформації, яка перебуває або обробляється в цих системах. Для оцінки

інформаційної безпеки в системі необхідна сукупність заходів, спрямованих на виявлення потенційних загроз інформації в інформаційній та телекомунікаційній системі (ІТС) і запобігання будь-яким несанкціонованим діям, спрямованим проти цієї інформації. Класифікація основних видів кіберзагроз представлена на рис. 2.1.


Рисунок 2.1 - Класифікація загроз безпеці інформації в автоматизованих системах [12, с. 10]

Для оцінки кібербезпеки вузлів зв'язку підприємства застосовується комплексний підхід, який враховує як зовнішні, так і внутрішні загрози, їх джерела, цілі та можливі наслідки атак на об'єкти безпеки.

### 2.2.2 Виявлення та виправлення загроз фаєрволами

Фаєрвол (файрвол, або мережевий екран) - це система захисту мережі, що контролює та регулює трафік між ПК або мережними сегментами. Фаєрволи

виконують ряд функцій для забезпечення безпеки мережі, включаючи виявлення і блокування потенційно небезпечного трафіку.

Ось деякі загрози, з якими фаєрволи зазвичай справляються:

- вторгнення ззовні (External Intrusions), фаєрволи виконують перевірку трафіку, який надходить з Інтернету або інших зовнішніх мереж, і блокують небажаний або шкідливий трафік, такий як шкідливі програми, шкідливі веб-сайти або атаки злому. Вони можуть базуватися на сигнатурах (характерних ознаках) відомих загроз, евристичних методах аналізу або аналізу використання уразливостей;

- атаки від внутрішніх користувачів (Internal User Attacks), фаєрволи можуть контролювати та обмежувати трафік між різними внутрішніми мережевими сегментами. Це дозволяє запобігти несанкціонованому доступу до інформації з обмеженим доступом або атакам з боку зловмисників всередині мережі;

- атаки злому (Hacking Attacks), фаєрволи можуть виявляти та блокувати різні види атак, такі як перехоплення даних, перебір паролів, SQL-ін'єкції, крос-сайтові скрипти та багато інших. Вони аналізують заголовки пакетів і дані, що передаються, та застосовують набір правил, які дозволяють або блокують певні типи трафіку;

- небажаний вміст (Unwanted Content): фаєрволи можуть блокувати доступ до небажаних або нецензурних веб-сайтів, спаму, шкідливих електронних листів та іншого небажаного контенту. Вони можуть використовувати фільтрацію URL-адрес, аналіз вмісту сторінок або списки доменів для блокування небажаного контенту;

- захист даних (Data Protection), фаєрволи можуть забезпечувати захист конфіденційної інформації та запобігати витоку даних. Вони можуть контролювати вихідний трафік, перевіряти шифрування та блокувати передачу конфіденційних даних через незахищені канали;

- захист від DDoS-атак (DDoS Protection), фаєрволи можуть виявляти та мінімізувати вплив розподіленого відмови в обслуговуванні (DDoS) атак. Вони можуть аналізувати трафік, ідентифікувати незвичайний або аномальний об'єм запитів та блокувати атакуючі джерела.

Це лише деякі загрози, з якими фаєрволи зазвичай справляються. Залежно від конкретного фаєрвола та його налаштувань, можуть бути реалізовані різні заходи безпеки, щоб захистити мережу від потенційних загроз.

### 2.2.3 Виявлення загроз з використанням фаєрволу

Фаєрволи можуть виявляти деякі загрози, але усунення проблеми може вимагати додаткових заходів безпеки або втручання з боку адміністратора мережі. Ось кілька прикладів таких загроз:

- соціально-інженерні атаки: фаєрволи можуть виявляти підозрілий трафік, пов'язаний з соціально-інженерними атаками, такими як шахрайства, шахрайські електронні листи, шахрайські веб-сайти тощо. Однак, усунення цих загроз вимагає освіти користувачів та дотримання політик безпеки, оскільки фаєрвол сам по собі не може змінити поведінку користувача.

- вразливості додатків: фаєрволи можуть виявляти спроби злому, що використовують відомі вразливості в додатках або операційних системах. Однак, після виявлення вразливостей, необхідно застосувати патчі та оновлення для виправлення цих вразливостей, що виходить за межі можливостей фаєрволу.

- атаки нульових днів (Zero-day Attacks): нульові дні - це вразливості, які ще не були відомі розробникам програмного забезпечення або не були виправлені патчами. Фаєрволи можуть виявляти підозрілу активність, яка може вказувати на наявність нульових днів, але усунення цих загроз вимагає виходу відповідних виробників програмного забезпечення з відповідними патчами та виправленнями.

- витік інформації: фаєрволи можуть виявляти спроби витоку конфіденційної інформації через мережу, наприклад, за допомогою крадіжки даних або використання каналів передачі даних, які обходять фаєрвол. Однак, усунення проблеми витоку інформації може вимагати використання шифрування, контролю доступу, обмежень на рівні додатків тощо.

Важливо розуміти, що фаєрволи є одним елементом комплексної системи безпеки мережі. Хоча вони можуть виявляти деякі загрози, захист від них вимагає комбінації різних технологій та підходів до безпеки, таких як антивірусне програмне забезпечення, виявлення вторгнень, моніторинг мережі та освіта користувачів.

## 2.3 Типи фаєрволів: їх завдання, переваги та недоліки

### 2.3.1 Необхідність використання фаєрволів

Використання фаєрволів є надзвичайно важливим для забезпечення безпеки мережі і захисту від різних загроз. Ось деякі ключові причини, чому використання фаєрволів є важливим:

- захист від несанкціонованого доступу: фаєрволи можуть фільтрувати трафік та контролювати доступ до мережі. Вони перешкоджають несанкціонованим користувачам, хакерам та зловмисникам, які намагаються проникнути у мережу або зламати системи;
- виявлення та блокування шкідливого трафіку: фаєрволи можуть аналізувати мережевий трафік та виявляти шкідливі пакети, віруси, троянські програми та інші загрози безпеці. Вони блокують такий трафік та запобігають його проникненню до мережі;
- контроль мережевого трафіку: фаєрволи дозволяють контролювати та керувати мережевим трафіком. Вони можуть встановлювати правила та

політики для дозволеного або забороненого трафіку, включаючи фільтрацію IP-адрес, портів та протоколів;

- захист від атак з мережі: фаєрволи допомагають упередити атаки, такі як DDoS (розподілене заподіяння послуг) або флуд мережі, шляхом обмеження трафіку, перевірки пакетів на відповідність правилам та виявлення надмірних або шкідливих запитів;

- розділення мереж: фаєрволи дозволяють розділяти мережу на зони та встановлювати політики комунікації між ними. Це допомагає уникнути небезпечного розповсюдження загроз усередині мереж.

Також було проведено статистичній збір інформації в середовищі ELK Stack, для розуміння обсягів роботи фаєрволу(рис 2.1).


Рисунок 2.1- Збір інформації по логах від фаєрволу FortiGate

Протягом останніх 15 хвилин, фаєрвол FortiGate зміг заблокувати 131 випадків різних зловмисних підключень та спроб компроментації систем.

### 2.3.2 Огляд фаєрволів

Фаєрволи - це безпечність мережевої інфраструктури, існують різні типи брандмауерів, які можуть бути використані для забезпечення захисту мережі.

Огляд типів фаєрволів та їхні характеристики:

Фаєрвол мережного рівня (Network Firewall) працює на рівні мережі (третій рівень моделі OSI) і забезпечує контроль та фільтрацію трафіку на основі інформації про джерело, призначення, IP-адреси та порти. Далі розглянути деякі переваги, суть використання, недоліки та приклади мережевих екранів мережного рівня.

Фаєрволи мережного рівня використовуються для забезпечення безпеки мережі шляхом контролю трафіку на рівні IP-адрес та портів. Вони допомагають запобігати несанкціонованому доступу, фільтрують шкідливий трафік та забезпечують захист від атак.

Переваги:

- контроль трафіку: фаєрвол мережного рівня дозволяє встановлювати правила, які контролюють, які пакети даних можуть входити або виходити з мережі. Це дозволяє обмежити несанкціонований доступ і зменшити ризик вторгнень у мережу;
- фільтрація пакетів: фаєрвол мережного рівня використовує правила фільтрації пакетів, що дозволяють блокувати або дозволяти пакети на основі їх характеристик, таких як IP-адреси джерела та призначення, порти, протоколи тощо;
- захист від атак: фаєрволи мережного рівня можуть розпізнавати та блокувати специфічні види атак, такі як DDoS атаки, використання вразливостей протоколів тощо.

До недоліків цього виду фаєрволів можна віднести обмеження на рівні мережі, фаєрволи мережного рівня не можуть аналізувати вміст пакетів, що може бути необхідним для виявлення деяких видів загроз, які можуть бути приховані

в дозволеному трафіку і відсутність контексту, фаєрволи мережного рівня не мають повного контексту застосунків, які використовують протоколи вищого рівня, що може обмежити їх здатність виявляти складні загрози.

До прикладів фаєрволів мережевого рівня відносяться Cisco ASA, Juniper SRX Series, Palo Alto Networks Firewall, Check Point Firewall, SonicWall Firewall.

Фаєрвол прикладного рівня (Application Firewall) працює на рівні застосунків (сьомий рівень моделі OSI) і здатний аналізувати дані, які передаються за допомогою конкретних протоколів, таких як HTTP, FTP, SMTP тощо.

Переваги:

- фаєрволи прикладного рівня використовуються для захисту застосунків і обмеження доступу до конкретних функцій або ресурсів на основі правил фільтрації вмісту та контексту протоколу. Вони дозволяють виявляти атаки, управляти безпекою застосунків та забезпечувати відповідність з вимогами безпеки;
- глибокий аналіз вмісту: фаєрволи прикладного рівня здатні аналізувати вміст пакетів і розпізнавати специфічні атаки або шкідливий вміст, які можуть бути приховані на рівні протоколів застосунків;
- виявлення вразливостей: фаєрволи прикладного рівня можуть виявляти та запобігати використанню вразливостей у веб-застосунках або інших протоколах застосунків;
- контроль доступу до функцій застосунків: фаєрволи прикладного рівня дозволяють встановлювати правила, які обмежують доступ до певних функцій або ресурсів у застосунках, що допомагає управляти ризиками та забезпечувати безпеку.

Недоліками можна вважати високу складність конфігурації, фаєрволи прикладного рівня можуть бути складними у налаштуванні через необхідність враховувати специфічні протоколи та правила фільтрації вмісту та потреба в

постійному оновленні, фаєрволи прикладного рівня потребують постійного оновлення бази правил та відстеження нових загроз та вразливостей.

Приклади фаєрволів прикладного рівня: F5 Networks BIG-IP Application Security Manager (ASM), Imperva SecureSphere Web Application Firewall (WAF) , Citrix Application Delivery Controller (ADC) with Web App Firewall, Barracuda Web Application Firewall, Fortinet FortiWeb Application Firewall

Фаєрвол рівня з'єднання (Connection Firewall) працює на рівні транспортного (четвертого рівня моделі OSI) і контролює та фільтрує трафік на основі стану з'єднання між джерелом і призначенням. Далі розглянуто деякі переваги, суть використання, недоліки та приклади фаєрволів рівня з'єднання.

Фаєрволи рівня з'єднання використовуються для контролю та фільтрації трафіку на основі стану з'єднання між джерелом і призначенням. Вони допомагають управляти доступом до ресурсів, запобігають атакам на стан з'єднання та забезпечують ефективне використання ресурсів мережі.

Переваги:

- контроль стану з'єднання: фаєрвол рівня з'єднання відстежує стан підключень між джерелом і призначенням. Він може визначати, чи є з'єднання дозволеним, забороненим або потребує подальшої автентифікації;
- мінімізація атаки "Stateful Attacks": фаєрволи рівня з'єднання виявляють атаки, спрямовані на злам стану з'єднання, такі як атаки на вікна із переповненням буферу або атаки на встановлення і підтримку стану з'єднання;
- збереження ресурсів: фаєрвол рівня з'єднання дозволяє належним чином застосовувати ресурси мережі, відкриваючи з'єднання лише для дозволеного трафіку і блокуючи небажаний трафік.

Недоліки:

- відсутність аналізу вмісту: фаєрволи рівня з'єднання не проводять аналіз вмісту пакетів, тому вони можуть пропустити шкідливий вміст, який може бути прихований на рівні даних;

- обмежена гнучкість: фаєрволи рівня з'єднання можуть мати обмежену гнучкість у встановленні складних правил фільтрації, особливо порівнюючи з фаєрволами на рівні застосунків;

Приклади фаєрволів рівня з'єднання Cisco ASA, Juniper SRX Series, Palo Alto Networks Firewall, Check Point Firewall, SonicWall Firewall.

Використання фаєрволів різних типів на одному пристрої допустиме, тому що може збільшити рівень захисту, проте зважаючи на матеріальні витрати, які потрібно буде сплачувати за використання різних мережевих екранів одночасно, більшість компаній відмовляються від такої ідеї на користь одного фаєрволу, оскільки такі витрати є не доцільними.

## 2.4 Обґрунтування обраного фаєрволу

Для аналізу логів було вибрано фаєрвол FortiGate від компанії Fortinet(рис 2.2), яка була засновна в 2000 році, але вже стала однією з провідних компаній в галузі кібербезпеки.


Рисунок 2.2 – Штаб-квартира Fortinet

FortiGate є одним з найпопулярніших і надійних брендів фаєрволів на ринку. Ось декілька причин, чому варто обрати FortiGate і як його переваги порівнюються з іншими фаєрволами:

- загальна безпека: FortiGate пропонує повноцінний пакет безпеки, який включає фаєрвол, виявлення і запобігання вторгнень (IPS), веб-фільтрацію, антивірусні функції та багато іншого. Ви можете мати повну впевненість у захисті вашої мережі від різних загроз;
- висока продуктивність: FortiGate пропонує широкий діапазон моделей з різними рівнями продуктивності, що відповідають потребам будь-якої компанії. Він може ефективно обробляти великі обсяги трафіку без втрати продуктивності;
- інтегрована безпека: FortiGate дозволяє інтегрувати різні функції безпеки в один пристрій. Це дозволяє зменшити складність і затрати на управління безпекою, оскільки вам не потрібно керувати окремими пристроями для кожної функції безпеки;

- висока надійність: FortiGate має вбудовані механізми відновлення після збоїв, такі як функція гарячої заміни, резервування та реплікація. Це дозволяє забезпечити неперервну роботу мережі навіть у разі виникнення проблем;
- простота управління: FortiGate має інтуїтивний і легкий у використанні інтерфейс управління. Ви можете легко налаштувати правила безпеки, моніторинг мережі та отримувати звіти про активність.

Щодо технічних характеристик, FortiGate пропонує різні моделі з різними параметрами, включаючи швидкість обробки трафіку, кількість портів, підтримку VPN, захист від DDoS-атак і багато іншого. Вибір конкретної моделі залежить від потреб вашої компанії та обсягу трафіку. На основі аналізу існуючих загроз та ефективності CPI необхідно підібрати відповідні алгоритми забезпечення фізичного захисту інформації та об’єктів інформаційної діяльності за допомогою фізичних міжмережевих екранів.

Архітектура безпеки Fortinet автоматизує всю інфраструктуру, забезпечуючи надійний захист і видимість для кожного сегмента вашої мережі та пристроїв, чи то віртуальна машина, чи фізичний пристрій, у хмарі чи локально.

Моделі брандмауерів нового покоління FortiGate New Generation Firewall (NGFW) доступні в кількох варіантах, виходячи з потреб клієнтів - від обладнання початкового ступеня до пристроїв високого класу - щоб відповідати найсуворішим вимогам щодо продуктивного захисту від загроз. З їх допомогою ви можете легко та надійно інтегрувати корпоративну мережу або внутрішній сегмент у будь-яке галузеве середовище [19].

Серія FortiGate 80F(рис.2. 3) пропонує компактні, безвентиляторні пристрої, які надають безпечні та масштабовані рішення SD-WAN для філій підприємств і компаній середнього розміру. Ці пристрої забезпечують захист від кіберзагроз, використовуючи прискорення на чіпі та передові захищені SD-WAN

технології, що є доступними та легкими у розгортанні. Fortinet має мережевий підхід, який акцентується на безпеці та забезпечує глибоку інтеграцію з мережею для наступного покоління безпеки. [20].


Рисунок 2.3 - Fortinet FortiGate 80F

Безпека:

- розпізнає тисячі додатків у мережевому трафіку для глибокого контролю та встановлення детальних політик;
- забезпечує захист від шкідливих програм та небажаних веб-сайтів незалежно від того, чи передається трафік у зашифрованому чи незашифрованому вигляді;
- запобігає відомим спробам атак завдяки постійному аналізу загроз засобами FortiGuard Labs, який базується на штучному інтелекті;
- реалізує блокування невідомих та складних атак у режимі реального часу завдяки вбудованій Fortinet Security Fabric FortiSandbox, що використовує штучний інтелект [20].

Ефективність:

- розроблено для інновацій з використанням спеціальних блоків обробки безпеки Fortinet (SPU) для захисту від загроз і найнижчої затримки;
- забезпечує провідну продуктивність в галузі та захист шифрованого трафіку SSL, включаючи перший на ринку брандмауер, який надає глибоку перевірку TLS 1.3 [20] ;

Мережеві характеристики:

- динамічний вибір шляху на будь-якому транспорті WAN для кращого досвіду з мережею, заснований на можливостях самовідновлення SD-WAN;
- розширена маршрутизація, масштабовані VPN, багатоканальна передача та переадресація IPV4/IPV6 з використанням спеціалізованих мережевих процесорів [20] .

Управління:

- SD-WAN Orchestration забезпечує інтуїтивно зрозумілий та спрощений робочий процес для централізованого управління та встановлення бізнес-політик за декілька простих кроків;
- швидке розгортання з підтримкою Zero Touch ідеально підходить для великих і розподілених інфраструктур;
- автоматичне налаштування VPN-тунелів для гнучкого розгортання концентраторів та повнорозмірних мереж з метою агрегації пропускної здатності та шифрування шляхів WAN;
- попередньо визначені списки аналізу впровадження та найкращі практики для поліпшення загального стану безпеки [20] .

FortiGate - це вибір безпеки, надійності та продуктивності для вашої мережі. Він здатний ефективно захищати ваші дані та інфраструктуру від потенційних загроз, забезпечуючи неперервну роботу вашої компанії. Незалежно від того, чи є ваша компанія місцевою, чи має міжнародний присутність, FortiGate забезпечить надійний захист та сприятиме успіху вашого бізнесу.

Отже, використання фаєрволу FortiGate є перспективним для захисту інформаційної системи, тому існує потреба в більш детальному дослідженні його ефективності.

# РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

## 3.1 Перегляд інструментів фаєрволу FortiGate для аналізу логів

Будь який фаєрвол зберігає всі події в журналах логів, проте користуватись ними завжди було складніше, ніж додатковими інструментами, які спрощують перегляд і аналіз будь яких випадків, зафіксованих фаєрволом. Для прикладу в обраному мною фаєрволом, існує система FortiGate-VM 64, яка дозволяє переглядати логи.

FortiGate-VM 64 - це віртуальна машина (VM), яка представляє віртуальну версію файервола FortiGate від компанії Fortinet. За допомогою FortiGate-VM 64 можна створити віртуальну інстанцію файервола FortiGate на віртуалізаційній платформі, такій як VMware ESXi, Microsoft Hyper-V або KVM. Цифра "64" у назві FortiGate-VM 64 вказує на обмеження кількості одночасних апаратних потоків, які підтримує дана версія VM. Значення "64" вказує на максимальну кількість одночасних потоків, які можуть оброблятися фаєрволом FortiGate-VM. FortiGate-VM дозволяє використовувати всі основні функції файервола FortiGate, такі як інспекція пакетів, фільтрація трафіку, VPN-з'єднання, захист від загроз та інші функції безпеки мережі. Вона пропонує ті самі можливості, що й фізичні пристрої FortiGate, але в віртуальному середовищі. FortiGate-VM надає більшу гнучкість і масштабованість, оскільки може бути розгорнута на віртуальних серверах та інтегрована з віртуалізаційними платформами та іншими віртуальними інфраструктурами. Вона також дозволяє забезпечити безпеку для віртуальних машин та віртуальних мереж, що дозволяє застосовувати політики безпеки на рівні віртуального середовища Процедура перегляду логів виглядає наступним чином (рис3.1).

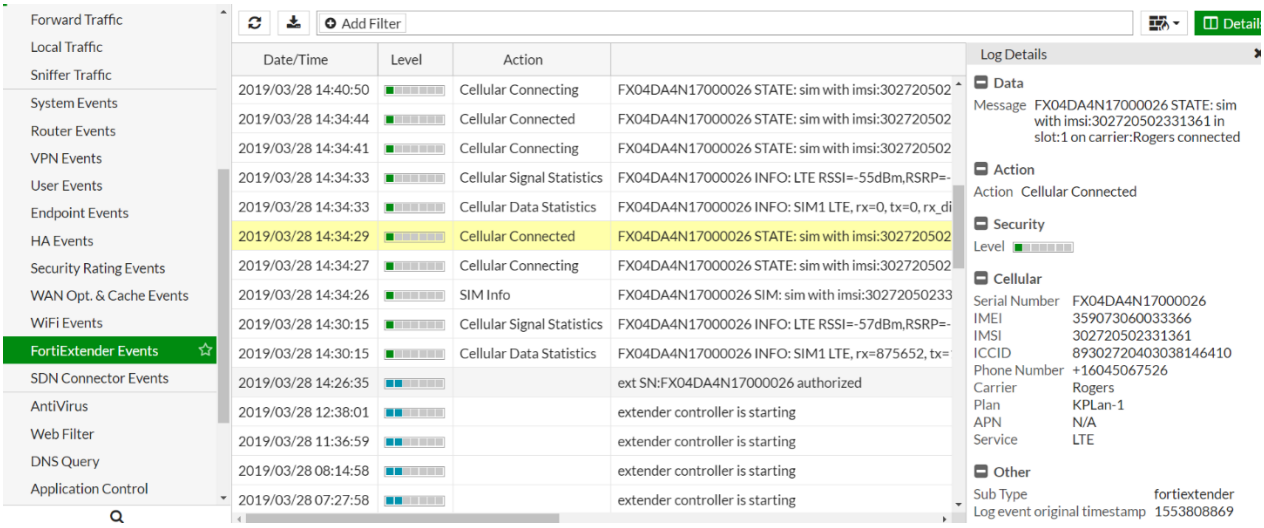



Рисунок 3.1 – Перегляд логів в FortiGate-VM 64

Проте більшою популярністю для перегляду логів, користуються альернативні інстументи, зокрема було обрано набір продуктів ELK Stack.

ELK Stack (також відомий як Elastic Stack) - це набір відкритих програмних продуктів, які працюють разом для збору, зберігання, обробки та візуалізації логів та інших структурованих та неструктурованих даних. ELK складається з трьох основних компонентів: Elasticsearch, Logstash і Kibana. Elasticsearch:

- Elasticsearch - це розподілена система зберігання та аналізу даних, яка використовуєся для потужного і швидкого пошуку, аналізу та візуалізації даних. Вона забезпечує масштабовану архітектуру, дозволяючи індексувати та шукати великі обсяги даних в реальному часі;

- Logstash: Logstash - це інструмент збору, перетворення та пересилання лог-даних. Він дозволяє витягувати дані з різних джерел, таких як журнали подій, бази даних, веб-служби тощо, і пересилати їх до Elasticsearch для зберігання та аналізу. Logstash також надає можливості фільтрації, обробки та збагачення даних перед їхнім збереженням;

- Kibana: Kibana - це інтерактивний інтерфейс візуалізації даних, який дозволяє створювати гнучкі та вражаючі графіки, діаграми, панелі та інші

візуалізації для аналізу даних, збережених у Elasticsearch. Kibana також надає потужні функції пошуку та фільтрації, дозволяючи вам швидко знаходити та аналізувати важливі дані.

Отже, інформація пересилається таким чином: дані зі збірників (наприклад, журналів) передаються до Logstash, де вони обробляються і нормалізуються, а потім пересилаються до Elasticsearch для зберігання. Коли дані зберігаються в Elasticsearch, вони стають доступними для використання в Kibana, де вони можуть бути візуалізовані та аналізовані користувачем. Діаграма взаємодії цих компонентів зображена на рисунку 3.2.

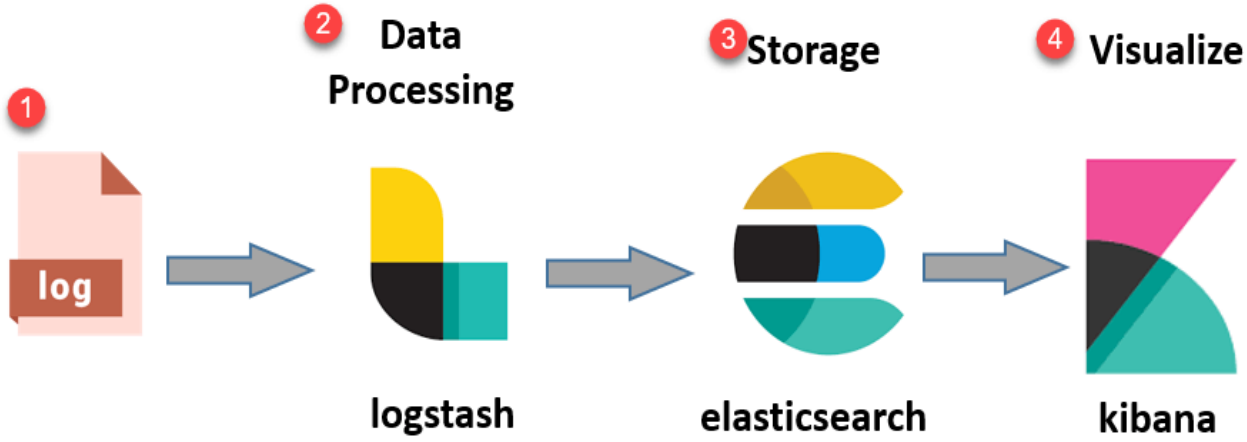



Рисунок 3.2 – Діаграма взаємодії компонентів ELK Search

ELK Stack є популярним рішенням для логування та аналізу даних, і він широко використовується для моніторингу, відладки, безпеки та аналітики даних. Він дозволяє організаціям отримувати цінну інформацію зі своїх лог-файлів та інших джерел даних швидко та ефективно.

## 3.2 Практичні результати аналізу логів

Аналіз логів є процесом вивчення та інтерпретації записів (логів), які створюються комп'ютерними системами, програмним забезпеченням або мережами. Логи містять інформацію про події, помилки, стан системи, діагностичні повідомлення та іншу корисну інформацію, яка допомагає адміністраторам систем, розробникам програмного забезпечення та іншим зацікавленим сторонам аналізувати та вирішувати проблеми.

Аналіз логів може виконуватися в різних контекстах, включаючи налагодження програмного забезпечення, моніторинг систем, виявлення вторгнень, дослідження подій безпеки, виявлення помилок та оптимізацію продуктивності. Цей процес може включати збір, агрегацію, фільтрацію, кореляцію та аналіз великої кількості лог-даних з метою отримання інсайтів, виявлення проблем та прийняття відповідних рішень.

Аналіз логів може використовувати різні техніки, інструменти та алгоритми, такі як пошук, фільтрація, статистичний аналіз, машинне навчання та інші методи. Результати аналізу логів можуть допомогти виявити проблеми безпеки, встановити причини помилок, покращити продуктивність системи або виявити несправності в програмному забезпеченні.

В цілому, аналіз логів є важливим інструментом для розуміння того, що відбувається в комп'ютерних системах і програмах, і допомагає вирішувати проблеми та оптимізувати їх роботу.

В даній роботі було розглянуто декілька різних проблем, а також проаналізовано і знайдено вирішення для кожної з них.

### 3.2.1 Виявлення Bruteforce attack

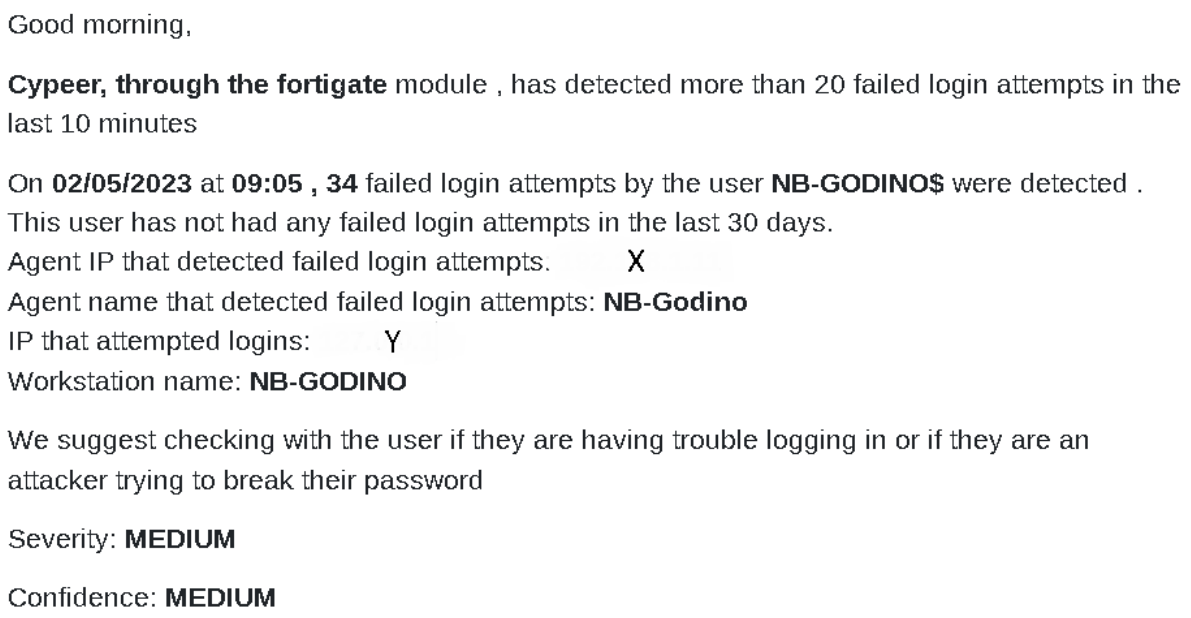
Брутфорс атака (Brute force attack) - це метод вторгнення в систему, при якому злоумисник послідовно перебирає всі можливі комбінації паролів або

ключів, намагаючись вгадати правильний пароль або ключ для отримання несанкціонованого доступу. Це тип атаки на основі перебору (грубої сили), де злоумисник використовує автоматизовані програми або скрипти, щоб швидко спробувати всі можливі комбінації.

Брутфорс атаки зазвичай використовуються для злому паролів облікових записів, доступу до систем або захищених ресурсів. Злоумисники можуть використовувати словники паролів, шаблони або випадкові комбінації для перебору паролів. Атаки можуть бути спрямовані на веб-сайти, поштові сервери, програми, мережеві пристрої та інші системи, які вимагають аутентифікації.

Метою брутфорс атаки є відкриття правильного пароля або ключа шляхом систематичного перебору. Це може зайняти тривалий час, особливо якщо пароль довгий або складний. Однак, якщо пароль недостатньо складний або система має вразливості, то брутфорс атаки можуть бути успішними.

Під час виконання кваліфікаційної роботи було розлянуто цікавий випадок брутфорс атаки(рис 3.3).


Good morning,

**Cypeer, through the fortigate** module , has detected more than 20 failed login attempts in the last 10 minutes

On **02/05/2023** at **09:05 , 34** failed login attempts by the user **NB-GODINO$** were detected .
This user has not had any failed login attempts in the last 30 days.
Agent IP that detected failed login attempts. X
Agent name that detected failed login attempts: **NB-Godino**
IP that attempted logins: Y
Workstation name: **NB-GODINO**

We suggest checking with the user if they are having trouble logging in or if they are an attacker trying to break their password

Severity: **MEDIUM**

Confidence: **MEDIUM**

Рисунок 3.3 – Повідомлення згенероване фаєрволом FortiGate (Bruteforce attack)

Це повідомлення вказує на те , що за допомогою модуля Fortigate, виявлено кілька невдалих спроб входу в систему за останні 10 хвилин. Зокрема, на 2 травня 2023 року о 09:05 було виявлено 34 невдалих спроби входу в систему з боку користувача з іменем NB-GODINO$.

Це повідомлення може свідчити про можливу спробу несанкціонованого доступу до системи або брутфорс атаку на обліковий запис NB-GODINO$.

| Time (@timestamp) | event.code | event.win.eventdata.targetUserName | watcher.description | event.win.eventdata.status |
|---|---|---|---|---|
| May 2, 2023 @ 10:05:27.684 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.681 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.678 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.675 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.672 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.669 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.666 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |
| May 2, 2023 @ 10:05:27.662 | 4625 | NB-GODINO$ | Detected a bruteforce attempt | 0xc000006d |

Рисунок 3.4 – Аналіз логів по Bruteforce attack

Проаналізувавши логи(рис. 3.4), було звернуто увагу на такі деталі:

- event.code - це значення, яке вказує на код або ідентифікатор конкретної події або логу. Воно може бути використано для класифікації та групування подій за типом або категорією. В даному випадку код події 4625 (Event Code 4625) відноситься до Windows Security Log і використовується для ідентифікації невдалої спроби входу в систему (Failed Logon Attempt). Цей код події вказує на те, що спроба входу в систему за обліковим записом була неуспішною.

- Субстатус 0xc000006d, який пов'язаний з Event Code 4625, вказує на конкретну причину невдачі аутентифікації під час спроби входу в систему. У цьому випадку, субстатус 0xc000006d вказує на помилку "LOGON_FAILURE_ACCOUNT_DISABLED" (Обліковий запис вимкнено). Це означає, що обліковий запис, за яким здійснюється спроба входу, був вимкнений або деактивований адміністратором або за певними політиками безпеки. Коли обліковий запис вимкнено, користувач не може використовувати його для входу

в систему, і спроба аутентифікації закінчується неуспішно. Це може бути частиною заходів безпеки, коли обліковий запис тимчасово вимикається або випадково деактивується з причин, таких як підозра на несанкціоновану діяльність, порушення політик безпеки, чи адміністративні дії.

- Знак “$” в кінці поля user.name.Ці облікові записи створюються автоматично операційною системою для використання в службах і додатках з метою забезпечення безпеки та автоматизації. У контексті події з кодом 4625 в Windows, знак долару вказує на спеціальний тип облікового запису, відомий як "Managed Service Account" (управляючий обліковий запис служби). Облікові записи служби, які використовуються в Windows, закінчуються знаком долару ($).

Таким чином, в цьому контексті можна стверджувати, що певна служба або програма автоматично намагалась ввійти в систему з використанням управляючого облікового запису служби, але зазначений обліковий запис був деактивований адміністратором.

### 3.2.2 Виявлення NewCountryAccess

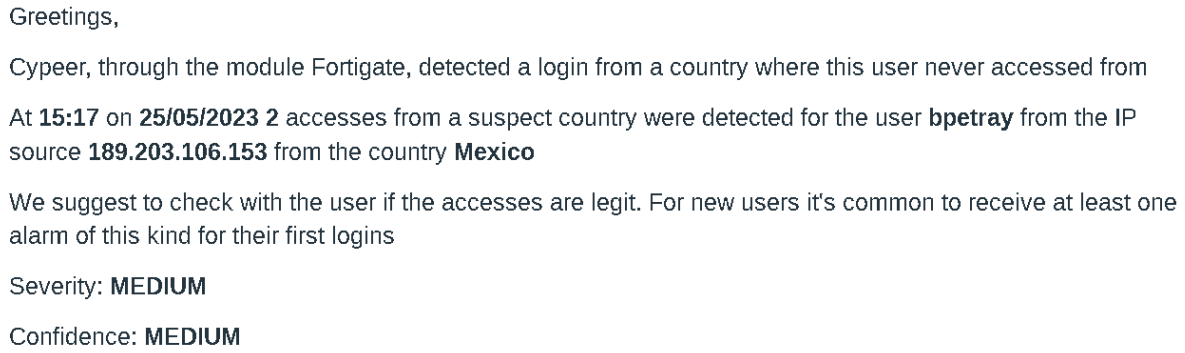
Аларм "NewCountryAccess” вказує на новий доступ з країни, яка раніше не спостерігалася або не була дозволена у вашій мережі або системі. Це означає, що хтось з нової країни намагається отримати доступ до ресурсів або системи, і це може бути потенційно небезпечно.

Такий аларм може спрацьовувати, коли в системі використовується механізм контролю доступу, який вимагає перевірки та авторизації для країн або географічних областей, з яких можна отримати доступ до системи або ресурсів. Якщо IP-адреса або діапазон IP-адрес, з яких надходить трафік, відноситься до нової країни, система спрацьовує аларм "NewCountryAccess".

Цей аларм може вказувати на потенційну загрозу безпеці, оскільки новий доступ може бути зловмисним або несанкціонованим. Він може бути викликаний

злочинною активністю, такою як хакерські атаки, спроби розподілених заперечень обслуговування (DDoS), фішинг або спам.

Залежно від політики безпеки організації, можуть бути прийняті різні заходи для обробки аларму "NewCountryAccess". Це може включати блокування доступу з нової країни, перевірку ідентифікації та авторизації користувачів, збільшення рівня моніторингу та впровадження інших заходів безпеки для зменшення ризиків. Конкретні дії будуть залежати від контексту та внутрішніх політик безпеки вашої організації.


Greetings,

Cypeer, through the module Fortigate, detected a login from a country where this user never accessed from

At **15:17** on **25/05/2023 2** accesses from a suspect country were detected for the user **bpetray** from the IP source **189.203.106.153** from the country **Mexico**

We suggest to check with the user if the accesses are legit. For new users it's common to receive at least one alarm of this kind for their first logins

Severity: **MEDIUM**

Confidence: **MEDIUM**

Рисунок 3.3 – Повідомлення згенероване фаєрволом FortiGate (NewCountryAccess)

Отже, аларм "NewCountryAccess"(рис. 3.5) вказує на спробу входу з країни, з якої цей користувач раніше не мав доступу. В конкретному випадку, о 15:17 25/05/2023 були виявлені дві спроби доступу з підозрілої країни для користувача bpetray з IP-адреси 189.203.106.153, що знаходиться в Мексиці(рис. 3.6).

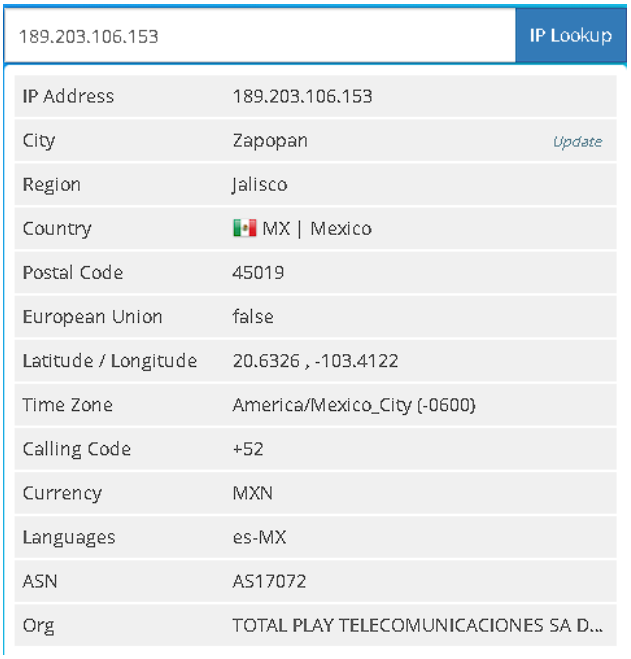



Рисунок 3.6 – Перевірка IP-адресу з якого відбулось з’єднання

В таких випадках, рекомендується перевірити з користувачем, чи ці спроби доступу є законними. Для нових користувачів досить поширене отримати принаймні один аларм такого типу під час перших входів до системи, оскільки це може бути несподіваною активністю для системи.

Проаналізувавши дану ситуацію в ELK Stack (рис.3.7), було виявлено, що користувач використував VPN, тому причин для додаткових дій немає.

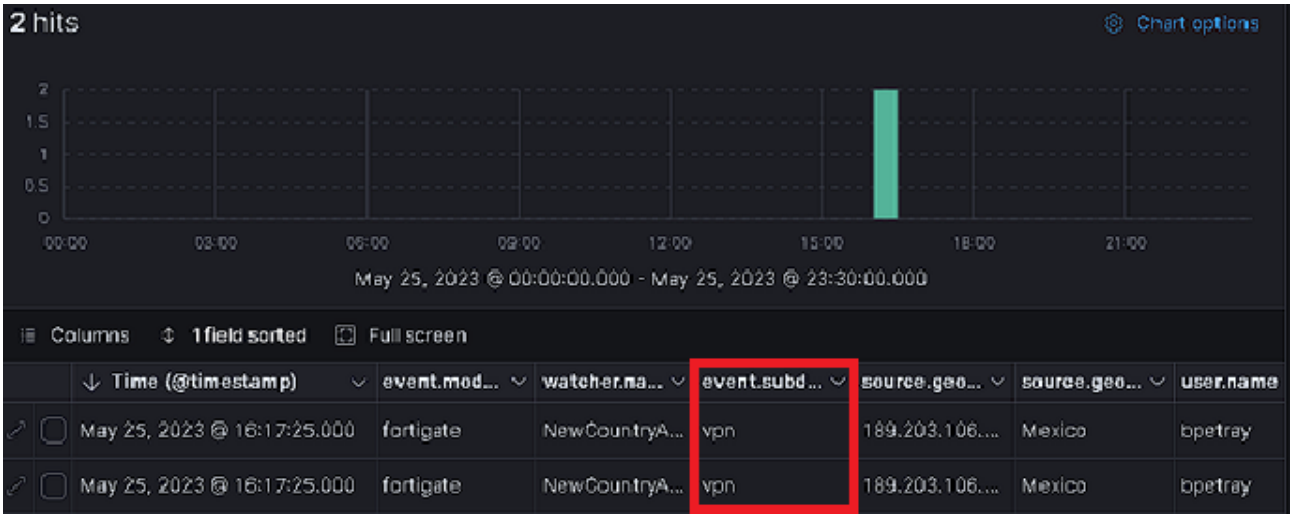



Рисунок 3.7 – Аналіз NewCountryAccess в ELK Stack

Важливо відмітити, що в інших вападках, такі аларми можуть вказувати на можливу загрозу безпеці, тому важливо перевірити легітимність цих доступів та при необхідності вжити відповідних заходів безпеки. Рекомендується зв'язатися з користувачем, підтвердити його ідентифікацію та перевірити, чи були ці доступи авторизовані.

### 3.2.3 Виявлення IntrusionPrevention

Аларм Intrusion Prevention (ІПС) є функцією, яку надає брандмауер (фаєрвол) FortiGate.

ІПС на FortiGate працює на основі сигнатур, що описують відомі шаблони зловмисних атак або небажаного трафіку. FortiGate постійно моніторить мережевий трафік, аналізує його та порівнює з визначеними сигнатурами. Якщо виявляється збіг, це може вказувати на потенційну атаку або небажаний трафік.

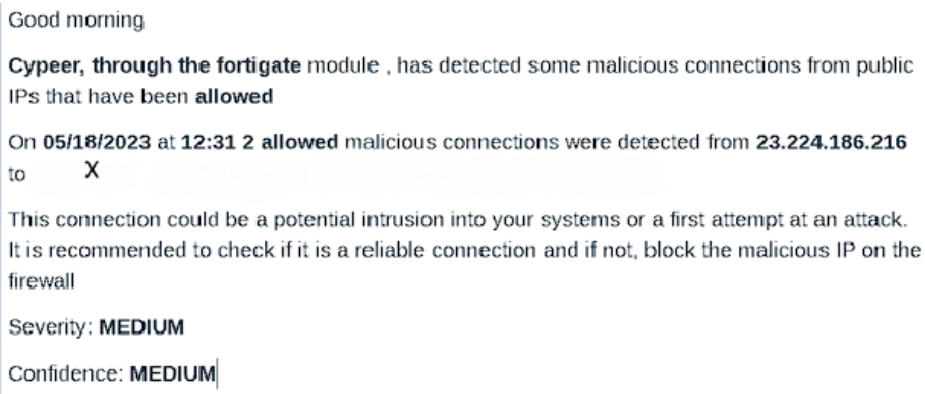
Коли FortiGate розпізнає відповідний сигнатурний збіг, він може прийняти різні заходи, залежно від налаштувань системи, включаючи блокування пакетів, відхилення атаки, запис подій в журнал або сповіщення адміністратора про виявлення.

Це дозволяє FortiGate забезпечити захист мережі від різних видів загроз, таких як вторгнення, атаки ДДоС, використання вразливостей і шкідливий трафік. ІПС є однією з важливих функцій FortiGate, яка допомагає забезпечити безпеку мережі та захистити її від потенційних загроз. Розглянемо цю функцію на конретному випадку.

Аларм Intrusion Prevention (ІПС) є функцією, яку надає брандмауер (фаєрвол) FortiGate. ІПС на FortiGate працює на основі сигнатур, що описують відомі шаблони зловмисних атак або небажаного трафіку. FortiGate постійно моніторить мережевий трафік, аналізує його та порівнює з визначеними сигнатурами. Якщо виявляється збіг, це може вказувати на потенційну атаку або небажаний трафік.

Коли FortiGate розпізнає відповідний сигнатурний збіг, він може прийняти різні заходи, залежно від налаштувань системи, включаючи блокування пакетів, відхилення атаки, запис подій в журнал або сповіщення адміністратора про виявлення.

Це дозволяє FortiGate забезпечити захист мережі від різних видів загроз, таких як вторгнення, атаки ДДоС, використання вразливостей і шкідливий трафік. ІПС є однією з важливих функцій FortiGate, яка допомагає забезпечити безпеку мережі та захистити її від потенційних загроз.


Good morning

**Cypeer, through the fortigate** module , has detected some malicious connections from public IPs that have been **allowed**

On **05/18/2023** at **12:31 2 allowed** malicious connections were detected from **23.224.186.216** to X

This connection could be a potential intrusion into your systems or a first attempt at an attack. It is recommended to check if it is a reliable connection and if not, block the malicious IP on the firewall

Severity: **MEDIUM**

Confidence: **MEDIUM**

Рисунок 3.8 – Повідомлення згенероване фаєрволом FortiGate (IntrusionPrevention)

З рисунку 3.8 (повідомлення згенероване фаєрволом FortiGate), було зроблено висновок, що цей запис логу вказує на виявлення двох дозволених зловмисних з'єднань з IP-адреси 23.224.186.216 (рис. 3.9) до певного хоста (позначеного як "X").


Рисунок 3.9 – Інформація про IP-адресу з бази даних AbuseIPDB

Проаналізувавши цю подію в ELK Stack, було виявлено, що ця атака відноситься до «Intrusion.Generic.WebLogic.Jue.b»(рис. 3.10).

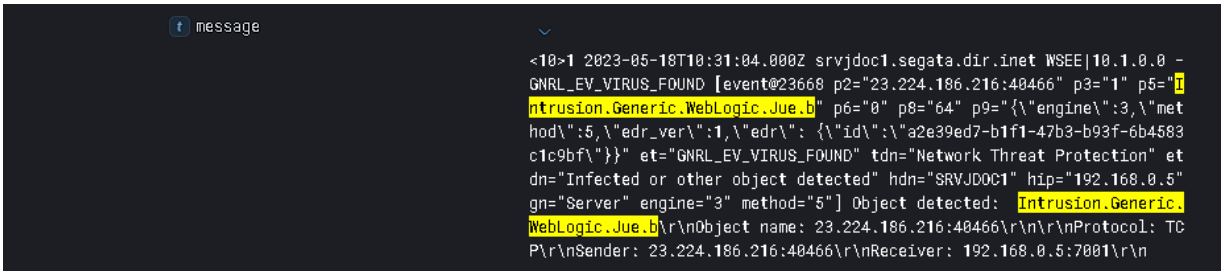



Рисунок 3.10 – Аналіз атаки IntrusionPrevention

Intrusion.Generic.WebLogic.Jue.b - це позначення конкретного типу вторгнення або сигнатури атаки, виявленої брандмауером Fortigate. Воно вказує на те, що була спроба використання вразливості або недоліку веб-сервера WebLogic.

Термін "Intrusion.Generic" вказує на те, що брандмауер виявив певний шаблон або поведінку, яка відповідає відомому методу вторгнення, але конкретні деталі цього варіанту ("Jue.b") можуть відрізнятися. Це може бути певний метод або навантаження, використане в атаку.
В таких випадках рекомендується вжити наступні кроки:

- перевірити системи на компрометацію: провести перевірку комп'ютера чи сервера, з якого здійснювалася невідома активність. Переконатися, що вони не були скомпрометовані або заражені шкідливим програмним забезпеченням. Виконати повний антивірусний скан та переглянути системні журнали на наявність підозрілої активності;
- змінити паролі: змінити паролі для всіх важливих облікових записів і переконатися, що вони є достатньо складними і унікальними. Це допоможе уникнути можливої компрометації облікових даних;
- заблокувати доступ: негайно заблокувати доступ для цієї IP-адреси на рівні брандмауера або іншого захисту мережі. Це можна зробити шляхом додавання правила або внесення IP-адреси до списку блокованих.

# РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

## 4.1 Долікарська допомога при шоку

Шок є серйозним станом, який виникає внаслідок недостатньої кровопостачання організму, що призводить до порушення нормального функціонування органів і тканин. Він може бути спричинений різними факторами, такими як травма, втрата крові, алергічна реакція, інфекція, отруєння або навіть психологічний стрес.

Один з таких факторів, який може викликати шок, пов'язаний з сучасним способом життя - це тривала робота з комп'ютером. Відчуття шоку при роботі з комп'ютером може бути результатом тривалого сидіння в неправильній позиції, поганої вентиляції робочого простору, надмірного напруження очей та надмірного використання м'язів.

Щоб запобігти шоковому стану, зважаючи на різноманітні фактори, що можуть призводити до нього необхідно:

- слідкувати за своїм здоров'ям. До цього відносяться регулярні медичні огляди, фізична активність (прогулянки, вправи розтяжки, йогу або інші види активності);
- створити комфортне середовище. Необхідно створити зручне робоче місце з належною підтримкою для спини та правильною позицією тіла. Відрегулювати стіл та стілець таким чином, щоб вони відповідали потребам. Забезпечиити достатню вентиляцію та освітлення, щоб запобігти втомі та напруженню очей;
- регулярні перерви та розслаблення. Якщо є потреба в роботі за комп'ютером або в будь-якій іншій діяльності, яка вимагає тривалого сидіння або стояння, важливо робити регулярні перерви. Під час перерв важливо вставати з

робочого місця, виконати будь які фізичні вправи, які оптимізують циркуляції крові.

Зважаючи на те, що шок є надзвичайно серйозним станом, важливо негайно вжити кроки для надання долікарської допомоги. Долікарська допомога при шоку включає в себе наступні кроки:

- виклик екстреної медичної допомоги. Потрібно негайно викликати швидку медичну допомогу або амбулаторію, щоб лікарі могли прибути на місце події і надати медичну допомогу;
- забезпечення безпеки. Перш за все, потрібно переконатися, що і потерпілий знаходиться у безпечному місці, щоб уникнути подальшої небезпеки;
- контроль за диханням та циркуляцією. Потрібно перевірити дихання та пульс потерпілого. Якщо вони відсутні, необхідно провести штучне дихання та невідкладну серцево-легеневу реанімацію (ШЛР), якщо є навички такої допомоги;
- забезпечення тепла та комфорту. Необхідно підтримувати потерпілого в теплій і зручній позиції, накрити його ковдрою або одягнути йому теплу одежу, щоб запобігти втраті тепла;
- підняття ніг. Якщо потерпілий не має підозри на травми хребта або нижніх кінцівок, потрібно підняти його ноги на 30 см, це може допомогти поліпшити кровообіг та зменшити симптоми шоку;
- зупинка кровотечі. Якщо є кровотеча, потрібно зупинити її, накладаючи тампон або стиск на поранення. Використовувати потрібно чисту тканину або пов'язку для накладання тиску на поранення;
- забезпечення психологічної підтримки. Шок може бути страшним і травматичним для потерпілого, тому потрібно заспокоїти його, дати підтримку та допомогти зі всім необхідним до прибуття медичної допомоги.

## 4.2 Ергономіка та безпека робочого місця

Розміщення обладнання FortiGate на робочому місці має важливе значення для забезпечення безпеки праці. Перелік аспектів безпеки, які необхідно враховувати при розміщенні обладнання FortiGate:

Вентиляція та охолодження, обладнання FortiGate виробляє тепло під час роботи, тому важливо забезпечити ефективну вентиляцію та охолодження приміщення. Необхідно переконатись, що вентиляційні отвори не заблоковані та повітря може вільно циркулювати навколо обладнання. Використання вентиляторів або кондиціонерів часто є необхідними для підтримки оптимальної температури.

Пожежна безпека, забезпечення пожежної безпеки є важливим аспектом при розміщенні обладнання FortiGate. Необхідно впевнитися, що обладнання розташоване на безпечній відстані від легкозаймистих матеріалів. Також потрібне встановлення системи пожежної сигналізації та вогнегасників у випадку надзвичайної ситуації.

В таблиці 4.1 проведено вибір типів та кількості вогнегасників відповідно до приміщень відповідно до нормативного документа ДБН В.1.1-7-2016 "Пожежна безпека об'єктів будівництва" в Україні.

Таблиця 4.1 -Вибір типу та кількості вогнегасників

| Найменування приміщень | Категорія приміщень за вибухопожежною небезпекою | Вогнегасники | |
|---|---|---|---|
| | | тип | кількість |
| Кабінет керівника | Д | ПВ | 1 |
| Офісні приміщення | Д | ПВ | 1 |
| Серверна | Г | ВВ | 1 |
| Технічні приміщення | Г | ВВ | 1 |
| Коридор | Д | ПВ | 1 |
| Кімната відпочинку персоналу | Д | ПВ | 1 |

Фізична безпека, для забезпечення фізичної безпеки обладнання FortiGate необхідно розмістити його в безпечному місці, де воно буде захищене від неприпустимого доступу та можливих пошкоджень. Також для додаткової безпеки можливе встановлення захисних систем, таких як системи контролю доступу або відеоспостереження.

Електрична безпека, при встановленні та підключенні обладнання FortiGate необхідно дотримуватися вимог електричної безпеки. Переконатися, що використовується правильний тип розеток та кабелів, а також, що підключення здійснюється відповідно до національних та місцевих норм та стандартів.

Ергономіка та безпека робочого місця включають в себе різні аспекти, в тому числі й питання комфортності робочого місця. Комфортне робоче місце є важливим для підтримки здоров'я та благополуччя працівників. Нижче наведені аспекти пов’язані з комфортом працівника при користуванні персональним комп’ютером.

Площу приміщень, в яких розташовані персональні комп’ютери, визначають згідно з чинними нормативними документами з розрахунку на одне робоче місце, обладнане ПК:

- площа - 6,2 м$^2$ (за нормативом не менше 6,0 м$^2$);
- робочі місця розташовані на відстані 1,5 м від стіни з вікном (норма – 1м);
- відстань між поверхнями ПК – 2 м (норма – не менше 1,2 м);
- прохід між рядами робочих місць становить 1,5 м (норма - не менше 1 м).

Заземлені конструкції, що знаходяться в приміщеннях (батареї опалення, водопровідні труби), захищені діелектричними щитками та сітками від випадкового дотику.

Висота робочої поверхні столу для ПК становить 80 см (за нормою має бути в межах 680 - 800 мм), а ширина - забезпечує можливість виконання операцій в зоні досяжності моторного поля.

Стілець працівника ПК має такі елементи, як сидіння, спинку, стаціонарні або знімні підлокітники. Більшість робочих сидінь працівників є поворотним, такими, що регулюються за висотою, кутом нахилу сидіння та спинки, за відстанню спинки до переднього краю сидіння, висотою підлокітників.

Розташування моніторів забезпечує зручність зорового спостереження у вертикальній площині. Клавіатура розміщена на поверхні столу або на спеціальній, регульованій за висотою, робочій поверхні окремо від столу.

Робочі місця з ПК оснащені тримачем для документів, що легко переміщується та встановлений вертикально або з нахилом на тому ж рівні та відстані від очей користувача ПК, що і монітор.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці розташовані так, що забезпечує добру видимість монітору, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля.

Норми мікроклімату та параметрах освітлення для виробничих приміщень згідно ДБН В.2.5-67:2018 “Опалення, вентиляція та кондиціонування повітря” та ДБН В.2.5-28:2018 “Природне та штучне освітлення” наведено в таблицях 4.2 та 4.3 відповідно.

Таблиця 4.2 - Норми мікроклімату робочих приміщень

| Робочі приміщення | Холодний період | | | Теплий період | | |
|---|---|---|---|---|---|---|
| | Тем-ра, °С | Відносна вологість, % | Швидкість руху, м/с | Тем-ра, °С | Відносна вологість, % | Швидкість руху, м/с |
| Кабінет керівника | 21-23 | 75 | 0,1 | 22-24 | 60 | 0,2 |
| Офісні приміщення | 21-23 | 75 | 0,1 | 22-24 | 60 | 0,2 |
| Серверна | 17-19 | 75 | 0,2 | 20-22 | 70 | 0,3 |
| Тех. приміщення | 17-19 | 75 | 0,2 | 20-22 | 70 | 0,3 |

Таблиця 4.3 - Норми і якісні показники освітлення

| Робочі приміщення | Системи освітлення | Норми освітлення | |
|---|---|---|---|
| | | Штучне, лк | Природне (коеф.), % |
| Кабінет керівника | Комбіноване | 300 | 1,8 |
| Офісні приміщення | Комбіноване | 300 | 1,8 |
| Серверна | Штучне, загальне | 300 | 1,5 |
| Технічні приміщення | Штучне, загальне | 300 | 1,5 |

Передбачається також встановлення аварійного та евакуаційного освітлення.

Ергономіка та безпека робочого місця важливі для забезпечення комфорту, здоров'я та ефективності працівників. Дотримання ергономічних принципів сприяє зменшенню фізичного та психологічного навантаження на працівників, що дозволяє їм бути більш продуктивними та зосередженими на виконанні своїх обов'язків.

Правильне розташування обладнання, меблів та інших робочих елементів допомагає уникнути напруги та пошкоджень м'язів і суглобів, зменшує ризик виникнення травм та професійних захворювань. Оптимальне освітлення та вентиляція сприяють збереженню зору, запобігають втомі та забезпечують здорове середовище праці.

Забезпечення безпеки на робочому місці має на меті запобігання виникненню нещасних випадків та негативних наслідків для працівників. Відповідне використання вогнегасників, евакуаційних шляхів, захисного спорядження та інших безпечних процедур допомагає знизити ризик пожежі, травм та інших аварійних ситуацій.

Дотримання ергономіки та безпеки робочого місця є необхідним для збереження здоров'я працівників, підвищення їх продуктивності та забезпечення безпеки в робочому середовищі.

# ВИСНОВКИ

Роботу присвячено дослідженню основних аспектів методики побудови ситеми управління кібербезпекою на підприємствах за допомогою фаєрволів.

В першому розділі роботи розглянуто основні заходи, які можуть бути вжиті для підвищення рівня кібербезпеки підприємства. До них віднесено методики оцінки ризиків загроз та методики протидії інцидентам. Таким чином, існує ряд методів оцінки загроз кібербезпеки підприємств, і їх можна використовувати як поодинці, так і в комплексі в роботі системи управління кібербезпекою, тому існує потреба в більш детальному дослідженні основних практичних засад створення та функціонування служби управління кібербезпекою підприємства на оперативному рівні. Для створення системи захисту об’єкта потрібно спочатку визначитись з рівнем загроз та інструментами протидії їм.

Наступним кроком є оцінка ризику і дії, прописані в політиці безпеки підприємства. В залежності від ризику втрати інформаційних ресурсів через фізичні чи електронні телекомунікаційні  канали можуть застосовуватись різні алгоритми дій, які входять в комплексну політику кібербезпеки і які варто розглянути детально.

У другому розділі було проаналізовано питання  застосування заходів та засобів управління кібербезпекою на основі фєрволів. Таким чином, ми дослідили задачі та дії, які покладаються на службу управління кібербезпекою для інформаційної мережі установи. Згідно визначених задач та цілей, служба управління кібербезпекою повинна регулярно аналізувати можливі загрози шляхом виявлення девіантної активності у будь-якому елементі розподіленої інформаційної мережі та відповідно виконувати заплановані алгоритмом дії, які дозволять уникнути чи мінімізувати наслідки кібератаки на інформаційну мережу. В результаті ефективних дій служби управління кібербезпекою

мінімізуються репутаційні та фінансові втрати підприємства, тому функціонування такої служби є обов’язковим елементом діяльності будь-якої інформаційно-комунікаційної мережі. Проведена розробка узагальненої структури системи захисту інформації в комп’ютерній мережі на основі фаєрволів та обрано апаратий фаєрвол Fortigate.

В третьому розділі було визначено програмні ресурси для перегляду логів, визначена їх ефективність, на основі результатів, які характеризують кількості атак і успішно попереджених чи відбитих інцидентів. Проаналізовано випадки різних інцидентів, знайдено причину їх виникнення, та спосіб їх вирішення.

Наявність логів та їх аналіз є необхідною складовою частиною системи кібербезпеки підприємства. Вони надають інформацію про стан безпеки мережі, можливі вразливості та інциденти, що відбуваються. Аналіз логів дозволяє своєчасно реагувати на загрози та вживати необхідні заходи для забезпечення безпеки даних та ресурсів підприємства.

Усвідомлення та аналіз логів фаєрволу FortiGate є критичними кроками для забезпечення безпеки мережі та захисту від потенційних загроз. Однак, кіберзлочинці постійно вдосконалюють свої методи та техніки атак, тому важливо постійно прогресувати в цьому напрямку. Необхідно забезпечувати оновлення фаєрволу, вдосконалювати навички аналізу логів та використовувати інші інструменти та технології, щоб виявляти нові загрози та реагувати на них. Тільки шляхом постійного прогресу та розвитку можна забезпечити ефективну кібербезпеку та захистити інформаційні ресурси підприємства від шкідливих атак.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Андон П. І., Ігнатенко О.П. Протидія атакам на відмову в мережі інтернет: концепція підходу. *Проблеми програмування.* 2008. № 2-3. С. 564-574.

2. Антонюк П. Є. Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/bozk/19text/g1927.htm. (Дата звернення 10.04.2023)

3. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах. *Сучасна спеціальна техніка.* 2011. № 1(24). С. 61-66.

4. Донець Л. І. Економічні ризики та методи їх вимірювання: навч. посіб. К.: Центр навчальної літератури, 2006. 312 с.

5. Загородній А.Г., Вознюк Г.Л. Фінансово-економічний словник. Львів : Вид-во НУ "Львівська політехніка", 2015. 498 с.

6. Ільницький А. Ю. Основи захисту інформації від несанкціонованого доступу / Д. Ю. Ільницький, В. А. Саницький, В. В. Порошев та ін. К. : Національна академія внутрішніх справ України, 2002. 208 с.

7. Інформаційна безпека (соціально-правові аспекти): підруч. / [В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. Є. Д. Скулиша. К. : КНТ, 2010. 776 с.

8. Кошель А. О. Поняття ризику та його види при використанні земельних ресурсів у ринкових умовах. URL: http://www.nbuv.gov.ua/portal/Chem_Biol/Vldau/APK/2010_1/files/ 10kalimc.pdf. (Дата звернення 10.04.2023)

9. Лук'янова В. В., Головач Т.В. Економічний ризик: навч. посіб. К.: Академвидав, 2007. 464 с.

10. Менеджмент інформаційної безпеки: підруч.: у 2 ч. / А. К. Гринь, О. Д. Довгань, В. І. Журавель та ін.; за заг. ред. Є. Д. Скулиша. – К. : Наук.–вид. Центр НА СБ України, 2013. Ч.1. 456 с.; Ч.2. 604 с.

11. Мороз Е. С., Хорошко В. О., Смычков Е.Е. Методы противодействия сетевым атакам. Збірник наукових праць. Севастополь, СНУЯЕтаІІ, 2007. Т. 18 (№ 5). С. 180-187.

12. Невойт Я. В. Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці : дис. канд. техн. наук. спец. 21.05.01; К. ДУТ, 2016. 110 с.

13. Перевалова Л. В., Кваша С.В. Захист конфіденційної інформації: проблеми та шляхи вирішення. *Вісник Національного технічного університету «Харківський політехнічний інститут». Збірник наукових праць. Тематичний випуск: Актуальні проблеми розвитку українського суспільства.* Харків : НТУ «ХПІ», 2011. № 30. 179 с.

14. Попов, Ю., Рузудженк, С., Погоріла, К. SQL-ін’єкції: огляд потенційних способів захисту. *Комп’ютерні науки та кібербезпека*, 2019. № 3. С. 22-26.

15. *SQL Injection: The Longest Running Sequel in Programming History. URL*: https://www.researchgate.net/publication/324227697_SQL_Injection_ The_Longest_Running_Sequel_in_Programming_History/link/5ac6a25d4585151e80a37b27/download (дата звернення 01.04.2023)

16. Бабенко Т. В. Дослідження ентропії мережевого трафіка як індикатора DDoS-атак. *Науковий вісник НГУ.* 2013. № 2. С. 86-89.

17. Багнюк Н. В. Види DDoS-атак та алгоритм виявлення DDoS-атак типу Flood-атак. *Комп’ютерно-інтегровані технології: освіта, наука, виробництво*. 2015. № 18. С. 6-12.

18. Шпінталь М. Я., Орловський Н.М. Методи захисту робочих станцій від DDoS-атак. *ACIT’2014.* Тернопіль, 16-17 травня 2014. С. 230-231.

19. Моделі та характеристики рішень Fortinet. URL: https://smartnet.ua/services/modeli-ta-harakteristiki-rishen-fortinet/ (дата звернення 07.04.2023)

20. Опис моделі Fortinet FortiGate 81F. URL: https://firewall.com.ua/tovari/merezhevi-ekrani-fortinet/fortinet-fortigate-81f (дата звернення 07.04.2023)

21. Павловська А.Ю Халімон З. Кібербезпека у банківському секторі: чи допоможе IT-outsourcing?. *Юридична газета.* 2018. № 10 (612). С. 10-11.

22. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Інформаційне право*. 2017. № 7. С. 109–116.

23. Гарасимчук О. І., Костів Ю.М. Оцінка ефективності систем захисту інформації. *Вісник КНУ імені Михайла Остроградського*. 2016. № 1. С. 16-20.

24. Хорошко В. А., Чередниченко В.С. Категории и виды информационных воздействий. *Захист інформації.* 2007. № 4(36). С. 31-36.

25. Хорошко В. О. Информационная безопасность Украины. Основные проблемы и перспективы. *Захист інформації.* 2008. № 40 (спец. вип.). С. 6-9.

26. Шпінталь М. Я., Орловський Н.М. Методи захисту робочих станцій від DDoS-атак. *ACIT'2014*. Тернопіль, 16-17 травня 2014. С. 230-231.

27. Єрмошин В. В., Хорошко В.О., Капустян М.В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою. *Сучасний захист інформації*. 2010. №3. С. 95–104.