ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту корпоративної мережі від внутрішніх та зовнішніх кібератак із використанням сучасних IDS/IPS рішень»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Андрій МІРОШНИЧЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-62
МІРОШНИЧЕНКО Андрій
(прізвище, ім'я)

Керівник доктор філософії ПЕДЧЕНКО Євген
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мірошниченко Андрій Валерійович
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захисту корпоративної мережі від внутрішніх та зовнішніх кібератак із використанням сучасних IDS/IPS рішень

керівник кваліфікаційної роботи ПЕДЧЕНКО Євген доктор філософії
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30 » жовтня 2025 року № 467.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 05.10.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси корпоративної мережі;
вибір оптимальних IDS/IPS рішень для виявлення та запобігання кібератакам;
наукова та технічна література, огляд сучасних систем мережевого захисту,
проведення тестувань IDS/IPS у корпоративному середовищі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту корпоративних мереж від внутрішніх і зовнішніх кібератак.
2. Аналіз сучасних IDS/IPS рішень та методів виявлення й запобігання мережевим атакам.
3. Розроблення рекомендацій щодо впровадження IDS/IPS технологій для підвищення захищеності корпоративної мережі.

4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 05.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту корпоративної мережі від кібератак	05.10.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи	15.10.2025 р.	
3.	Аналіз сучасних IDS/IPS рішень та методів виявлення мережевих атак	25.10.2025 р.	
4.	Практична реалізація вибраного IDS/IPS рішення та налаштування тестового середовища	10.11.2025 р.	
5.	Розроблення рекомендацій щодо впровадження IDS/IPS для корпоративної мережі	15.11.2025 р.	
6.	Оформлення результатів дослідження.	25.11.2025 р.	
7.	Підготовка доповіді до захисту.	05.12.2025 р.	

Здобувач вищої освіти _____ Андрій МІРОШНИЧЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача МІРОШНИЧЕНКО Андрій

на тему: «Технологія захисту корпоративної мережі від внутрішніх та зовнішніх кібератак із використанням сучасних IDS/IPS рішень»

Актуальність: актуальність кваліфікаційної роботи зумовлена стрімким зростанням кількості та складності внутрішніх і зовнішніх кібератак на корпоративні мережі сучасних організацій. Умови цифрової трансформації, використання розподілених інформаційних систем і зростання обсягів мережевого трафіку призводять до підвищення ризиків несанкціонованого доступу, порушення цілісності та доступності інформаційних ресурсів. Особливу небезпеку становлять цільові атаки, шкідливе програмне забезпечення, DDoS-атаки, інсайдерські загрози та автоматизовані методи компрометації мережевої інфраструктури. У зв'язку з цим дослідження та впровадження ефективних технологій захисту корпоративних мереж на основі сучасних IDS/IPS-рішень є своєчасним та надзвичайно актуальним.

Позитивні сторони:

1. Текст кваліфікаційної роботи викладено логічно, грамотно та послідовно. Сформульовано чіткі висновки за результатами кожного розділу.
2. У роботі здійснено ґрунтовний аналіз внутрішніх і зовнішніх кібератак, сучасних підходів до захисту корпоративних мереж та можливостей IDS/IPS-систем.
3. Графічний матеріал та ілюстрації оформлено якісно й доречно, вони доповнюють і наочно пояснюють основні положення роботи.
4. Графічний матеріал та ілюстрації оформлено якісно й доречно, вони доповнюють і наочно пояснюють основні положення роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б детальніше продемонструвати впровадження IDS/IPS-рішень на прикладі конкретної корпоративної організації або реального підприємства.
2. Запропоновані рекомендації щодо підвищення рівня захищеності корпоративної мережі можна було б додатково проілюструвати практичними сценаріями використання в умовах конкретної інфраструктури.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"відмінно"**, а здобувач **МІРОШНИЧЕНКО Андрій** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня магістр

Направляється здобувач МІРОШНИЧЕНКО Андрій до захисту кваліфікаційної роботи
(прізвище, ім'я)

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

на тему: «Технологія захисту корпоративної мережі від внутрішніх та зовнішніх кібератак із використанням сучасних IDS/IPS рішень».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***МІРОШНИЧЕНКО Андрій Валерійович*** обрав актуальну тему кваліфікаційної роботи, присвячену захисту корпоративної мережі від внутрішніх і зовнішніх кібератак із використанням сучасних IDS/IPS-рішень. У роботі проаналізовано сучасні загрози корпоративним мережам, досліджено принципи функціонування IDS/IPS-систем та виконано практичну реалізацію захисту на основі Snort. Здобувач продемонстрував належний рівень теоретичної підготовки та практичних навичок, уміння самостійно працювати з науковими джерелами, формулювати висновки й обґрунтовувати прийняті рішення. Робота виконана своєчасно, акуратно та відповідає встановленим вимогам.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***МІРОШНИЧЕНКО Андрій*** на оцінку **"відмінно"** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **МІРОШНИЧЕНКО Андрій** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 74 сторінки, 34 рисунки, 2 таблиці, 46 джерел.

Об'єкт дослідження – захист корпоративної комп’ютерної мережі від внутрішніх та зовнішніх кібератак.

Предмет дослідження – технологія виявлення та запобігання вторгненням в корпоративній комп’ютерній мережі для підвищення рівня кіберзахисту корпоративних інфраструктур.

Мета роботи – підвищення рівня кіберзахисту корпоративної мережі шляхом впровадження сучасних IDS/IPS-рішень, та практичної реалізації системи на основі Snort.

У роботі подано короткий зміст проведених досліджень, що охоплює аналіз сучасних загроз для корпоративних мереж, оцінку вразливостей інфраструктури, порівняння підходів і технологій мережевої безпеки (Firewall, IDS, IPS, SIEM), а також огляд існуючих рішень виявлення кібератак. Особливу увагу приділено архітектурі та функціональним можливостям Snort IDS/IPS. Практична частина містить розгортання, конфігурацію, розробку сигнатур і інтеграцію Snort у систему моніторингу та реагування на інциденти. На основі проведених досліджень сформульовано рекомендації щодо підвищення рівня кіберзахисту корпоративних мереж.

Галузь використання – кібербезпека корпоративних мереж та захист інформаційних ресурсів підприємства.

IDS, IPS, SNORT, КІБЕРБЕЗПЕКА, КОРПОРАТИВНА МЕРЕЖА, ВТОРГНЕННЯ, МЕРЕЖЕВІ АТАКИ, АНАЛІЗ ТРАФІКУ, СИГНАТУРИ, МОНІТОРИНГ, ВИЯВЛЕННЯ АНОМАЛІЙ, ІНЦИДЕНТИ, КІБЕРЗАХИСТ

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасних умовах цифрової трансформації підприємства дедалі більше залежать від безперебійної роботи корпоративних мереж та захисту інформаційних ресурсів. Зростання кількості кібератак, їх складності та автоматизації створює критичні ризики для організацій будь-якого масштабу. Більшість атак сьогодні орієнтовані на отримання несанкціонованого доступу до мережевої інфраструктури, викрадення конфіденційної інформації, порушення роботи бізнес-процесів або нанесення фінансових збитків. При цьому серйозну загрозу становлять не лише зовнішні порушники, а й внутрішні інсайдери, помилки персоналу та неконтрольований мережевий трафік.

У відповідь на ці виклики особливу роль відіграють сучасні IDS/IPS системи, які забезпечують виявлення вторгнень, аналіз аномалій, блокування шкідливої активності та швидке реагування на інциденти. На відміну від традиційних засобів захисту, IDS/IPS здатні працювати з високошвидкісним трафіком, використовувати як сигнатурні, так і поведінкові моделі, а також інтегруватися з SIEM-рішеннями для побудови комплексної системи кібербезпеки.

Разом із тим, ефективне впровадження IDS/IPS вимагає глибокого розуміння їх архітектури, алгоритмів, можливостей і недоліків, а також врахування специфіки корпоративної інфраструктури. Тому дослідження технологій захисту мереж на основі IDS/IPS є актуальним і необхідним для забезпечення надійної кібербезпеки, підвищення стійкості підприємства до зовнішніх та внутрішніх атак і мінімізації потенційних збитків.

Об'єкт дослідження – захист корпоративної комп’ютерної мережі від внутрішніх та зовнішніх кібератак.

Предмет дослідження – технології виявлення та запобігання вторгненням (IDS/IPS), методи їх інтеграції, налаштування та застосування для підвищення рівня кіберзахисту корпоративних інфраструктур.

Мета роботи – підвищення рівня безпеки корпоративної мережі шляхом впровадження сучасних IDS/IPS-рішень, аналізу механізмів виявлення атак та

практичної реалізації системи на основі Snort.

Наукові завдання:

здійснити аналіз внутрішніх і зовнішніх кібератак, що становлять загрозу корпоративним мережам, та визначити їх основні класи, особливості й методи проведення;

провести дослідження вразливостей корпоративної мережевої інфраструктури та оцінити чинники, що впливають на рівень її захищеності;

проаналізувати існуючі підходи та моделі забезпечення мережевої безпеки, включаючи засоби моніторингу, фільтрації й контролю доступу;

дослідити сучасні IDS/IPS системи, їх архітектури, алгоритми виявлення кібератак та способи інтеграції у корпоративні мережі;

порівняти можливості сигнатурних, поведінкових та гібридних методів виявлення загроз для визначення їх ефективності в різних умовах функціонування мережі;

розробити наукове обґрунтування вибору IDS/IPS рішень для підвищення рівня захисту корпоративної інфраструктури;

сформувати рекомендації щодо впровадження IDS/IPS технологій з урахуванням специфіки мережевого середовища, вимог до продуктивності й безпеки.розроблення рекомендацій щодо оцінки ефективності та надійності обраних антивірусних рішень для забезпечення максимального рівня кібербезпеки;

Методи дослідження:

1. Аналіз літературних та технічних джерел – вивчення сучасних підходів до захисту мереж, методів виявлення вторгнень, сигнатурних і поведінкових моделей IDS/IPS.

2. Методи системного аналізу та проєктування – розроблення архітектури системи захисту, моделювання потоків даних та вибір оптимальної стратегії моніторингу.

3. Методи конфігурації та програмної реалізації – налаштування Snort IDS/IPS, створення сигнатур, інтеграція з мережею та інструментами збору подій.

4. Експериментальні методи – тестування роботи системи на реальних

мережевих трафіках, імітація атак, оцінка точності виявлення, ефективності реагування та надійності захисту.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування сучасних IDS/IPS методів та засобів захисту корпоративної мережі від внутрішніх і зовнішніх кібератак; а також сформовано практичні поради для фахівців з кібербезпеки щодо впровадження та оптимізації IDS/IPS рішень у мережевій інфраструктурі підприємства.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Класифікація внутрішніх і зовнішніх кібератак

У контексті забезпечення кібербезпеки корпоративних мереж загрози поділяють на внутрішні та зовнішні (рис. 1.1), що дозволяє точніше ідентифікувати джерело небезпеки та розробити відповідні механізми протидії.

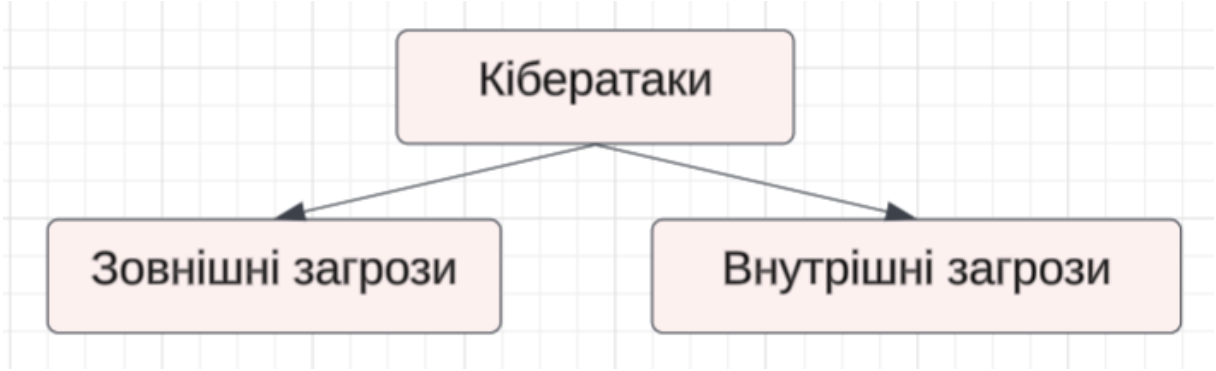

Рис. 1.1 – Класифікація кібератак

Зовнішні загрози – це потенційно шкідливі дії або впливи, що походять з-поза меж корпоративної інфраструктури і здійснюються суб’єктами, які не мають легітимного доступу до внутрішніх ресурсів організації. До таких загроз належать атаки хакерських угруповань, автоматизовані ботнети, шкідливе програмне забезпечення, експлойти мережевих сервісів, а також розвідувальні дії, спрямовані на пошук вразливостей. Метою зовнішніх атак, як правило, є отримання несанкціонованого доступу, порушення роботи сервісів, викрадення даних або нанесення репутаційних чи фінансових збитків [1].

Внутрішні загрози – це загрози, що формуються усередині організації та походять від співробітників, підрядників, партнерів або компрометованих внутрішніх систем. Вони можуть бути як умисними, так і ненавмисними. До внутрішніх загроз належать зловживання привілеями, помилки персоналу, порушення політик доступу, несанкціоноване використання обладнання, витік інформації або недотримання правил кібергігієни. Особливу небезпеку такі загрози становлять через те, що внутрішній порушник зазвичай має легітимний доступ до

систем та ресурсів, що ускладнює їх виявлення традиційними засобами захисту.

Розмежування внутрішніх і зовнішніх загроз є системного підходу до побудови комплексної моделі безпеки корпоративної мережі, оскільки кожна з цих категорій потребує специфічних методів виявлення та реагування. Кібератаки на корпоративні мережі відзначаються значною різноманітністю, що зумовлено як еволюцією інструментів зловмисників, так і розвитком цифрової інфраструктури. Для системного аналізу доцільно класифікувати атаки за характером реалізації, механізмами впливу та джерелом загроз. На рис. 1.2 наведено огляд найбільш поширених типів зовнішніх та внутрішніх атак, які становлять критичну небезпеку для сучасних організацій.

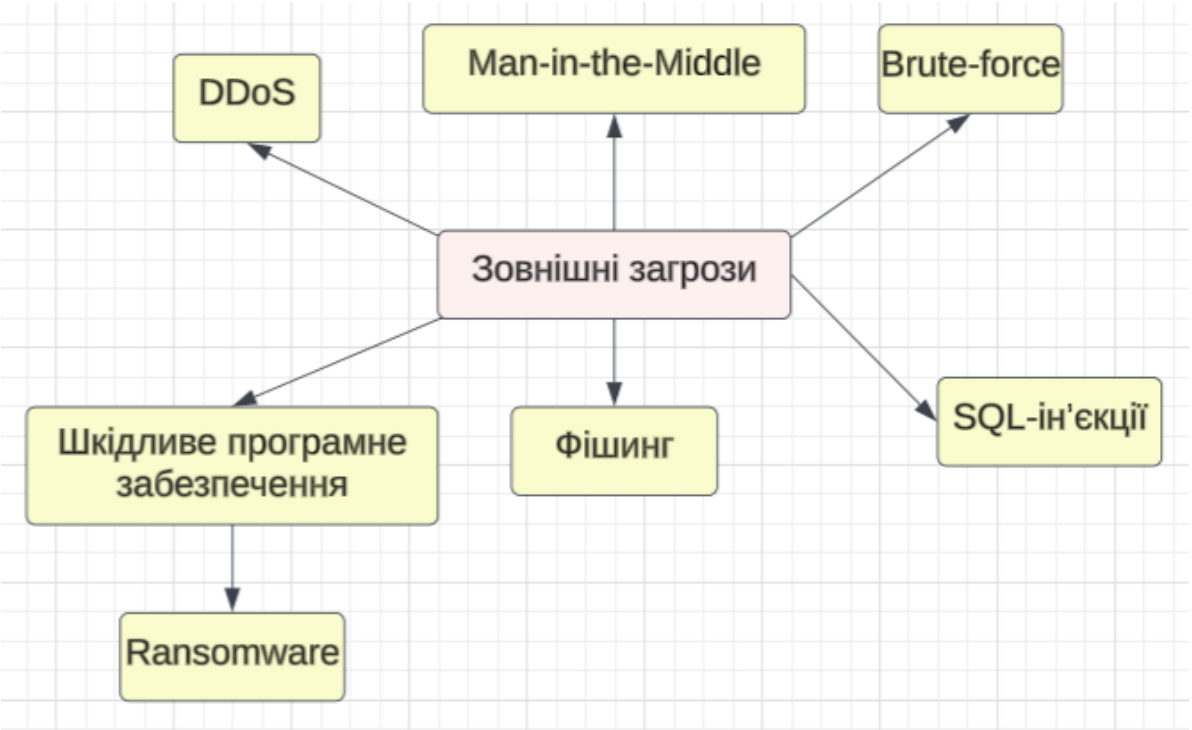

Рис. 1.2 – Зовнішні кібератаки

Фішинг – це соціотехнічний вид атаки, спрямований на отримання конфіденційної інформації шляхом введення користувача в оману. Зловмисники імітують легітимні ресурси або офіційні повідомлення, спонукаючи жертву переходити за шкідливими посиланнями, завантажувати файли або розкривати облікові дані [2]. Фішинг часто є початковим вектором для складніших атак, включно з компрометацією мережі, встановленням шкідливого ПЗ та подальшою

ескалацією привілеїв.

Malware (шкідливе програмне забезпечення), до категорії шкідливого ПЗ входять програми, створені для порушення нормальної роботи систем, викрадення даних або отримання несанкціонованого контролю над корпоративними ресурсами. Malware включає віруси, трояни, шпигунські модулі, ботнет-клієнти та інші шкідливі компоненти. Їхнє поширення здійснюється через заражені файли, електронну пошту, експлойти вразливостей або USB-пристрої.

Ransomware є специфічним видом шкідливого ПЗ, основною метою якого є шифрування даних або блокування роботи системи з подальшою вимогою викупу. Такі атаки можуть призводити до зупинки бізнес-процесів, втрати інформації та суттєвих фінансових збитків. Сучасні версії ransomware часто поєднують шифрування із попереднім викраденням даних (double extortion), що підвищує рівень ризику для організацій.

Man-in-the-Middle (MITM), атака "людина посередині" полягає у прихованому перехопленні та можливому модифікуванні даних під час їх передавання між двома легітимними сторонами. MITM-атаки стають можливими у разі використання незахищених мереж, протоколів або скомпрометованих сертифікатів. Зловмисник може перехоплювати облікові дані, змінювати контент або підміняти автентифікаційні ключі[3].

SQL-ін’єкції – це тип атаки, спрямований на маніпулювання запитами до бази даних шляхом введення шкідливого SQL-коду через веб-форми або параметри URL. Внаслідок такої атаки зловмисник може отримати доступ до конфіденційної інформації, змінювати записи, обходити автентифікацію або знищувати дані. SQLi належить до найбільш критичних веб-уразливостей відповідно до OWASP Top 10.

Distributed Denial of Service (DDoS), атака полягає у навмисному перевантаженні мережевих сервісів за рахунок генерації надмірної кількості запитів з великої кількості заражених пристроїв (ботнетів). Така атака унеможливлює нормальне функціонування веб-ресурсів, серверів або мережевої інфраструктури. Деякі DDoS-кампанії мають також відволікаючий характер, прикриваючи інші, більш складні атаки.

Brute-force (атаки методом перебору), атаки передбачають систематичний перебір паролів або ключів автентифікації з метою отримання доступу до захищених ресурсів. Сучасні інструменти автоматизації дозволяють здійснювати мільйони спроб автентифікації за короткий час. Особливо вразливими є системи без обмеження кількості спроб або з використанням слабких паролів.

Внутрішні загрози посідають особливе місце в структурі ризиків корпоративної мережевої безпеки, оскільки вони виникають у межах самої організації та пов’язані з діями співробітників, підрядників або інших осіб, які володіють легітимним доступом до інформаційних ресурсів. На відміну від зовнішніх атак, внутрішні загрози часто залишаються непомітними протягом тривалого часу, що ускладнює їх виявлення традиційними засобами захисту та збільшує потенційний масштаб збитків. З метою систематизації основних проявів таких ризиків внутрішні загрози поділяють на три ключові категорії: інсайдерські загрози, зловмисні працівники та ненавмисні помилки персоналу. Структурне відображення цієї класифікації наведено на рис. 1.3.

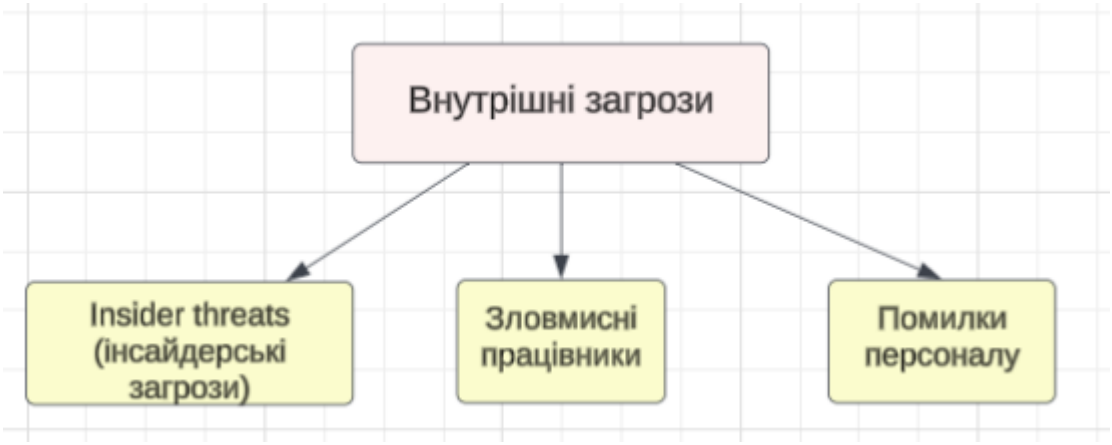

Рис. 1.3 – Класифікація внутрішніх загроз

Insider threats (інсайдерські загрози), виникають у випадках, коли співробітники або особи, які мають законний доступ до ресурсів компанії, використовують цей доступ у шкідливих цілях. Інсайдер може приховано викрадати інформацію, змінювати конфігурації систем, обходити політики безпеки або навмисно створювати вразливості. Такі загрози важко виявити, оскільки дії порушника зовні можуть виглядати як легітимні.

Помилки персоналу – ненавмисні дії співробітників є одним із найбільш розповсюджених джерел інцидентів інформаційної безпеки. До них належать неправильне налаштування обладнання, випадкове видалення даних, недотримання політик доступу, відкриття фішингових листів, використання ненадійних носіїв або порушення правил кібергігієни. Помилки персоналу можуть створювати критичні вразливості навіть за умови високого рівня технічного захисту.

Зловмисні працівники – це окрема підкатегорія інсайдерів, дії яких мають чітко виражений умисний характер. Такі працівники можуть саботувати системи, здійснювати несанкціоноване копіювання даних, допомагати зовнішнім зловмисникам або продавати внутрішню інформацію конкурентам. Зловмисні працівники часто мають глибоке знання внутрішніх процесів компанії, що суттєво підвищує рівень їх небезпеки [4].

Еволюція цифрових технологій зумовила появу нових форм кібератак, що відзначаються високим рівнем автоматизації, складністю виявлення та значними можливостями для обходу традиційних засобів захисту. Однією з ключових тенденцій є зростання кількості атак типу Zero-Day, що експлуатують вразливості, які ще не були задокументовані або виправлені розробниками програмного забезпечення. Такі атаки становлять критичну загрозу, оскільки захисні системи не володіють сигнатурами відповідних експлойтів, що дозволяє зловмисникам непомітно проникати в корпоративні інфраструктури.

Ще одним важливим напрямом розвитку загроз є атаки з використанням технологій штучного інтелекту, які забезпечують автоматичний аналіз поведінки користувачів, динамічне формування шкідливих сценаріїв та адаптацію до механізмів захисту. AI-підходи використовуються як для створення більш переконливих фішингових повідомлень, так і для генерації змінних версій шкідливого коду, здатних обходити сигнатурні механізми виявлення.

Крім того, суттєво зросла роль автоматизованих сканерів та ботнет-платформ, які здійснюють масове сканування мережевих портів, протоколів та веб-додатків з метою виявлення вразливостей. Такі інструменти дозволяють

зловмисникам оперативно знаходити слабкі місця у великій кількості систем, що підвищує ефективність подальших атак, включно з brute-force, SQL-ін’єкціями чи розгортанням шкідливих програм. У сукупності ці тенденції свідчать про ускладнення загрозового середовища та потребу у впровадженні адаптивних, інтелектуальних механізмів моніторингу та захисту, здатних протидіяти швидко змінним та високотехнологічним атакам [5].

Різноманіття кібератак, їхня динамічна еволюція та поява нових високотехнологічних загроз зумовлюють необхідність комплексного підходу до оцінювання поточного стану безпеки корпоративної мережі. Ефективне протистояння як традиційним, так і сучасним атакам можливе лише за умови системного аналізу внутрішніх та зовнішніх вразливостей, що можуть бути використані зловмисниками. Тому наступним етапом дослідження є розгляд методів і принципів виявлення слабких місць інфраструктури, які визначають загальний рівень кіберстійкості організації.

1.2 Оцінка вразливостей корпоративної інфраструктури

Ефективний захист корпоративної мережі неможливий без систематичного аналізу її вразливостей, які визначають потенційні шляхи реалізації кібератак. Вразливості можуть виникати як у програмному забезпеченні та мережевому обладнанні, так і в організаційних процесах, політиках доступу чи поведінці користувачів. Їх своєчасне виявлення дозволяє зменшити ризик експлуатації з боку зловмисників, мінімізувати можливі наслідки інцидентів та забезпечити відповідність сучасним вимогам кібербезпеки. Тому оцінка вразливостей є ключовим елементом управління інформаційною безпекою та визначає основу для планування подальших заходів із впровадження засобів захисту.

У контексті аналізу вразливостей корпоративної інфраструктури концептуальним підходом є розгляд так званої «захисної поверхні» (attack surface). Під цим поняттям розуміють сукупність усіх точок контакту системи із зовнішнім чи внутрішнім середовищем, через які зловмисник може спробувати реалізувати

атаку. Чим складнішою є інфраструктура та чим більше вона містить відкритих сервісів, інтерфейсів взаємодії, мережевих портів або користувацьких облікових записів, тим ширшою стає її захисна поверхня, а отже – зростає ймовірність експлуатації слабких місць (табл. 1.1). Аналіз attack surface дозволяє систематично оцінити всі потенційні канали доступу, визначити найбільш вразливі компоненти та сформувати пріоритети захисних заходів, спрямованих на мінімізацію площини можливого нападу [6].

Таблиця 1.1.

Типові слабкості корпоративних мереж

Слабкість	**Опис**
Неправильна сегментація мережі	Відсутність чіткого поділу мережі на ізольовані сегменти призводить до неконтрольованого переміщення зловмисника всередині інфраструктури після компрометації одного вузла. Це відкриває шлях до ескалації привілеїв та доступу до критичних ресурсів.
Слабкі паролі та відсутність політик автентифікації	Використання простих або повторюваних паролів робить систему вразливою до brute-force, credential stuffing та інших методів підбору доступу. Відсутність багатофакторної автентифікації значно посилює ризики.
Відсутність або недостатній моніторинг мережі	Брак SIEM, IDS/IPS чи інших інструментів моніторингу призводить до того, що інциденти залишаються непоміченими тривалий час. Це дає зловмисникам можливість безперешкодно здійснювати проникнення, аномальні дії та ексфільтрацію даних.
Некоректні правила ACL та управління доступом	Помилки в налаштуванні ACL, надмірно широкі дозволи або порушення принципу найменших привілеїв створюють можливості для несанкціонованого доступу між сегментами мережі та до критичних систем.
Застаріле програмне забезпечення або обладнання	Використання невчасно оновленого ПЗ та обладнання без підтримки виробника відкриває доступ до відомих експлойтів. Це робить систему легкою мішенню навіть для автоматизованих атак.

У науковій та нормативній літературі поняття вразливості використовується для позначення властивостей інформаційної системи, які можуть бути використані зловмисником для порушення її конфіденційності, цілісності або доступності.

Відповідно до стандарту ISO/IEC 27005, вразливість визначається як слабкість активу або групи активів, що може бути експлуатована однією чи декількома загрозами. У документах NIST SP 800-30 вразливість розглядається як недолік у системі безпеки, який може призвести до успішної атаки за умови наявності відповідного вектора загрози.

Вразливості можуть бути результатом помилок проєктування, недосконалості реалізації програмного забезпечення, неправильного налаштування мережевих компонентів або недотримання організаційних політик безпеки. Їх наявність не обов’язково означає неминучий інцидент, проте значно збільшує ймовірність успішної атаки, оскільки створює потенційні точки входу для зловмисників.

Важливою характеристикою вразливостей є їхня експлуатованість, тобто можливість практичного використання недоліку для отримання небажаного результату. У цьому контексті вразливість набуває значення лише тоді, коли існує загроза, здатна її реалізувати, а також відповідний шлях доступу. Саме тому системна оцінка вразливостей є невід’ємною складовою управління ризиками корпоративної мережевої безпеки [7].

Для ефективного аналізу вразливостей корпоративної інфраструктури необхідно використовувати систематизовані моделі загроз, які дозволяють описувати можливі дії зловмисника, визначати ймовірні вектори атак та прогнозувати потенційні наслідки. Найбільш поширеними у практиці кібербезпеки є моделі MITRE ATT&CK та STRIDE, які доповнюють одна одну і забезпечують всебічний підхід до оцінки ризиків.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це глобальна структурована база знань, яка описує тактики, техніки та процедури, що використовуються реальними зловмисниками під час кібератак (рис. 1.4). Модель побудована у вигляді матриці, де кожна тактика відображає етап атаки, а кожна техніка – конкретний спосіб її реалізації.

Рис. 1.4 – Логотип MITRE ATT&CK

Основні характеристики MITRE ATT&CK:

– Тактики – високорівневі цілі зловмисника (наприклад: Initial Access, Execution, Persistence, Privilege Escalation, Lateral Movement, Exfiltration).

– Техніки – конкретні методи досягнення цілей (наприклад: phishing, credential dumping, pass-the-hash, remote service exploitation).

– Підтехніки – деталізовані варіанти технік.

– Зв’язок з реальними інцидентами – база постійно оновлюється на основі аналізу атак відомих груп APT [8].

– Застосування у корпоративній безпеці:

– оцінка відповідності поточних засобів захисту актуальним методам атаки;

– моделювання атак (threat emulation);

– тестування стійкості систем (purple teaming);

– формування карти вразливих точок в інфраструктурі.

Завдяки MITRE ATT&CK організація може оцінити не лише наявні вразливості, а й реальні сценарії їх експлуатації, що значно підвищує точність моделювання ризиків.

Модель STRIDE, розроблена компанією Microsoft, використовується для класифікації загроз за типом впливу на систему (рис. 1.5).

Рис. 1.5 – Модель STRIDE

Назва є абревіатурою шести категорій загроз:

– S – Spoofing (підміна особи)

– T – Tampering (несанкціонована модифікація даних)

– R – Repudiation (відмова від дій / неможливість довести причетність)

– I – Information Disclosure (розголошення інформації)

– D – Denial of Service (відмова в обслуговуванні)

– E – Elevation of Privilege (підвищення привілеїв)

Особливості моделі STRIDE:

– орієнтована на аналіз впливу конкретної загрози на властивості інформаційної безпеки;

– легко інтегрується на етапі проєктування архітектури системи;

– дозволяє визначити, які контролі потрібні для кожного типу загроз;

– часто використовується разом із моделями DFD (Data Flow Diagrams) для виявлення слабких місць у взаємодії компонентів.

Модель STRIDE є зручною для оцінки ризиків на ранніх етапах створення інформаційних систем, оскільки дозволяє виявити слабкі місця ще до їхньої реалізації в інфраструктурі.

Обидві моделі виконують різні, але взаємодоповнювальні функції у процесі аналізу загроз. MITRE ATT&CK є орієнтованою на практику базою знань, що дозволяє досліджувати поведінкові патерни зловмисників, моделювати реалістичні сценарії атак та оцінювати ефективність наявних засобів захисту. Вона дає змогу зіставити конкретні техніки атаки з існуючими контрольними механізмами та визначити, наскільки інфраструктура готова до протидії сучасним загрозам.

У свою чергу, STRIDE зосереджується на виявленні потенційних загроз на рівні архітектури, логічних взаємодій та бізнес-процесів. Завдяки поділу загроз за типами впливу модель дає можливість системно проаналізувати слабкі місця на етапах проєктування, інтеграції та експлуатації компонентів корпоративної мережі. Таким чином, STRIDE використовується переважно для попереджувального аналізу, тоді як MITRE ATT&CK – для оцінювання практичної стійкості до реальних атак [9].

Оцінка вразливостей корпоративної інфраструктури є комплексним процесом, що охоплює технічні, організаційні, людські та архітектурні аспекти безпеки. Її проведення потребує використання як формальних моделей і методологій, так і практичних інструментів аналізу, що дозволяють виявляти слабкі місця та прогнозувати можливі сценарії їх експлуатації. Застосування моделей загроз, таких як MITRE ATT&CK і STRIDE, забезпечує всебічний погляд на ризики та дозволяє сформувати обґрунтовані пріоритети захисту. Оцінка вразливостей виступає фундаментальною передумовою для побудови ефективної системи мережевої безпеки, що визначає необхідність подальшого аналізу сучасних технологій та методів, розглянутих у наступному підрозділі.

1.3 Огляд сучасних технологій мережевої безпеки Firewall, IDS, IPS, SIEM

Зростання масштабів корпоративних мереж та ускладнення кіберзагроз зумовлюють потребу у впровадженні багаторівневих технологій захисту, здатних забезпечити безперервний контроль доступу, виявлення аномальної діяльності та оперативне реагування на інциденти. Традиційні засоби, орієнтовані лише на периметрову безпеку, вже не дозволяють ефективно протидіяти сучасним атакам, які охоплюють як зовнішні, так і внутрішні вектори проникнення. Тому сучасна система мережевої безпеки являє собою комплекс взаємопов'язаних рішень, серед яких ключову роль відіграють фаєрволи, системи виявлення та запобігання вторгненням, а також платформи централізованого аналізу подій безпеки. Ці технології формують основу кіберзахисту організації, забезпечуючи як превентивні, так і реактивні механізми протидії загрозам.

До базових механізмів мережевої безпеки, що тривалий час залишаються фундаментом захисту корпоративних інфраструктур, належать фаєрволи (Firewall), трансляція мережевих адрес (NAT) та віртуальні приватні мережі (VPN). Незважаючи на появу складних адаптивних рішень і поведінкових систем захисту, ці технології зберігають ключову роль у побудові безпечної мережевої архітектури, забезпечуючи периметровий контроль, захист від несанкціонованого доступу та безпечний віддалений зв'язок.

Firewall є основним інструментом контролю трафіку на межі корпоративної мережі. Він здійснює фільтрацію пакетів відповідно до визначених політик доступу, обмежує небажані з'єднання та запобігає проникненню зовнішніх загроз у внутрішній сегмент. Класичні фаєрволи працюють на мережевому та транспортному рівнях моделі OSI, аналізуючи IP-адреси, порти та протоколи. Вони забезпечують базову сегментацію мережі та створюють «першу лінію оборони», яка значно ускладнює несанкціоноване проникнення.

NAT (Network Address Translation) виконує трансляцію приватних внутрішніх IP-адрес у публічні адреси, що використовується для підвищення

безпеки та економії адресного простору (рис. 1.6). Хоча NAT не є засобом захисту у вузькому значенні, він приховує внутрішню структуру мережі та ускладнює прямий доступ до внутрішніх ресурсів із зовнішнього середовища. Завдяки ізоляційній природі NAT корпоративна мережа отримує додатковий рівень непрямого захисту, що знижує ризик прямої атаки на внутрішні вузли [10].

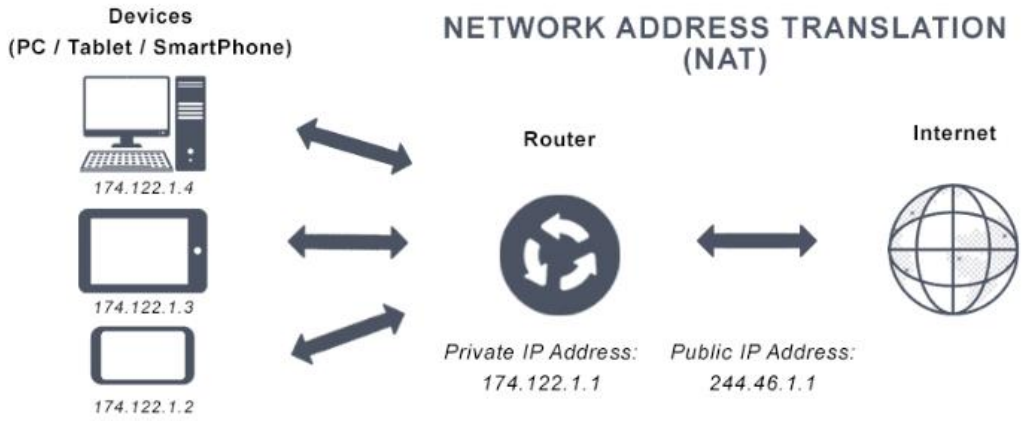

Рис. 1.6 – Приклад Network Address Translation

VPN (Virtual Private Network) забезпечує захищений канал передавання даних між віддаленими користувачами або філіями підприємства за допомогою криптографічних методів шифрування (рис. 1.7). Завдяки VPN організації можуть безпечно підключати співробітників до корпоративних ресурсів, навіть через ненадійні публічні мережі. VPN-технології, зокрема IPSec та SSL VPN, гарантують цілісність, конфіденційність і автентичність трафіку, що робить їх невід'ємною частиною сучасних інфраструктур віддаленого доступу.

Рис. 1.7 – Приклад Virtual Private Network

У сукупності firewall, NAT та VPN формують базовий захисний контур корпоративної мережі, забезпечуючи початкову ізоляцію, контроль доступу та конфіденційний зв’язок. Ці інструменти створюють основу, на якій вибудовуються більш складні та адаптивні системи сучасної мережевої безпеки.

SIEM (Security Information and Event Management) є централізованою платформою для збору, кореляції та аналізу подій безпеки з різних джерел – firewall, серверів, робочих станцій, мережевого обладнання, IDS/IPS та застосунків [11]. SIEM дозволяє поєднати розрізнені журнали подій у цілісну картину інцидентів, виявляти приховані зв’язки між подіями, визначати комплексні атаки та забезпечувати відповідність вимогам нормативних стандартів. Завдяки аналітичним модулям SIEM значно підвищує точність детекції й зменшує кількість хибних спрацювань.

EDR (Endpoint Detection and Response) та XDR (Extended Detection and Response) представляють нове покоління систем захисту, орієнтованих на кінцеві пристрої та комплексну видимість інфраструктури. EDR забезпечує постійний моніторинг поведінки кінцевих вузлів, виявляє шкідливу активність, а також надає можливість ізоляції заражених пристроїв і глибокої форензіки. XDR є розширеною моделлю, що об’єднує дані з кінцевих пристроїв, мережі, хмарних середовищ та поштових систем, створюючи єдиний контекст для аналізу загроз. Завдяки машинному навчанню та кореляції подій XDR дозволяє виявляти складні атаки, які непомітні для окремих традиційних інструментів.

У сукупності IDS, IPS, SIEM та EDR/XDR формують ядро сучасної архітектури захисту корпоративної мережі, забезпечуючи як виявлення й блокування атак, так і глибокий аналіз подій та автоматизоване реагування. Ці технології дозволяють організаціям ефективно протистояти багатовекторним і високотехнологічним загрозам, що визначає їх ключову роль у сучасній кібербезпеці.

Для забезпечення ефективного виявлення та запобігання мережевим атакам у сучасних інформаційних системах широко застосовуються рішення класу IDS/IPS, що ґрунтуються на сигнатурних, поведінкових та комбінованих методах

аналізу. У зв’язку з цим доцільним є проведення порівняльного аналізу найбільш поширених систем виявлення та запобігання вторгненням, зокрема Snort, Suricata, Zeek та Cisco Secure IDS. Такий аналіз дає змогу виокремити їх ключові технічні характеристики, оцінити функціональні можливості, визначити сфери доцільного застосування та встановити їх сильні й слабкі сторони. Порівняльна таблиця 1.2, що наведена нижче, узагальнює основні параметри цих систем та дозволяє встановити оптимальний інструмент залежно від вимог конкретної інфраструктури та специфіки мережевого середовища.

Таблиця. 1.2.

Порівняння основних систем IDS/IPS (Snort, Suricata, Zeek, Cisco Secure IDS)

Критерій	**Snort**	**Suricata**	**Zeek (Bro)**	**Cisco Secure IDS**
Тип системи	Система виявлення та запобігання вторгненням (IDS/IPS)	IDS/IPS	Система мережевого аналізу та моніторингу (IDS)	Комерційна IDS/IPS
Розробник	Cisco (раніше — Sourcefire)	Open Information Security Foundation (OISF)	Zeek Project	Cisco Systems
Ліцензування	Відкрите (open-source)	Відкрите (open-source)	Відкрите (open-source)	Пропрієтарне
Основний принцип роботи	Сигнатурне виявлення	Сигнатурне та поведінкове виявлення	Поглиблений аналіз трафіку та поведінкові методи	Комбіноване (сигнатурне, поведінкове, машинне навчання)
Продуктивність	Середня, залежить від архітектури	Висока, завдяки повній багатопотоковості	Висока у сфері аналітики логів	Дуже висока, оптимізована апаратними засобами
Багатопоточність	Частково (повноцінна у Snort 3)	Повна підтримка	Підтримується, але застосовується в іншій архітектурі	Повна
Метод аналізу	Сигнатурний	Сигнатурний + аномалії	Поведінковий аналіз, скрипти	Сигнатурний, аномалії, ML

Продовження таблиці. 1.2.

Підтримка протоколів	Широка	Дуже широка, включає глибоку інспекцію	Максимально широка, орієнтована на глибокий аналіз	Широка, включаючи корпоративні протоколи
Швидкість обробки трафіку	Середня	Вища за Snort у 2–4 рази	Не орієнтована на роботу в режимі IPS	Максимальна (апаратне прискорення)
Режим IPS	Підтримується	Підтримується	Не підтримується	Підтримується
Вимоги до ресурсів	Невисокі	Високі	Середні	Залежні від моделі обладнання
Гнучкість конфігурації	Висока	Дуже висока	Максимальна завдяки скриптовому підходу	Середня
Складність налаштування	Середня	Вище середнього	Висока (потребує програмування)	Низька для користувачів Cisco
Сфери застосування	Невеликі та середні мережі	Високонавантажені системи, SOC	Кіберфорензіка, аналітическі центри	Великі підприємства, державні структури
Основні переваги	Популярність, простота, наявність великої бази сигнатур	Висока швидкість, багатопоточність, сучасні алгоритми	Потужний поведінковий аналіз, детальний збір даних	Максимальний рівень захисту, інтеграція з інфраструктурою Cisco
Основні недоліки	Обмежена продуктивність без багатопоточності	Підвищені вимоги до ресурсів	Відсутність IPS-режиму та складна конфігурація	Висока вартість

Висновок до розділу 1

Проведений огляд щодо методів захисту корпоративних мереж дозволив зробити кілька ключових висновків. Класифікація кіберзагроз показала, що корпоративні мережі піддаються як внутрішнім, так і зовнішнім атакам, серед яких найбільш поширеними є шкідливе програмне забезпечення, фішинг, DDoS-атаки та несанкціонований доступ. Розуміння природи загроз є критичним для побудови ефективної стратегії захисту.

Оцінка вразливостей корпоративної інфраструктури виявила типові слабкі місця, такі як неправильна сегментація мережі, слабкі паролі, відсутність моніторингу та застаріле програмне забезпечення, що підкреслює необхідність регулярного аудиту та впровадження багаторівневого захисту.

Огляд сучасних технологій мережевої безпеки, включно з класичними засобами, такими як Firewall, та новітніми рішеннями, зокрема IDS, IPS, SIEM, EDR/XDR і принципами Zero Trust, показав, що комплексне поєднання різних підходів забезпечує ефективний захист корпоративних мереж. Використання політик безпеки, сегментації та багаторівневого захисту дозволяє суттєво зменшити ризик успішного впровадження атак.

Проведений аналіз підтвердив, що сучасна корпоративна мережа потребує інтегрованого підходу до кіберзахисту, який передбачає систематичну оцінку вразливостей, впровадження сучасних технологій безпеки та дотримання принципів багаторівневого захисту.

2 АНАЛІЗ І ТЕОРЕТИЧНІ ОСНОВИ IDS/IPS-СИСТЕМ

2.1 Класифікація та архітектура систем виявлення вторгнень

До ключових рішень, що формують основу багаторівневої моделі безпеки, належать системи виявлення та запобігання вторгненням (IDS та IPS), платформи централізованої аналітики подій безпеки (SIEM), а також сучасні інструменти захисту кінцевих пристроїв (EDR/XDR).

IDS (Intrusion Detection System) – це система, призначена для виявлення спроб несанкціонованого доступу або аномальної активності у мережевому трафіку чи на кінцевих пристроях. IDS може працювати на основі сигнатурного підходу, порівнюючи трафік із базою відомих атак, або на основі поведінкового аналізу, виявляючи відхилення від нормальної активності. Основною функцією IDS є ідентифікація інцидентів у режимі близькому до реального часу та сповіщення адміністратора для подальшого реагування [12].

IPS (Intrusion Prevention System) є логічним продовженням IDS, доповнюючи механізми виявлення можливістю автоматичного блокування шкідливої активності. IPS активно втручається в трафік, запобігаючи реалізації атак шляхом відхилення пакетів, завершення сесій або модифікації маршрутизації. Завдяки цьому IPS здатна зупиняти атаки ще на ранніх стадіях, мінімізуючи шкоду та знижуючи навантаження на інші засоби захисту. Сучасні IPS інтегрують функції аналізу протоколів, захисту вебдодатків та виявлення zero-day-атак за допомогою машинного навчання.

Системи виявлення та запобігання вторгнень (IDS та IPS) є компонентами сучасної стратегії забезпечення безпеки корпоративних мереж, проте вони відрізняються за своєю функціональною суттю та методами взаємодії з мережевим трафіком. IDS (Intrusion Detection System) є аналітичною системою, основним завданням якої є моніторинг мережевого та системного трафіку з метою виявлення потенційних загроз та підозрілих дій. Такі системи здійснюють порівняння аналізованих даних із сигнатурами відомих атак або використовують поведінковий

аналіз для ідентифікації аномалій. При цьому IDS носить пасивний характер, оскільки вона не втручається безпосередньо у мережеві процеси, а лише формує сповіщення для адміністратора безпеки або інтегрованих систем управління інцидентами. Такий підхід дозволяє організаціям отримувати своєчасну інформацію про потенційні загрози, проте не забезпечує автоматичного блокування атак.

На відміну від IDS, IPS (Intrusion Prevention System) виконує проактивну функцію захисту, поєднуючи можливості виявлення вторгнень із автоматичними заходами реагування. Системи IPS, зазвичай інтегровані безпосередньо в мережевий потік (in-line), здатні в реальному часі блокувати підозрілі пакети, розривати небезпечні з'єднання, змінювати правила доступу та запобігати поширенню атак на інші компоненти інфраструктури. Таким чином, IPS забезпечує активний захист мережі, зменшуючи час реагування на інциденти та потенційні втрати від успішних атак [13].

Основна концептуальна різниця між IDS та IPS полягає в характері їхньої взаємодії з мережевим середовищем: IDS виконує функцію виявлення та інформування, а IPS – виявлення та запобігання. У комплексних стратегіях кіберзахисту обидва підходи часто інтегруються для забезпечення багаторівневого моніторингу та управління загрозами, що дозволяє підвищити стійкість корпоративних мереж до сучасних кіберзагроз.

За принципом розташування та аналізованого середовища виділяють три основні типи систем. NIDS (Network-based Intrusion Detection System) призначені для моніторингу та аналізу мережевого трафіку. Вони встановлюються на ключових ділянках мережі, що дозволяє виявляти атаки, спрямовані на різні пристрої, та аналізувати взаємодію між ними. HIDS (Host-based Intrusion Detection System) функціонує на окремих кінцевих пристроях або серверах і здійснює контроль за системними журналами, процесами та змінами в критичних файлах, що дає змогу виявляти локальні атаки та внутрішні загрози. NBA (Network Behavior Analysis) системи зосереджуються на виявленні аномальної поведінки мережевого трафіку, аналізуючи відхилення від встановлених норм і шаблонів, що дозволяє

ідентифікувати нові або приховані загрози, які не визначаються традиційними методами [14].

За методами виявлення загроз системи поділяються на сигнатурні, поведінкові та гібридні. Сигнатурні системи працюють на основі бази відомих сигнатур атак і забезпечують високу точність при виявленні класичних атак, проте є обмеженими у виявленні нових загроз. Поведінкові системи аналізують типову поведінку користувачів та мережевого трафіку й ідентифікують відхилення, що може свідчити про аномалії або атаки нульового дня. Вони більш адаптивні, проте можуть генерувати більшу кількість помилкових спрацювань. Гібридні системи поєднують обидва підходи, що дозволяє досягти балансу між точністю та здатністю виявляти нові, раніше невідомі загрози.

2.2 Методи виявлення атак: сигнатурний, евристичний, поведінковий, гібридний

Сучасні системи виявлення та запобігання вторгнень використовують широкий спектр методів аналізу даних, що забезпечують багаторівневу оцінку безпеки мережі. Одним із найбільш традиційних підходів є сигнатурний метод (rule-based), який ґрунтується на використанні заздалегідь визначених правил та сигнатур відомих атак. Сигнатура являє собою унікальний шаблон шкідливої активності, що описує характерні ознаки конкретної атаки – структуру пакету, послідовність команд, характерний трафік або відомі експлойти [15]. Перевагою цього підходу є висока точність визначення загроз, які вже мають відповідні сигнатури, а недоліком – нездатність виявляти нові, невідомі атаки, особливо загрози нульового дня. Крім того, ефективність сигнатурних систем безпосередньо залежить від регулярності оновлення бази правил та швидкості реакції постачальника на появу нових вразливостей.

На відміну від сигнатурного підходу, поведінковий метод (anomaly detection) орієнтується на аналіз нормальної активності в мережі та виявлення відхилень від встановлених шаблонів. На основі попереднього навчання система формує модель

«нормальної» поведінки користувачів, серверів або мережевого трафіку, після чого фіксує аномалії: незвично великий потік даних, нехарактерні команди, підозрілу активність у нетиповий час тощо. Такий метод дозволяє ідентифікувати нові та невідомі атаки, але водночас може генерувати більшу кількість помилкових спрацювань через широкий спектр природних змін у поведінці системи. Поведінковий аналіз широко застосовується в NBA-системах та у сучасних EDR/XDR-платформах.

Подальший розвиток поведінкового аналізу привів до активного впровадження машинного навчання в IDS/IPS, що значно підвищує їхню здатність виявляти складні та раніше невідомі загрози. Алгоритми класифікації (SVM, Random Forest, нейронні мережі), методи кластеризації (K-means, DBSCAN), а також глибинне навчання дозволяють будувати адаптивні моделі, які самостійно навчаються на великому обсязі даних. Використання ML уможливлює автоматичне виявлення складних аномалій, в тому числі атаки з прихованими шаблонами, які неможливо зафіксувати традиційними методами. Проте застосування машинного навчання потребує значних обчислювальних ресурсів, якісних навчальних вибірок та постійної актуалізації моделей, що ускладнює впровадження таких рішень у великих корпоративних інфраструктурах.

Не менш важливим компонентом сучасних систем безпеки є методи кореляції подій, які дозволяють об’єднувати різні сигнали, журнали та повідомлення від IDS, IPS, SIEM, антивірусів, мережевих пристроїв та серверних систем у єдину аналітичну картину. Кореляція передбачає визначення взаємозв’язків між подіями, що окремо можуть не виглядати загрозливими, але разом формують чіткий індикатор атаки. Наприклад, неуспішна авторизація, за якою слідує підозріла активність у мережі та зміни у файловій системі, можуть свідчити про початок компрометації облікового запису. Завдяки кореляції підвищується точність виявлення атак, зменшується кількість false positives і забезпечується своєчасне виявлення складних, багатокрокових загроз (APT-кампаній).

Окрему категорію складає аналіз мережевого трафіку на основі DPI (Deep Packet Inspection), який дозволяє досліджувати не лише заголовки, а й вміст пакетів даних. На відміну від традиційного аналізу, DPI забезпечує глибокий перегляд переданої інформації, включаючи протоколи додатків, вміст повідомлень, файлів або HTTP-запитів. Це дозволяє ефективно виявляти складні атаки, приховані в легітимному трафіку, наприклад SQL Injection, XSS, шкідливі вкладення або обфускований код. DPI активно використовується у сучасних IPS, NGFW та системах захисту веб-додатків (WAF). Недоліками DPI є вплив на пропускну здатність мережі та підвищені вимоги до обчислювальних ресурсів, проте його ефективність у виявленні комплексних загроз робить цей метод незамінним у високонавантажених корпоративних системах [16].

2.3 Порівняння існуючих IDS/IPS (Snort, Suricata, Zeek, Cisco Secure IDS)

Від часу появи перших систем виявлення та запобігання вторгненням минуло багато років, і за цей період було створено значну кількість рішень, що відрізняються підходами, архітектурою та рівнем доступності. Сучасні IDS/IPS активно розвиваються, орієнтуючись на зменшення кількості хибних спрацювань та підвищення загальної ефективності роботи. Наслідком такого розвитку стало формування класу систем NGIPS (Next Generation Intrusion Prevention System) - систем нового покоління, здатних виконувати повний спектр функцій у режимі реального часу.

Особливістю NGIPS є те, що їх робота не створює додаткового навантаження на мережеву інфраструктуру та не знижує продуктивність мережі підприємства. Окрім цього, рішення нового покоління підтримують розширений моніторинг застосунків та можуть інтегруватися зі сторонніми базами даних вразливостей, що значно підвищує їхню ефективність у виявленні сучасних кіберзагроз.

У подальшому розділі буде детально проаналізовано найбільш поширені на сьогодні системи IDS/IPS, а також розглянуто особливості їх розгортання та інтеграції в цільову мережеву інфраструктуру [14].

1. StoneGate Intrusion Prevention System

Розробник: StoneSoft Corporation

Офіційний сайт: www.stonesoft.com

Тип реалізації: програмно-апаратний комплекс, доступний також як образ VMware

Підтримувані ОС: 32/64-бітові Windows (2003, Vista, 7, 2008R2), Linux (CentOS, RHEL, SLES)

Модель ліцензування: комерційна

Сучасні мережеві інфраструктури потребують більш складних та багаторівневих засобів захисту, ніж один лише фаєрвол. Прості методи фільтрації портів уже давно не забезпечують належного рівня кібербезпеки, оскільки сучасні атаки стають дедалі складнішими, комбінованими та здатними обходити базові механізми захисту. Саме це й спричинило активний розвиток систем запобігання вторгненням, що поєднують кілька методів аналізу трафіку [17].

Попри те, що на ринку існує велика кількість як програмних, так і апаратних рішень, багато з них орієнтуються лише на базовий сигнатурний аналіз та здатні ідентифікувати лише найпростіші види атак. Їх ефективність значною мірою залежить від актуальності сигнатур, у яких описано характерні шаблони шкідливого трафіку.

Однак це твердження не стосується **StoneGate Intrusion Prevention System**, розробленої компанією StoneSoft. Це комплексне корпоративне рішення, призначене для протидії широкому спектру атак. Система відзначається розширеною функціональністю та здатністю забезпечувати високий рівень кіберзахисту в режимі реального часу.

Функціональні можливості StoneGate IPS

StoneGate IPS пропонує широкий набір можливостей, серед яких:

– аналіз та шифрування мережевого трафіку;
– веб-фільтрація із застосуванням постійно актуалізованої бази сайтів;
– захист від DDoS-атак;

– виявлення та блокування експлойтів, спрямованих на вразливості ПЗ та мережевого обладнання;

– протидія складним технікам обходу безпеки;

– блокування вірусів, spyware, небажаних програм (P2P, IM тощо).

Особливої уваги в системі приділено захисту від **AET - Advanced Evasion Techniques**. Це сучасний клас атак, у яких шкідливий трафік модифікується або маскується так, щоб уникнути виявлення традиційними системами IDS/IPS. Фахівці StoneSoft провели ґрунтовні дослідження в цій галузі та інтегрували у продукт механізми протидії подібним технікам, що суттєво підвищує рівень захисту корпоративних мереж.

Загальна характеристика

StoneGate IPS створена фінською компанією, яка спеціалізується на розробці корпоративних рішень для мережевої безпеки. Програмно-апаратний комплекс поєднує у собі всі ключові функції сучасної системи захисту:

– глибокий аналіз трафіку,

– веб-фільтрацію,

– роботу із зашифрованими даними,

– протидію DDoS та 0-day атакам,

– виявлення та нейтралізацію складних загроз.

Унікальні механізми ідентифікації загроз та здатність приймати автоматичні рішення щодо їх нейтралізації роблять StoneGate IPS одним із найпотужніших комерційних рішень для корпоративних мереж [14].

Для поділу корпоративної мережі на кілька логічних сегментів у StoneGate IPS використовується технологія Transparent Access Control. Її перевага полягає в тому, що реальна фізична топологія мережі залишається незмінною, а кожен віртуальний сегмент може отримати власний набір політик безпеки. Формування таких політик відбувається в офлайн-режимі із застосуванням вбудованих шаблонів, які містять типові правила аналізу трафіку. Після створення профілів адміністратор перевіряє їх коректність і надсилає на віддалені вузли IPS.

StoneGate IPS аналізує події, що є схожими за структурою чи поведінкою, за принципами, притаманними системам класу SIM/SIEM. Такий підхід значно спрощує процес обробки інцидентів та підвищує ефективність аналізу мережевого трафіку [18].

Інтеграція та керування інфраструктурою StoneSoft

Однією з ключових переваг рішень StoneSoft є можливість об'єднання кількох пристроїв у кластер, а також їх інтеграція з іншими продуктами компанії, такими як [14]:

– StoneGate Firewall/VPN,
– StoneGate SSL VPN.

Це дозволяє сформувати єдину екосистему мережевої безпеки, якою можна централізовано керувати через StoneGate Management Center. Дана консоль складається з трьох основних компонентів:

1. Log Server – збирання та зберігання журналів подій;
2. Management Server – керування політиками та конфігураціями;
3. Management Client – клієнтська частина для роботи адміністратора.

Оскільки консоль реалізована на Java, вона може працювати як у Windows-, так і в Linux-середовищі. Через Management Center адміністратор має доступ до моніторингу мережі в режимі реального часу, перегляду журналів, управління обладнанням та створення нових політик безпеки.

Варіанти розгортання

StoneGate IPS доступна не лише як апаратний комплекс, але і як віртуальний VMware-образ, що дозволяє розгортати її на власних серверах підприємства або в будь-якому сучасному віртуальному середовищі.

Переваги інтеграції

Суттєвою перевагою даного рішення є можливість формування єдиної системи захисту, яка складається з різних компонентів StoneSoft. Така інтеграція забезпечується централізованою консоллю керування та дозволяє:

– більш ефективно будувати архітектуру безпеки,
– централізовано керувати конфігураціями,

– виконувати оновлення всіх компонентів,

– оптимізувати взаємодію між елементами мережевої безпеки.

У сукупності ці можливості роблять StoneGate IPS потужним та гнучким рішенням для корпоративних мереж з підвищеними вимогами до захисту.

Застосування єдиної інтегрованої платформи безпеки, такої як StoneGate IPS, є значно надійнішим підходом порівняно з побудовою мережевого периметру на базі обладнання та програмного забезпечення від різних виробників. Використання різних несумісних рішень ускладнює керування системою захисту та збільшує витрати на її підтримку, тоді як єдина екосистема StoneGate забезпечує спрощення адміністрування та економію ресурсів [19].

Система запобігання вторгненням StoneGate IPS доступна у двох основних формах – як програмне рішення та як апаратний комплекс. Апаратні моделі мають однакову архітектуру та функціонал, але відрізняються пропускною здатністю й оптимізовані для мереж різного масштабу. Програмна версія призначена для інсталяції на серверне обладнання будь-якого виробника або для роботи у віртуальних середовищах.

Функціональні можливості StoneGate IPS для корпоративного захисту

StoneGate IPS забезпечує комплексний контроль внутрішнього трафіку та здатна блокувати підозрілу діяльність, що надходить з корпоративних робочих станцій. Це дозволяє ефективно нейтралізовувати загрози, які можуть виникнути вже всередині організації, а не лише на мережевому периметрі.

Система включає механізми захисту від атак нульового дня, а також містить розвинений набір інструментів для протидії DDoS-атакам, спрямованим на корпоративні сервіси. Завдяки цьому забезпечується безперервність функціонування мережі та мінімізується ризик відмови в обслуговуванні.

Одним із ключових компонентів StoneGate IPS є система виявлення складних методів обходу безпеки. Вона інтегрує у процес інспекції трафіку власний механізм нормалізації, що працює на всіх рівнях мережевої моделі та унеможливлює використання технік ухилення з боку зловмисників.

Веб-фільтрація та контроль користувацької активності

Окрему роль у забезпеченні безпеки відіграє вбудована веб-фільтрація. Цей механізм дозволяє адміністраторам блокувати доступ до небажаних сайтів та вебресурсів. Система використовує велику, постійно оновлювану базу вебсайтів, класифікованих за категоріями, що підвищує точність фільтрації. Крім підвищення рівня кіберзахисту, веб-фільтрація має й організаційний ефект – вона допомагає зменшити кількість відволікань працівників, блокуючи ресурси, що негативно впливають на їх продуктивність.

Щоб відповідати сучасним вимогам до мережевої безпеки, система StoneGate IPS підтримує роботу з протоколом IPv6, що забезпечує сумісність із новими мережевими стандартами. Крім того, рішення включає повноцінну підтримку протоколів SSL/TLS, що дає змогу аналізувати та контролювати зашифрований трафік. Це означає, що система здатна виявляти та блокувати атаки, які реалізуються через протокол HTTPS, що особливо важливо для сучасних корпоративних мереж, у яких шифрування застосовується повсюдно.

Можливості моніторингу та контролю трафіку

StoneGate IPS має у своєму складі спеціалізовані інструменти, які надають адміністраторам розширені можливості контролю активності в мережі. Завдяки цим механізмам можна чітко визначити, який трафік належить бізнес-критичним додаткам, а який є несуттєвим або небажаним. На основі таких даних адміністратор може блокувати певні потоки трафіку з метою оптимізації навантаження на мережу й підвищення її продуктивності.

Режими роботи: IDS та IPS

Система StoneGate IPS може працювати в одному з двох основних режимів:

1. IDS (Intrusion Detection System) – виконує пасивний моніторинг і виявляє аномалії чи спроби вторгнення, сповіщаючи адміністратора.

2. IPS (Intrusion Prevention System) – не лише аналізує трафік, але й здійснює активні дії при виявленні загроз: блокує атаки, ізолює небезпечну активність та запобігає поширенню шкідливого коду.

Під час інтеграції StoneGate IPS з іншими продуктами компанії створюється комплексна система багаторівневого захисту, орієнтована на повну протидію сучасним кіберзагрозам.

Технологія Transparent Access Control

Окремо варто відзначити технологію Transparent Access Control. Вона дозволяє розділити велику корпоративну мережу на окремі віртуальні сегменти без зміни її фізичної структури. Для кожного сегменту можна встановити власні політики доступу та безпеки, що дає змогу більш точно контролювати трафік і локалізувати потенційні загрози.

Аналізатор подій та зменшення хибних спрацювань

Для обробки всієї інформації, яку надсилають сенсори системи, застосовуються інтелектуальні механізми аналізу. Вони збирають дані з різних джерел у єдиному центрі обробки та виконують пошук підозрілих сигнатур і шаблонів. Такий підхід дозволяє суттєво зменшити кількість хибних спрацювань, оскільки аналіз відбувається комплексно, з урахуванням контексту подій у мережі.

Масштабованість та кластеризація

Однією з ключових переваг StoneGate IPS є можливість легкого масштабування. За необхідності підприємство може під’єднувати додаткові вузли або апаратні модулі, створюючи нові кластери. Це дозволяє розширювати систему без негативного впливу на вже працююче обладнання і без простоїв мережі.

Консоль управління та адміністрування

За допомогою єдиної консолі адміністратор може здійснювати:

- моніторинг стану системи в реальному часі,
- аналіз роботи окремих вузлів,
- формування звітів у текстовому та графічному вигляді,
- налаштування політик безпеки,
- управління журналами подій,
- дослідження зареєстрованих інцидентів.

Таким чином, система надає широкий спектр можливостей для централізованого керування та спрощує виконання обов’язків адміністратора, роблячи процес контролю загроз більш ефективним і зручним.

IBM Security Network Intrusion Prevention System

Розробник: IBM

Офіційний сайт: https://www.ibm.com/

Тип реалізації: програмно-апаратний комплекс, доступний також у вигляді VMware-образу

Ліцензія: комерційна

Система IBM Security Network Intrusion Prevention System створена для виявлення та нейтралізації атак, спрямованих на корпоративну мережу підприємства, а також для виконання аудиту її безпеки. Висока ефективність рішення забезпечується завдяки використанню унікальної технології аналізу протоколів, розробленої IBM. Ця технологія дозволяє підтримувати постійний активний захист мережевої інфраструктури від широкого спектру загроз.

Архітектура та ключові технології

IBM впровадила власну унікальну технологію поглибленого аналізу протоколів, на основі якої побудовано модульну архітектуру системи. Центральним компонентом є Protocol Analysis Module, який об’єднує два підходи:

– сигнатурне виявлення;

– поведінковий аналіз.

Завдяки цьому модуль здатний розпізнавати кілька сотень протоколів прикладного рівня та найпоширеніші формати даних. Такий підхід дозволяє виявляти навіть складний та прихований шкідливий код. Аналіз мережевого трафіку включає використання більш ніж 3000 алгоритмів, з яких понад 200 призначені для виявлення DoS-атак.

У склад системи також входить вбудований брандмауер, що забезпечує контроль доступу на рівні портів і IP-адрес, підвищуючи загальний рівень мережевого захисту.

Функції захисту та виявлення загроз

Однією з важливих можливостей системи є технологія Virtual Patch, що дозволяє:

– блокувати віруси на етапі їх поширення;

– тимчасово захищати мережу до установлення оновлень безпеки;

– створювати власні сигнатури у разі потреби.

Крім того, IBM IPS містить модуль контролю застосунків, який дає змогу заблокувати окремі програми при виявленні небезпечної активності.

Додатково інтегровано модуль DLP (Data Loss Prevention), який контролює спроби передачі конфіденційних даних та їх переміщення всередині корпоративної мережі. Це дозволяє виявляти можливі витоки інформації ще на ранніх етапах.

Зважаючи на те, що веб-додатки залишаються однією з найбільш уразливих точок інфраструктури, IBM оснастила систему спеціальним модулем захисту вебрівня, який протидіє найпоширенішим типам атак на вебзастосунки.

Механізми реагування та гнучкість налаштувань

У разі виявлення атаки система підтримує кілька варіантів реагування:

– блокування джерела (хоста),

– надсилання попередження,

– детальне логування трафіку під час інциденту,

– ізоляція компрометованого вузла мережі.

Політики безпеки можна гнучко налаштовувати як на рівні окремих IP-адрес, так і для цілих VLAN-сегментів, що забезпечує високий ступінь адаптивності системи.

Система також підтримує спеціальний режим безперервної роботи: навіть у разі виходу з ладу одного з компонентів, IPS продовжує функціонувати без збоїв.

Інтеграція з екосистемою IBM

Якщо у корпоративній інфраструктурі використовується кілька продуктів IBM, їх можна об’єднати в єдину централізовану систему керування. Це спрощує моніторинг, оптимізує процеси реагування та підвищує загальну ефективність системи безпеки.

Превентивний характер захисту в IBM Security Network Intrusion Prevention System ґрунтується на безперервному моніторингу різноманітних загроз, що здійснюється у спеціалізованому центрі безпеки GTOC (Global Threat Operations Center), розташованому за адресою gtoc.iss.net. Такий підхід забезпечує оперативне виявлення нових атак та формування актуальних сигнатур.

Основні можливості IBM Security Network Intrusion Prevention System

Система має широкий набір функцій, серед яких:

– Підтримка 167 різних протоколів, включно з протоколами прикладного рівня та різноманітними форматами даних.

– Використання понад 2500 алгоритмів аналізу трафіку для виявлення вразливостей і шкідливих дій.

– Технологія Virtual Patch, яка дозволяє забезпечувати захист до встановлення офіційних оновлень.

– Наявність вбудованого пасивного режиму моніторингу та двох режимів підключення в канал передачі даних.

– Підтримка декількох зон безпеки на одному пристрої, включаючи VLAN-сегменти.

– Інтеграція вбудованих та зовнішніх bypass-модулів, які забезпечують безперервну передачу даних у разі технічної помилки або відключення живлення.

– Використання сучасної технології FlowSmart, що оптимізує обробку трафіку.

– Великий вибір механізмів реагування на події, включно з детальним логуванням пакетів, що містять ознаки атаки.

– Контроль витоків інформації у даних та офісних документах, що передаються через пірингові мережі, месенджери, вебпошту та інші протоколи.

Переваги використання IBM Security Network IPS

Використання цього рішення надає низку суттєвих переваг:

– Превентивний захист дозволяє блокувати атаки на ранніх стадіях, унеможливлюючи несанкціонований доступ до критичних ресурсів і служб компанії.

– Система формує детальні звіти та архіви подій, що надають повну картину стану мережевої безпеки. Ці дані допомагають відповідати вимогам сучасних стандартів кібербезпеки та спрощують аудит.

McAfee Network Security Platform 7

Розробник: McAfee Inc.

Офіційний сайт: www.mcafee.com

Тип реалізації: програмно-апаратний комплекс

Ліцензія: комерційна

McAfee Network Security Platform (NSP) є сучасною системою запобігання вторгненням, яка використовує багаторівневий підхід до аналізу мережевого трафіку. В її основі поєднані сигнатурні та безсигнатурні методи, що дозволяє ефективно реагувати на широкий спектр загроз. Для оцінки типових моделей атак система застосовує інтелектуальні алгоритми, які полегшують роботу спеціалістів з інформаційної безпеки та зменшують час на реагування. Значна кількість процесів у McAfee NSP автоматизована, що забезпечує оперативне і точне усунення загроз [20].

Побудована на основі технологій IntruShield IPS, сьома версія McAfee Network Security Platform отримала як переваги свого попередника, так і низку принципово нових можливостей. Рішення надає широкий вибір інструментів для глибокого аналізу мережевого трафіку, здатне швидко виділяти небезпечні пакети та здійснювати негайну реакцію на інциденти.

Глобальний інтелект загроз та можливості аналітики

В основі McAfee NSP лежить технологія Global Threat Intelligence, яка дозволяє оцінювати надійність IP-адрес, посилань або протоколів на основі інформації, отриманої з сотень вузлів по всьому світу. Це забезпечує:

– виявлення підозрілого трафіку;

– ідентифікацію загроз нульового дня;

– розпізнавання різних типів атак;

– мінімізацію хибних спрацювань.

Така глобальна база знань дозволяє системі оперативно адаптуватися до нових моделей кібератак та підтримувати високий рівень превентивного захисту.

Захист у фізичних та віртуальних середовищах

Однією з важливих функцій McAfee NSP є можливість аналізувати трафік:

– між віртуальними машинами,

– між віртуальною машиною та фізичним сервером.

Для реалізації цієї можливості використовується модуль компанії Reflex Systems, який відстежує активність віртуальних вузлів і передає інформацію на фізичний хост. Це дозволяє ефективно контролювати безпеку в складних гібридних інфраструктурах.

Хостовий захист

Окрім мережевого рішення, McAfee також пропонує хостову систему Host Intrusion Prevention for Desktop, яка забезпечує комплексний захист робочих станцій. Вона аналізує трафік, з'єднання, поведінку додатків і блокує потенційні атаки на рівні окремого ПК.

Можливості виявлення та реагування

У порівнянні з іншими IPS-системами McAfee NSP забезпечує захист від найсерйозніших категорій загроз, включаючи:

– атаки нульового дня,

– DoS і DDoS атаки,

– складні інструменти обходу безпеки.

Єдиний модуль системи містить засоби:

– для запобігання вторгненням,

– для збору та аналізу даних про мережеві додатки,

– для моніторингу поведінкових аномалій.

Система корелює отриману інформацію з даними сьомого рівня моделі OSI, що забезпечує глибоку інспекцію трафіку.

Пошук аномалій та виявлення шкідливих вузлів

McAfee NSP включає модулі поведінкового аналізу, які:

– виявляють підозрілі пристрої,

– ідентифікують аномалії в мережевій активності,

– здатні знаходити бот-мережі або заражені вузли.

Це істотно підвищує точність визначення загроз, які можуть залишитися непоміченими традиційними сигнатурними методами.

Переваги архітектури Security Connected

Завдяки архітектурі Security Connected система має змогу у реальному часі обмінюватися даними з іншими продуктами компанії McAfee. Це дає можливість:

– оперативно оновлювати сигнатури та правила;

– використовувати централізований підхід до управління загрозами;

– підвищувати ефективність захисту порівняно з використанням рішень від різних виробників.

McAfee Network Security Platform здатна обробляти трафік на швидкості до 40 Гбіт/с, що досягається завдяки використанню потужної апаратної платформи операторського рівня. Система поєднує високопродуктивне обладнання та механізми однопрохідної (single-pass) обробки трафіку, що забезпечує максимальну швидкість аналізу без втрати точності.

Компоненти McAfee NSP

McAfee NSP складається з кількох ключових модулів, кожен з яких виконує свою функцію у загальній архітектурі:

1. Network Security Sensor (сенсор)

Виконує основні завдання IDS/IPS: аналізує мережевий трафік, виявляє загрози та блокує атаки в реальному часі.

2. Network Security Manager (менеджер)

Централізований компонент, який забезпечує конфігурацію системи, управління політиками, формування звітів та інтеграцію з іншими продуктами McAfee.

3. McAfee Update Server (сервер оновлень)

Відповідає за оперативне оновлення сигнатур, правил, шаблонів та всіх необхідних компонентів системи.

Переваги McAfee Network Security Platform

Система вирізняється рядом важливих переваг, які визначають її ефективність і надійність:

1. Поєднання сигнатурних та безсигнатурних методів аналізу

Забезпечує комплексний захист: NSP виконує повну інспекцію трафіку, перевіряє понад півтори тисячі мережевих протоколів і застосунків, а також блокує шкідливий код.

2. Розширений аналіз, кореляція подій та обмін інформацією

Завдяки архітектурі *McAfee Security Connected* система може інтегруватися з іншими продуктами компанії, створюючи єдине середовище безпеки.

3. Висока швидкість виявлення загроз

Завдяки вбудованим механізмам та процесам система швидко ідентифікує вразливості, аномалії та атаки, зводячи до мінімуму хибні спрацювання.

4. Машинне навчання та евристичні методи

Дозволяють ефективно протидіяти DoS і DDoS атакам, а також обмежувати кількість з’єднань з конкретними серверами та хостами.

5. Незалежність пропускної здатності від складності конфігурацій

На відміну від деяких інших систем, продуктивність McAfee NSP не знижується при використанні великої кількості складних політик - навіть у таких випадках пропускна здатність залишається стабільно високою.

6. Висока продуктивність при аналізі SSL-з’єднань

Система демонструє одні з найкращих результатів на ринку під час обробки зашифрованого трафіку.

Suricata

Розробник: Open Information Security Foundation (OISF)

Офіційний сайт: www.openinfosecfoundation.org

Тип реалізації: програмна платформа

Підтримувані ОС: Linux, *BSD, macOS, Solaris, Windows/Cygwin

Ліцензія: GNU GPL

У 2010 році OISF представила систему Suricata – сучасну IDS/IPS, розробка якої тривала три роки та включала створення нових методів виявлення атак.

Подібно до інших систем виявлення вторгнень, Suricata використовує правила, на основі яких здійснюється аналіз підозрілої активності. Адміністратор може:

– підключати готові набори правил,
– використовувати правила інших IDS/IPS,
– створювати власні сигнатури.

На ранніх етапах розвитку існували проблеми сумісності правил Suricata з наборами правил Snort та інших систем, проте з часом ці труднощі були усунені.

Формат правил Suricata

Розробники створили власний формат, який за структурою нагадує правила Snort, але має розширену функціональність. Правило складається з:

1. Дії (pass, drop, reject, alert)
2. Заголовка (IP/порт джерела і призначення)
3. Опису, який визначає критерії пошуку

Ключовою перевагою Suricata є можливість аналізувати дані безпосередньо з потоку трафіку, ще до повного завершення передачі пакета. Це дає змогу фіксувати шкідливу активність на початковому етапі атаки та оперативно реагувати. Такий підхід робить Suricata більш ефективною в порівнянні зі Snort.

Оцінка системи

З урахуванням перелічених характеристик Suricata часто розглядається як швидша та продуктивніша альтернатива Snort. Основним недоліком є обмежений обсяг документації, що ускладнює процес налаштування для користувачів без попереднього досвіду.

Samhain

Розробник: Samhain Labs

Офіційний сайт: www.la-samhna.de/samhain

Тип реалізації: програмна

Підтримувані ОС: Unix, Linux, Windows/Cygwin

Ліцензія: GNU GPL

Samhain – це система з відкритим вихідним кодом, призначена для захисту хостів, на яких розгорнута IDS. Метою цього продукту є моніторинг цілісності

системи та виявлення підозрілих змін на рівні файлової системи й системних процесів. Для цього застосовується комплекс аналітичних методів.

Функціональні можливості Samhain

Система забезпечує:

– створення бази сигнатур важливих файлів під час першого запуску та подальше порівняння з поточним станом;
– моніторинг та аналіз записів системних журналів;
– контроль входів та виходів користувачів із системи;
– спостереження за підключеннями до відкритих мережевих портів;
– виявлення прихованих процесів і контроль файлів із прапором SUID.

Однією з унікальних характеристик Samhain є режим невидимості. При його активації процеси, що виконуються на ядрі ОС, не відображаються у пам’яті, що ускладнює можливість їх приховування або модифікації зловмисниками.

Архітектура та моніторинг у мережі

Samhain підтримує можливість централізованого моніторингу кількох вузлів одночасно, незалежно від їх операційних систем. Усі події передаються на єдиний сервер через захищений канал, де відбувається їх обробка та запис у базу даних.

Сервер також:

– надсилає оновлення,
– передає змінені конфігураційні файли,
– синхронізує налаштування на клієнтських хостах.

Сумісність

Продукт орієнтований передусім на Linux-системи, з повною підтримкою більшості дистрибутивів. Також передбачена можливість використання у середовищі Windows через Cygwin.

2.4 Інтеграція IDS/IPS у корпоративні мережі та взаємодія з SIEM

Ефективне впровадження систем виявлення та запобігання вторгненням (IDS/IPS) у корпоративні мережі потребує комплексного підходу, що охоплює не

лише технічні аспекти розгортання, а й їхній подальший взаємозв’язок з іншими складовими інфраструктури інформаційної безпеки. Одним із ключових елементів такої взаємодії є інтеграція IDS/IPS із системами управління інформаційною безпекою та подіями (SIEM – Security Information and Event Management) [21].

У сучасних корпоративних мережах IDS/IPS виконують роль першої лінії оборони, здійснюючи глибоку інспекцію трафіку, виявляючи аномалії та блокуючи підозрілу активність у режимі реального часу. Однак навіть найпотужніша IPS-система не здатна повноцінно забезпечити аналіз усіх подій у мережі без централізованого узгодження даних. Саме тому інтеграція із SIEM-рішеннями дозволяє значно підвищити рівень видимості, кореляції та реагування на інциденти.

Роль IDS/IPS в архітектурі корпоративної безпеки

У корпоративних мережах IDS/IPS можуть бути розміщені:

– на периметрі мережі для контролю зовнішніх загроз,

– у внутрішніх сегментах для виявлення латерального поширення атак,

– у віртуальних середовищах та хмарах для контролю міжвіртуального трафіку,

– у критичних зонах (дата-центри, серверні сегменти, DMZ).

Правильний вибір місця розташування системи дозволяє оптимізувати моніторинг, мінімізувати «сліпі зони» та підвищити точність виявлення атак.

Взаємодія з SIEM: ключові переваги

Об’єднання IDS/IPS із SIEM забезпечує:

– кореляцію подій на різних рівнях – від мережевого трафіку до дій користувачів;

– зниження кількості хибних спрацювань шляхом порівняння подій між різними джерелами;

– створення повної картини інциденту, включно з хронологією, джерелами, каналами поширення та впливом;

– централізоване управління політиками безпеки та автоматизацію реагування;

– відповідність вимогам стандартів безпеки, таких як ISO 27001, PCI DSS та ін.

SIEM отримує дані від IDS/IPS у вигляді журналів, сигнатурних спрацювань, метаданих про трафік, попереджень щодо поведінкових аномалій тощо. Завдяки потужним механізмам кореляції SIEM здатний поєднувати ці дані з іншими джерелами - журналами серверів, даними з фаєрволів, проксі, антивірусів, систем контролю доступу тощо.

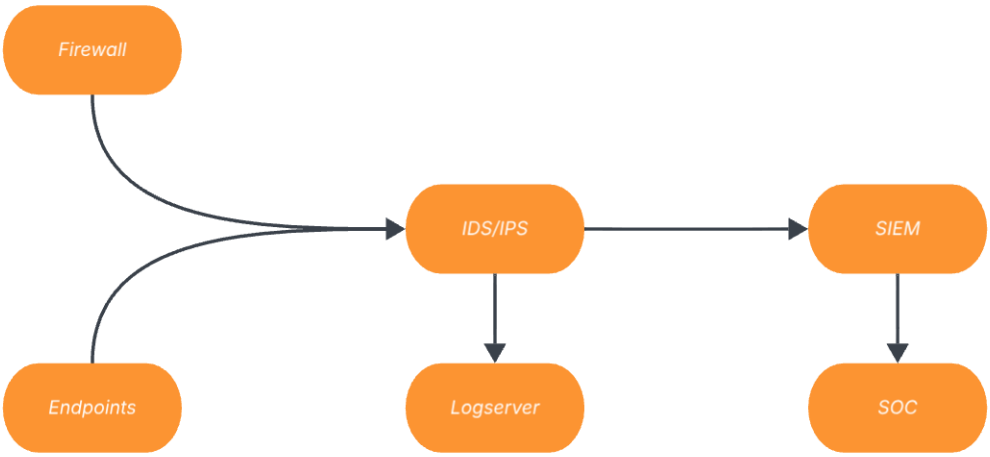

Рис. 2.1 Схема інтеграції IDS/IPS із SIEM»

Висновок до розділу 2

Проведено комплексний аналіз теоретичних основ функціонування систем виявлення та запобігання вторгненням (IDS/IPS), що є ключовими елементами сучасної інфраструктури кібербезпеки корпоративних мереж. Розглянуто класифікацію IDS/IPS за архітектурними принципами, функціональними можливостями та сценаріями застосування. Детально описано сигнатурний, евристичний, поведінковий та гібридний підходи до виявлення атак, що дозволило визначити їх сильні та слабкі сторони в контексті протидії сучасним кібератакам різного рівня складності.

Проведене порівняння поширених IDS/IPS-рішень – Snort, Suricata, Zeek, Cisco Secure IDS, StoneGate IPS, IBM Security NIPS та McAfee NSP – показало, що кожна система має власні переваги та сфери застосування. Snort вирізняється гнучкістю, відкритим кодом і широкою підтримкою спільноти, тоді як Suricata демонструє вищу продуктивність завдяки багатопотоковій обробці. Промислові рішення на кшталт Cisco, IBM та McAfee забезпечують розширені можливості поведінкового аналізу, кореляції подій, масштабованості та інтеграції в корпоративні екосистеми. Особливої уваги заслуговують системи класу NGIPS, орієнтовані на обробку зашифрованого трафіку, захист від AET-технік та мінімізацію хибних спрацювань.

Досліджено аспекти інтеграції IDS/IPS з платформами SIEM, що є критично важливим для формування комплексної системи моніторингу та реагування на інциденти. Встановлено, що об’єднання IDS/IPS із SIEM забезпечує повноцінну кореляцію подій з різних джерел, покращує точність виявлення атак, зменшує кількість хибнопозитивних спрацювань та підвищує ефективність автоматизованого реагування. Така взаємодія дозволяє отримати цілісне уявлення про безпековий стан корпоративної мережі та оперативно локалізувати загрози.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД ВНУТРІШНІХ ТА ЗОВНІШНІХ КІБЕРАТАК

3.1 Варіант технології розгортання Snort IDS/IPS

У межах розв’язання поставленої задачі – налаштування на персональному комп’ютері системи виявлення та запобігання вторгненням (IDS/IPS) – було обрано програмний комплекс **Snort**. Такий вибір зумовлений рядом переваг: наявністю безкоштовної версії, можливістю встановлення на операційні системи сімейства Windows, а також невисокими вимогами до апаратного забезпечення. Варто підкреслити, що Snort підтримує роботу як у Linux-середовищі, так і під Windows, проте для цілей даної роботи інсталяція здійснювалася на комп’ютер із операційною системою Windows [18].

Технічні характеристики середовища

Для реалізації проєкту було використано таку конфігурацію обладнання та ПЗ:

– Операційна система: Windows 10 (версія 19042)

– Апаратні характеристики: процесор Intel Pentium N4200, 4 GB оперативної пам’яті

– Версія Snort: 2.9.17.1

Особливості процесу розгортання

Інсталяція Snort у середовищі Windows є багатоступеневим процесом і вимагає від користувача уважності та розуміння низки додаткових налаштувань. Для недосвідчених користувачів така процедура може бути складною, що підвищує ймовірність помилок під час встановлення. З огляду на це було вирішено автоматизувати більшість рутинних дій створенням спеціального **bat-скрипта**, який виконує основні етапи інсталяції. Попри це, деякі операції залишаються такими, що потребують ручного втручання та не піддаються повній автоматизації [22].

Підготовчий етап

Перед запуском скрипта необхідно було сформувати робочу директорію, розмістивши в ній усі файли та інсталятори, потрібні для подальшої роботи Snort.

До переліку таких компонентів увійшли:

– архіватор **7-Zip** (версія 19.00);
– пакет захоплення мережевого трафіку **Npcap** (версія 0.9984);
– дистрибутив **Snort 2.9.17.1**;
– архів із правилами для відповідної версії Snort;
– попередньо підготовлений файл конфігурації Snort;
– bat-скрипт, що автоматизує процес інсталяції [18].

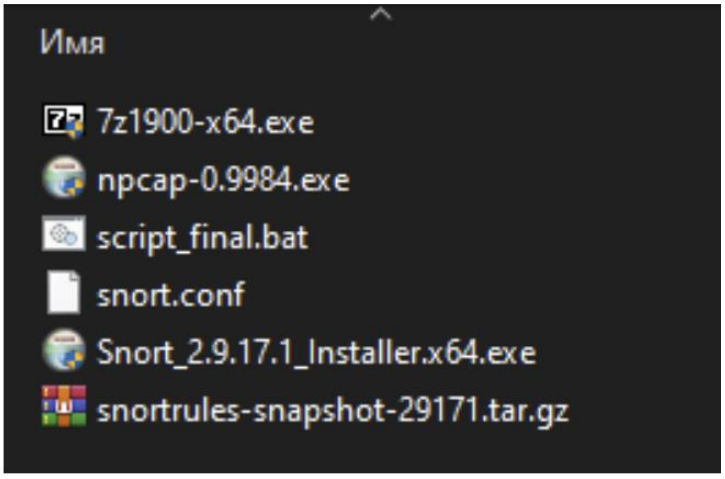

Рис. 3.3 Робоча директорія, що містить інсталятори та інсталяційний скрипт

Після розміщення всіх необхідних інсталяторів та службових файлів у єдиній робочій директорії наступним кроком є внесення змін до конфігураційного файлу, що відповідає за базовий запуск системи виявлення та запобігання вторгненням. Після завершення інсталяції Snort конфігурацію можна буде деталізувати та адаптувати під конкретні потреби мережі й політики безпеки підприємства [23].

У рамках даної роботи виконується лише первинне налаштування. Для цього відкривається файл **snort.conf**, який містить основні параметри запуску програми. Для редагування було використано редактор NotePad++, однак може бути

застосовано будь-яке інше текстове середовище. Повністю змінений та готовий до використання конфігураційний файл наведено в **Додатку Б** [19].

Близько до 103-го рядка конфігураційного файлу знаходиться параметр, встановлений розробниками за замовчуванням, а саме шлях до директорії з правилами:

c:\snort\rules

Цей шлях необхідно замінити на фактичне розташування каталогу правил на локальному комп'ютері. У нашому випадку воно співпадає зі структурою каталогів у робочій директорії. За потреби можна зазначити інше місце зберігання правил, однак тоді аналогічні зміни слід внести й у bat-скрипт, оскільки розробником передбачено позначення місць для редагування шляху спеціальними маркерами у вигляді двох крапок [19].

```
16 # Path to your rules files (this can be a relative path)
17 # Note for Windows users: You are advised to make this an absolute path, #such as: c:\snort\rules
18 var RULE_PATH c:\Snort\rules
19 var SO_RULE_PATH c:\Snort\so_rules
20 var PREPROC_RULE_PATH c:\Snort\preproc_rules
21 # If you are using reputation preprocessor set these
22 var WHITE_LIST_PATH c:\snort\rules
23 var BLACK_LIST_PATH c:\snort\rules
```

Рис. 3.2 Зміна шляху до директорії з правилами (Rules)

Наступним кроком є визначення шляху до директорії, у якій зберігатимуться **log-файли** – саме туди Snort записуватиме журнали своєї роботи. Вміст цих журналів можна буде переглядати з метою аналізу подій, діагностики або подальшого удосконалення системи безпеки.

Під час інсталяції Snort у кореневій директорії програми автоматично створюється папка для логів. Тому достатньо скопіювати шлях до цієї папки та внести його у конфігураційний файл. Для цього в **snort.conf** необхідно перейти до рядка приблизно під номером 182 та вказати:

```
181
182 config logdir: c:\snort\log
```

Рис. 3.3 Задання шляху до директорії з log-файлами

При цьому слід обов’язково прибрати символ # на початку рядка, оскільки він означає коментар і, відповідно, призводить до ігнорування параметра програмою.

За аналогічною логікою необхідно скорегувати й шлях до бібліотек, які використовує Snort. Важливо враховувати, що у випадку встановлення програми в нестандартну директорію, усі відповідні шляхи мають бути відкориговані вручну. Це забезпечує коректне завантаження необхідних модулів та уникнення помилок під час запуску системи [19].

```
236 #path to dynamic preprocessor libraries
237 dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor
238 #path to base preprocessor engine
239 dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
240 #path to dynamic rules libraries
241 #dynamicdetection directory c:\Snort \lib\snort_dynamicrules
```

Рис. 3.4 Зміна шляху до необхідних бібліотек

На наступному етапі необхідно вимкнути низку параметрів, тимчасово закоментувавши відповідні рядки конфігураційного файлу. Перелік цих рядків наведено нижче.

```
247 # Inline packet normalization. For more information, see README.normalize
248 # Does nothing in IDS mode
249 # preprocessor normalize_ip4
250 # preprocessor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp,
251 ips, ecn stream
252 # preprocessor normalize_icmp4
253 # preprocessor normalize_ip6
254 # preprocessor normalize_icmp6
255 # Back Orifice detection.
256 # preprocessor bo
```

Рис. 3.5 Рядки конфігурації Snort, які необхідно закоментувати

У певних випадках потрібно виконати протилежну дію – вилучити символ коментаря з окремих рядків конфігураційного файлу, щоб задіяти відповідні модулі або параметри Snort.

```
261 # Portscan detection. For more information, see README.sfportscan
262 preprocessor sfportscan: proto {all} memcap { 10000000 } sense_level { low }
```

Рис. 3.6 Активування модуля виявлення сканування портів (sfPortscan)

Далі необхідно відредагувати параметри, що визначають шляхи до файлів white.list та black.list, які використовуються Snort для фільтрації трафіку відповідно до списків дозволених та заборонених адрес. У конфігураційному файлі потрібно знайти відповідний рядок та замінити значення шляхів на актуальні для робочої директорії [19].

```
504 whitelist $WHITE_LIST_PATH\white.list,
505 blacklist $BLACK_LIST_PATH\black.list
```

Рис. 3.7 Встановлення шляхів до файлів white.list та black.list

У проміжку між рядками 545 та 660 необхідно виконати технічне коригування шляхів: у кожному з них символ “/” слід замінити на символ “\”. Це забезпечує відповідність форматування шляхів стандартам файлової системи Windows, що є критично важливим для коректного функціонування Snort у цьому середовищі.

3.2 Конфігурація, налаштування та створення сигнатур у Snort

Для реалізації поставленої задачі було вирішено використати bat-скрипт, створений на основі стандартних команд операційної системи Windows. Такий підхід дає змогу автоматизувати більшість рутинних операцій, пов’язаних з інсталяцією та налаштуванням необхідних компонентів [20].

Автоматизована інсталяція програмного забезпечення

У початковому блоці скрипта виконується встановлення всіх потрібних програм та утиліт. Для максимального спрощення процесу застосовано режим «тихої» інсталяції, за якого встановлення відбувається без залучення користувача. Зокрема, використано команду:

"%~dp0\Snort_2.9.17.1_Installer.x64.exe" -y /S

– параметр -y забезпечує автоматичний вибір варіанта «ОК» у відповідь на будь-які системні запити інсталятора;

– параметр /S активує режим повністю беззвучної інсталяції.

Слід враховувати, що різні інсталятори можуть використовувати власні параметри для «silent-mode», тому команда може дещо відрізнятися залежно від конкретної програми. Після виконання команди інсталяції скрипт робить паузу тривалістю 5 секунд, а потім перевіряє, чи було успішно встановлено Snort. Для цього використано таку послідовність команд:

```
ping -n 6 localhost>Nul
set "prog="C:\Snort\bin\snort.exe""
if exist "%prog%" (
 @echo Програма Snort успішно встановлена
 @echo.
)
```

Команда ping у цьому випадку використовується для організації затримки, а перевірка наявності файлу snort.exe у відповідній директорії підтверджує факт успішної інсталяції [21].

Розпакування архіву правил Snort

Наступним етапом bat-скрипт виконує розпакування архіву з правилами Snort. Оскільки файл має формат .tar.gz, для його обробки застосовується утиліта 7-Zip, яка дозволяє послідовно зняти стискання та витягнути вміст архіву. Для цього використовується така команда:

```
"C:\Program Files\7-Zip\7z.exe" e "E:\Мої файли\Навчання\Диплом\Завдання практика\Snort_installing\snortrules-snapshot-29171.tar.gz" -so | "C:\Program Files\7-Zip\7z.exe" x -aoa -si -ttar -o"C:\Snort\"
```

У результаті правила Snort розпаковуються безпосередньо у відповідну директорію.

Створення службових списків

Після розпакування правил скрипт автоматично формує файли black.list та white.list, що можуть використовуватися для блокування або дозволу певних IP-адрес чи доменів:

@echo Створення blacklist и whitelist

@echo .>C:\Snort\rules\black.list

@echo .>C:\Snort\rules\white.list

Копіювання конфігураційного файлу

Далі до кореневої директорії Snort переноситься попередньо підготовлений файл конфігурації:

@echo Перенос файлу конфігурації

xcopy "%~dp0\snort.conf" C:\Snort

Додавання власних правил

Скрипт також автоматично доповнює local.rules власними правилами, які використовуються для сповіщення адміністратора про спроби користувачів відвідувати небажані веб-ресурси. У прикладі наведено правило, що фіксує звернення до популярного розважального сайту:

@echo Додавання власних правил

echo f| copy C:\Snort\rules\local.rules C:\Snort\rules\temp.txt

echo. alert tcp any any -> any any (content: "pikabu.ru"; msg: "Visiting site pikabu.ru detected"; sid:1000008; rev:1)>C:\Snort\rules\local.rules

type C:\Snort\rules\temp.txt >>C:\Snort\rules\local.rules

del C:\Snort\rules\temp.txt

Подібна логіка дозволяє автоматично сформувати набір ознак небажаної активності, що можуть бути використані для контролю дисципліни працівників у корпоративній мережі.

Запуск скрипта

Після завершення усіх підготовчих дій можна запускати bat-скрипт. Для коректної роботи його необхідно виконувати від імені адміністратора, оскільки низка операцій потребує підвищених привілеїв. Процес виконання займає небагато

часу, а користувач отримує інформативні повідомлення про хід виконання кожного етапу [21].

Виконати "тиху" інсталяцію для пакета Npcap виявилося неможливим, оскільки режим автоматичної установки без участі користувача доступний лише у комерційній версії цього програмного забезпечення. У зв’язку з цим під час роботи скрипта процес інсталяції буде тимчасово призупинено появою стандартного інсталяційного вікна Npcap.

У вікні майстра встановлення користувачеві потрібно вручну натиснути кнопку «I agree», а на наступному етапі – обрати всі чотири доступні компоненти, необхідні для коректної роботи Snort.

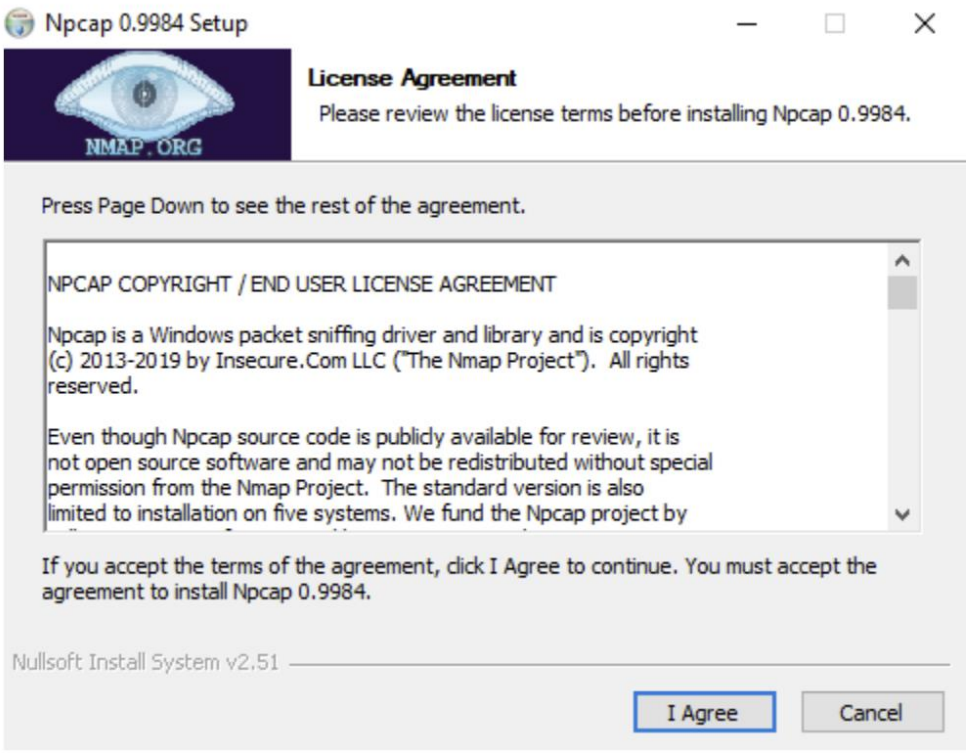

Рис. 3.8 Процес інсталяції компонента Npcap

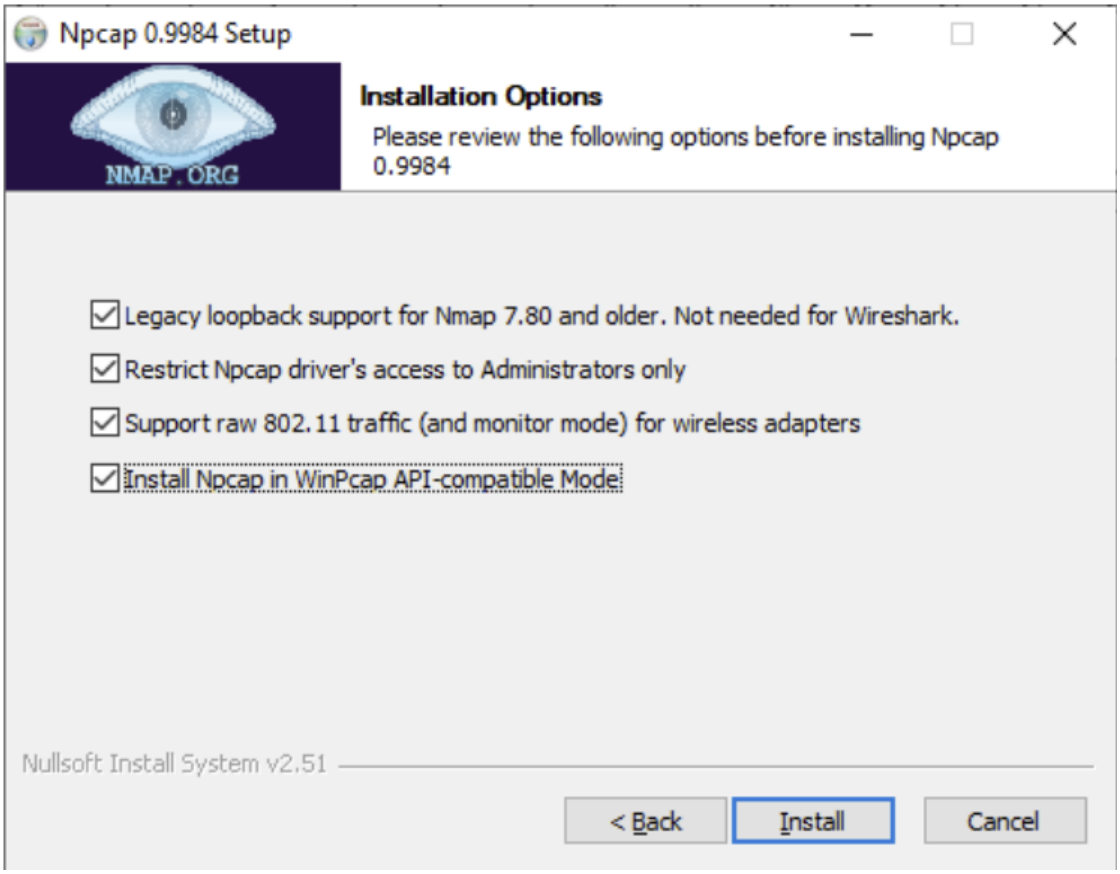

Рис. 3.9 Інсталяція пакета Npcap

У процесі виконання bat-скрипта всі його дії супроводжуються текстовими коментарями, що дозволяє користувачеві відстежувати перебіг інсталяції й налаштування компонентів. Після завершення роботи скрипт не завершується автоматично: у командному вікні відображається перелік команд, необхідних для здійснення першого запуску системи Snort. Це полегшує подальший етап налаштування та гарантує правильний старт IDS/IPS.

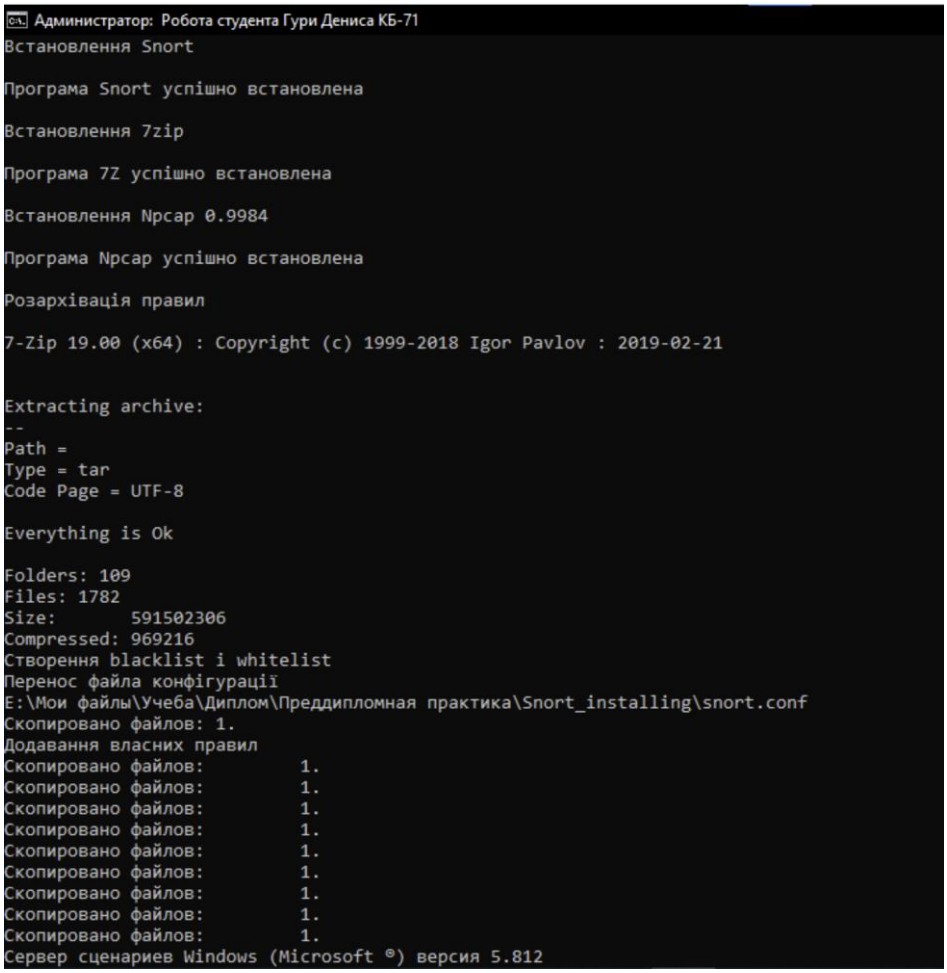

Рис. 3.10 Результат виконання інсталяційного скрипта

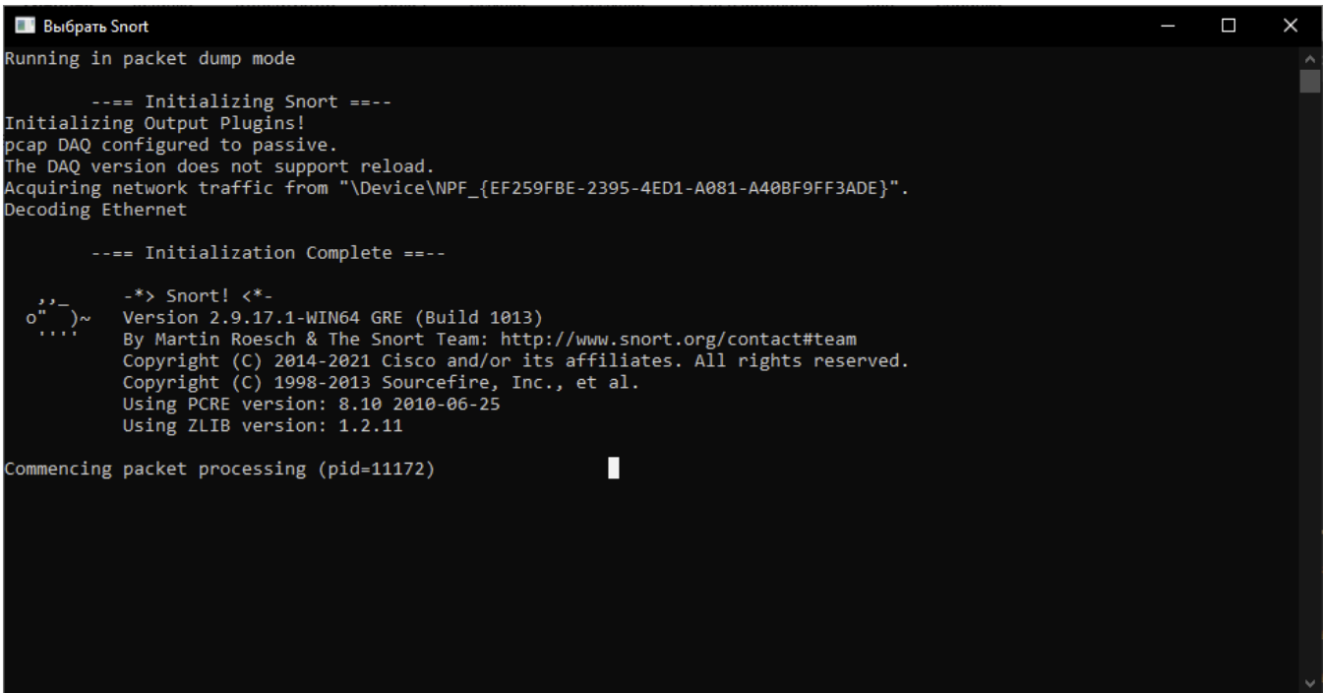

Рис. 3.11 Запуск системи Snort у робочому режимі\

Після успішного завершення роботи інсталяційного скрипта можна перейти до ручного запуску системи Snort. Для цього необхідно відкрити командний рядок, перейти до кореневого каталогу програми – Snort\bin\ – і виконати команду:

snort -W

Дана команда виводить список доступних мережевих інтерфейсів, що дозволяє визначити, через який інтерфейс Snort здійснюватиме аналіз мережевого трафіку.

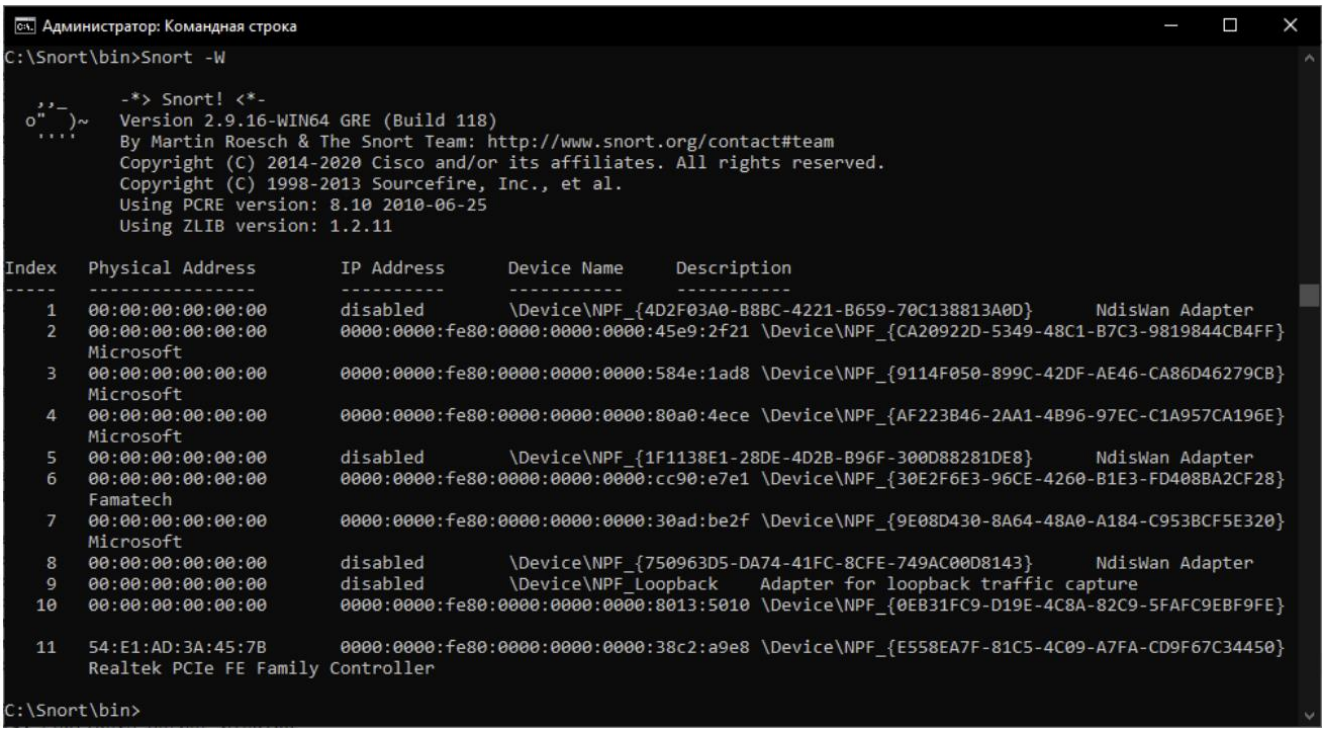

Рис. 3.12 Виконання команди snort -W для перегляду мережевих інтерфейсів

У результаті виконання команди snort -W на екрані відображається перелік доступних мережевих інтерфейсів. Із цього списку необхідно визначити інтерфейс, що відповідає основній мережевій карті комп’ютера. У нашому випадку потрібний адаптер позначений номером 11.

Для додаткової перевірки коректності налаштувань конфігураційного файлу snort.conf виконується команда:

snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 11

де:

– T - запускає Snort у режимі тестування конфігурації;

– c - вказує шлях до конфігураційного файлу;
– l - визначає директорію для запису логів;
– i 11 - позначає номер мережевого інтерфейсу, визначеного на попередньому етапі.

Якщо всі параметри задано коректно й конфігураційний файл не містить помилок, після виконання тестової команди Snort виведе відповідне повідомлення про успішну перевірку.

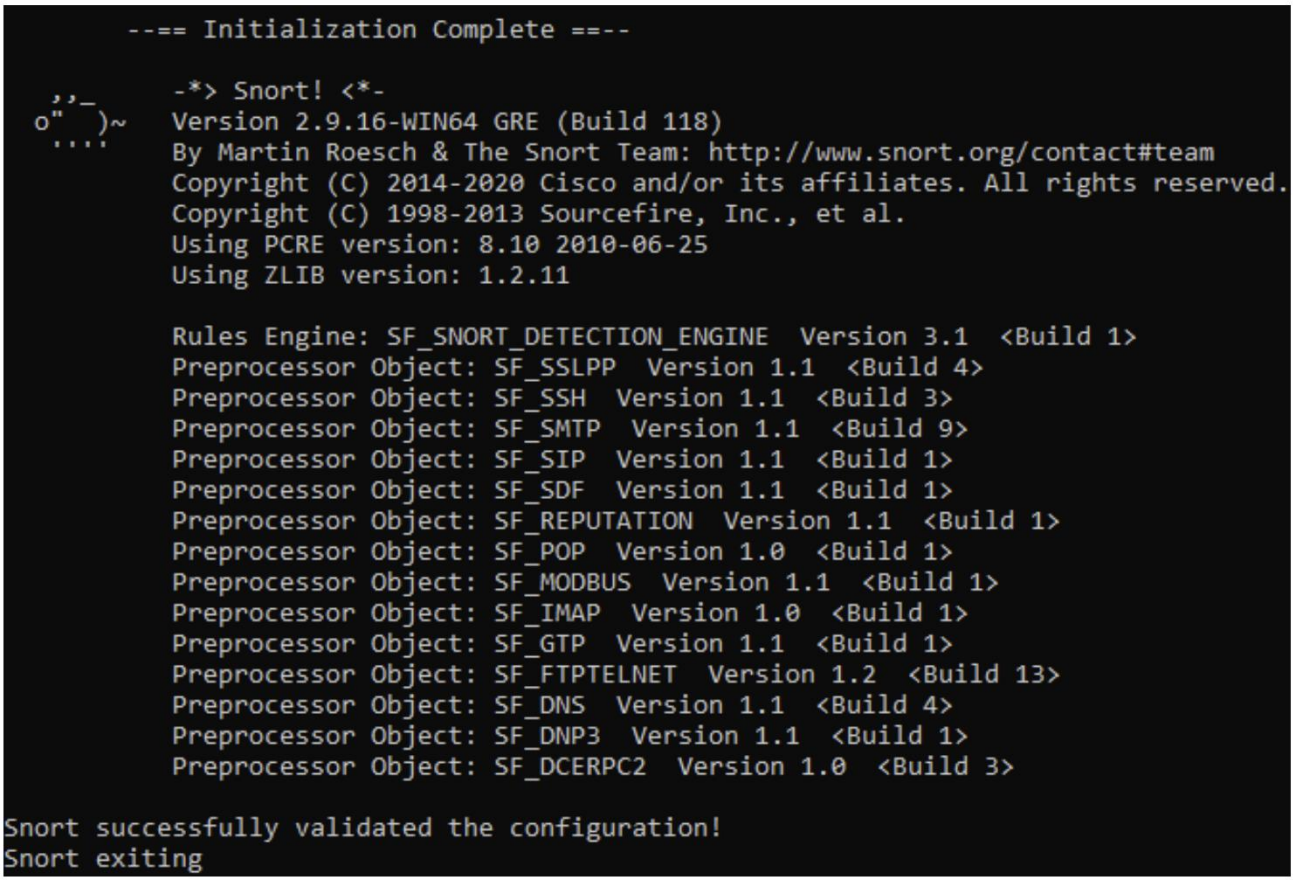

Рис. 3.13 Результат успішної перевірки параметрів конфігураційного файлу

Після того як конфігураційний файл успішно пройшов перевірку, систему Snort можна запускати в робочому режимі. Для цього у командному рядку виконується команда:

snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 11

де:

– A console - виводить сповіщення Snort безпосередньо в консоль;
– c - вказує шлях до конфігураційного файлу;

– l - задає директорію для збереження логів;
– і 11 - визначає мережевий інтерфейс, через який здійснюватиметься моніторинг трафіку.

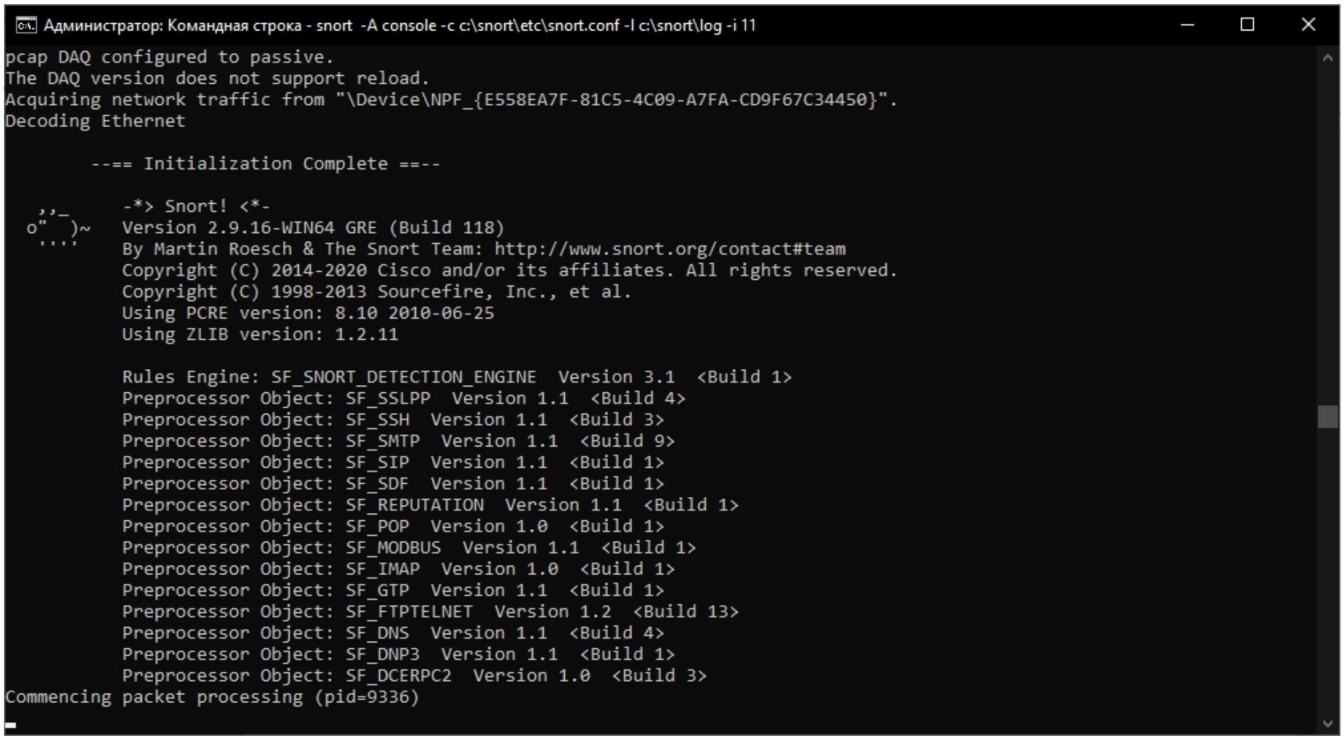

Рис. 3.14 Запущена система Snort у режимі моніторингу мережевого трафіку

Після запуску системи Snort користувач може скористатися додатковими параметрами командного рядка, які дозволяють керувати режимами роботи IDS/IPS. Основні з них наведені у таблиці 3.1.

Таблиця 3.1

Опис основних ключів командного рядка Snort

№	Ключ	Опис дії
1	-T	Виконує тестування поточної конфігурації Snort, дозволяючи перевірити правильність синтаксису та узгодженість параметрів перед запуском.
2	-c	Задає шлях до файлу snort.conf та активує режим IDS, у якому Snort аналізує трафік за визначеними правилами.
3	-l	Вмикає запис логів на жорсткий диск та визначає директорію, у яку вони будуть збережені.
4	-A	Вказує спосіб виведення попереджень (alerts); зокрема, параметр console дублює повідомлення безпосередньо на екран.
5	-i	Визначає порядковий номер (індекс) мережевого інтерфейсу, через який Snort отримуватиме трафік для аналізу.

3.3 Програмна імплементація та інтеграція Snort у систему моніторингу та реагування

Для перевірки працездатності системи необхідно виконати тестування Snort. Перший етап діагностики здійснюється через командний рядок за допомогою команди:

snort -i 1 -c c:\Snort\etc\snort.conf -T

Ця команда запускає Snort у режимі тестування конфігурації з використанням мережевого інтерфейсу під номером 1. На рисунку 3.15 продемонстровано процес виконання початкового тесту системи.

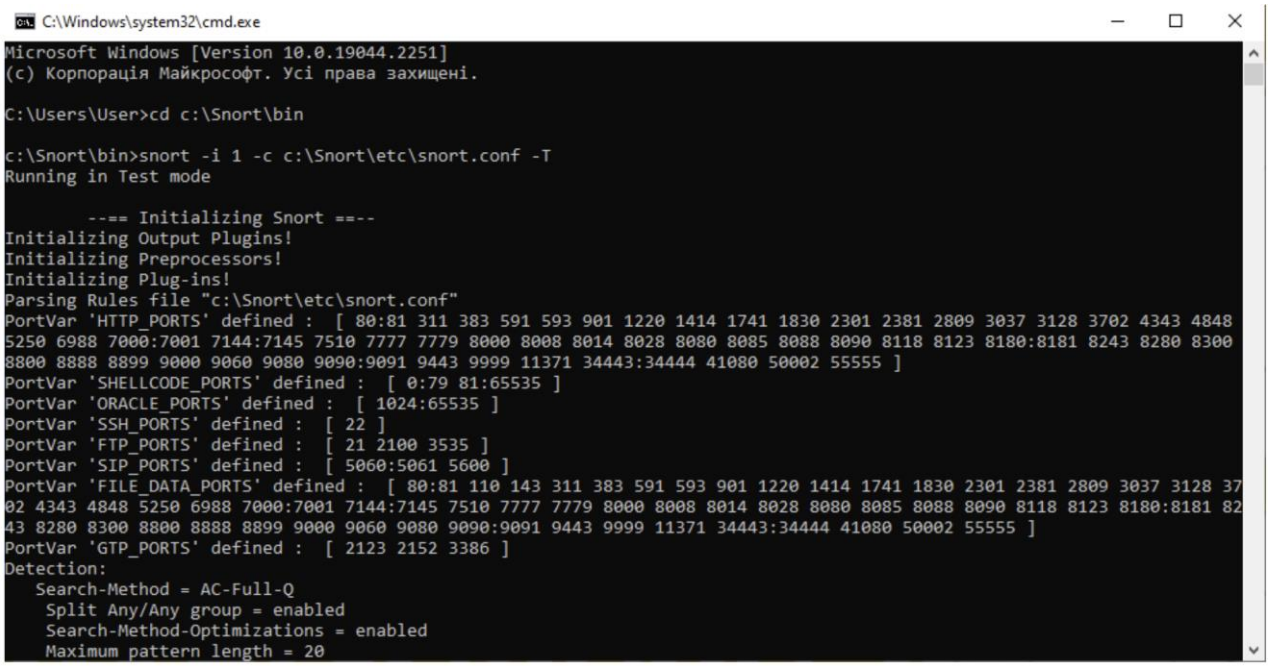

Рис. 3.15 Запуск першого тестування

Бачимо, що виконались всі препроцесори (рис. 3.16)

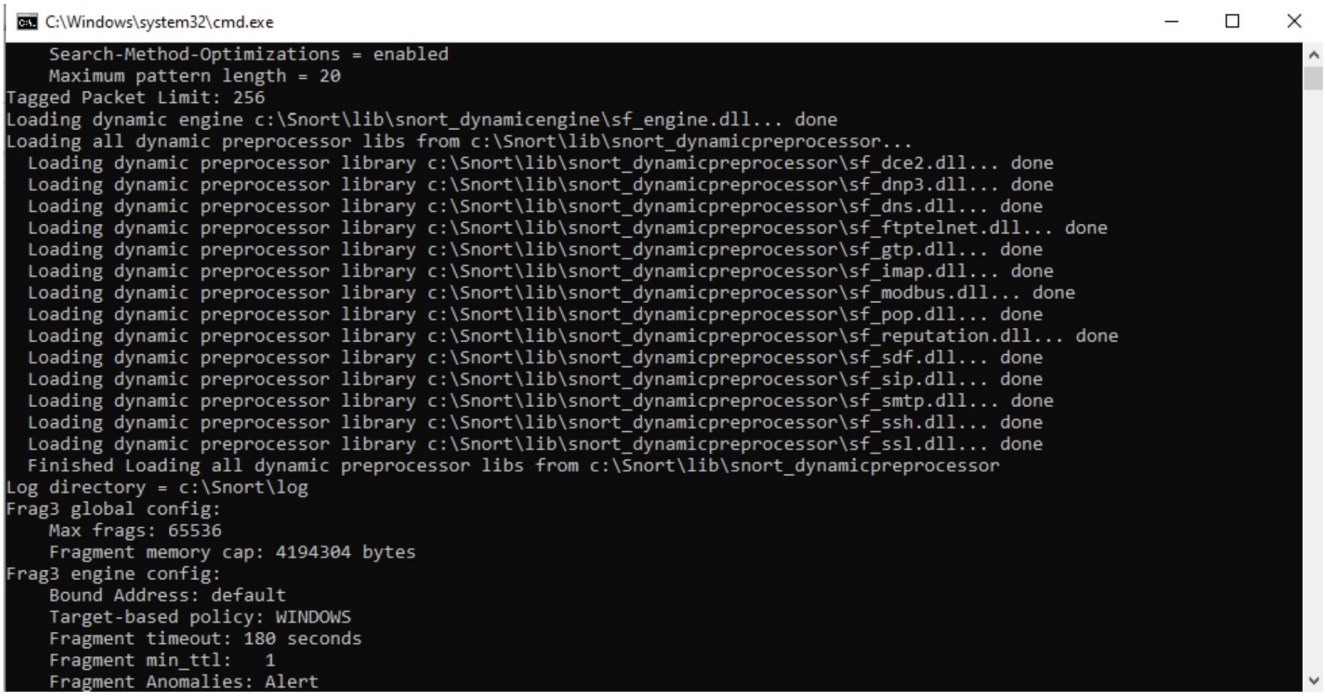

Рис. 3.16 Успішна ініціалізація та виконання препроцесорів Snort

Під час аналізу результатів тестування можна побачити, що Snort успішно завантажив усі правила. Загалом система опрацювала 10 614 правил різних типів, що підтверджує коректність їх розташування та налаштувань (Рис. 3.17). Також було виконано валідацію препроцесорів, яка завершилася успішно.

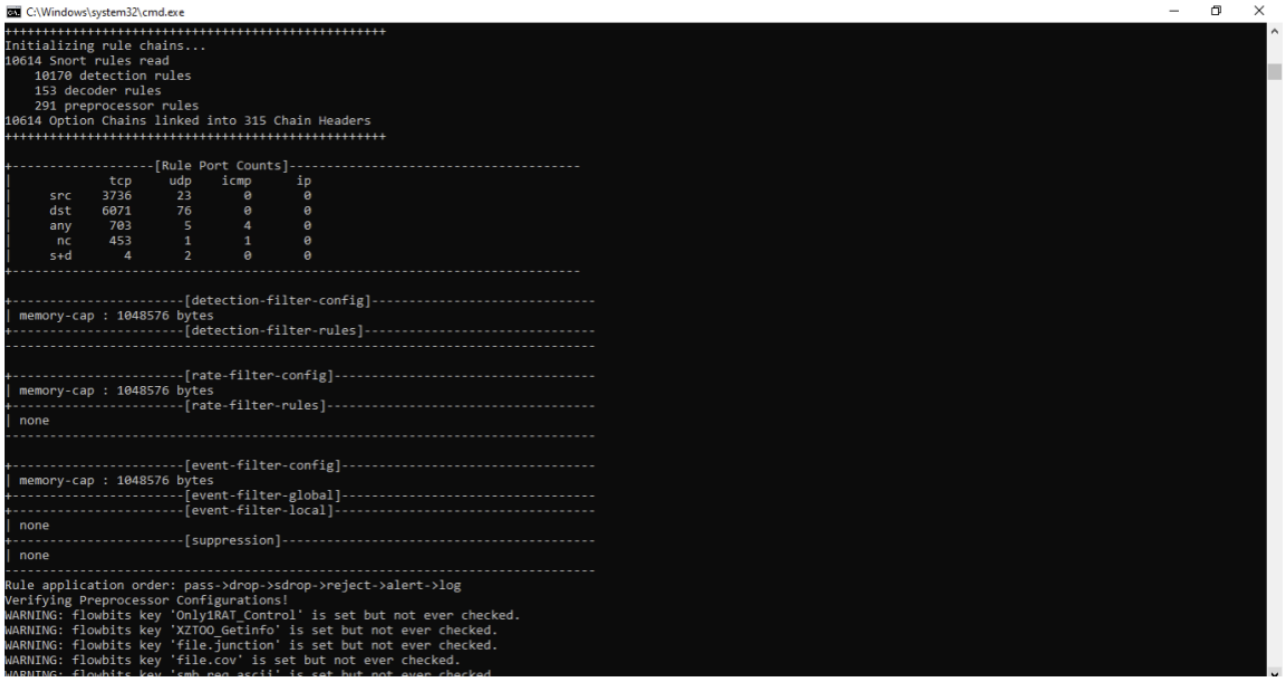

Рис. 3.17 Успішне завантаження та обробка правил системою Snort

У підсумку можна зробити висновок, що тестування завершилося успішно, а система Snort коректно опрацювала всі необхідні компоненти (Рис. 3.18).

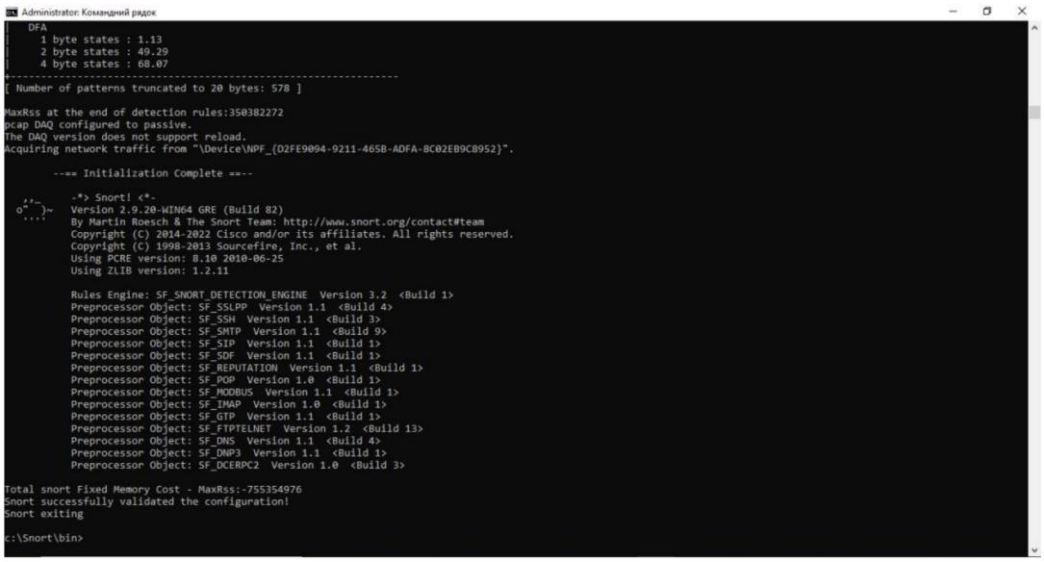

Рис. 3.18 Позитивний результат першого тестування системи Snort

Оскільки перше тестування пройшло успішно, можна переходити до більш розширеної перевірки роботи системи. Для цього необхідно виконати додаткові налаштування правил. Спочатку слід перейти до директорії:

c:\Snort\rules

та відкрити файл local.rules у будь-якому текстовому редакторі. До нього потрібно додати три тестові оповіщення, які дозволять перевірити роботу Snort з різними типами трафіку:

alert icmp any any -> any any (msg:"Testing ICMP"; sid:1000001;)

alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002;)

alert udp any any -> any any (msg:"Testing UDP"; sid:1000003;)

Ці правила згенерують сповіщення при перехопленні ICMP-, TCP- та UDP-пакетів відповідно. На рисунку 3.19 показано, як саме тестові оповіщення були додані до файлу local.rules.

```
#Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#This file contains (1) proprietary rules that were created, tested and certified by
#Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT #Certified Rules License Agreement (v 2.0), and (ii) rules that were
#The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created by Sourcefire and other third parties. The GPL Rules created by Sou
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
#their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
#list of third party owners and their respective copyrights.
#In order to determine what rules are VRT Certified Rules or GPL Rules, please refer to the VRT Certified Rules License Agreement (v2.0).
#LOCAL RULES
alert icmp any any alert tcp any any alert udp any any
-> any any (msg:"Testing ICMP"; sid:1000001;) -> any any (msg:"Testing TCP"; sid: 1000002;) -> any any (msg:"Testing udp"; sid:1000003;)
```

Рис. 3.19 Додавання тестових оповіщень до файлу local.rules

Після внесення тестових правил необхідно виконати запуск Snort у режимі активного моніторингу, щоб перевірити роботу доданих оповіщень. Для цього у командному рядку слід виконати команду:

snort -i 1 -c c:\Snort\etc\snort.conf -A console

Ця команда ініціює аналіз трафіку через мережевий інтерфейс №1, використовуючи наявний конфігураційний файл, а всі згенеровані оповіщення виводитимуться безпосередньо в консоль. Це дозволяє оперативно оцінити, чи коректно відпрацьовують додані до local.rules тестові правила.

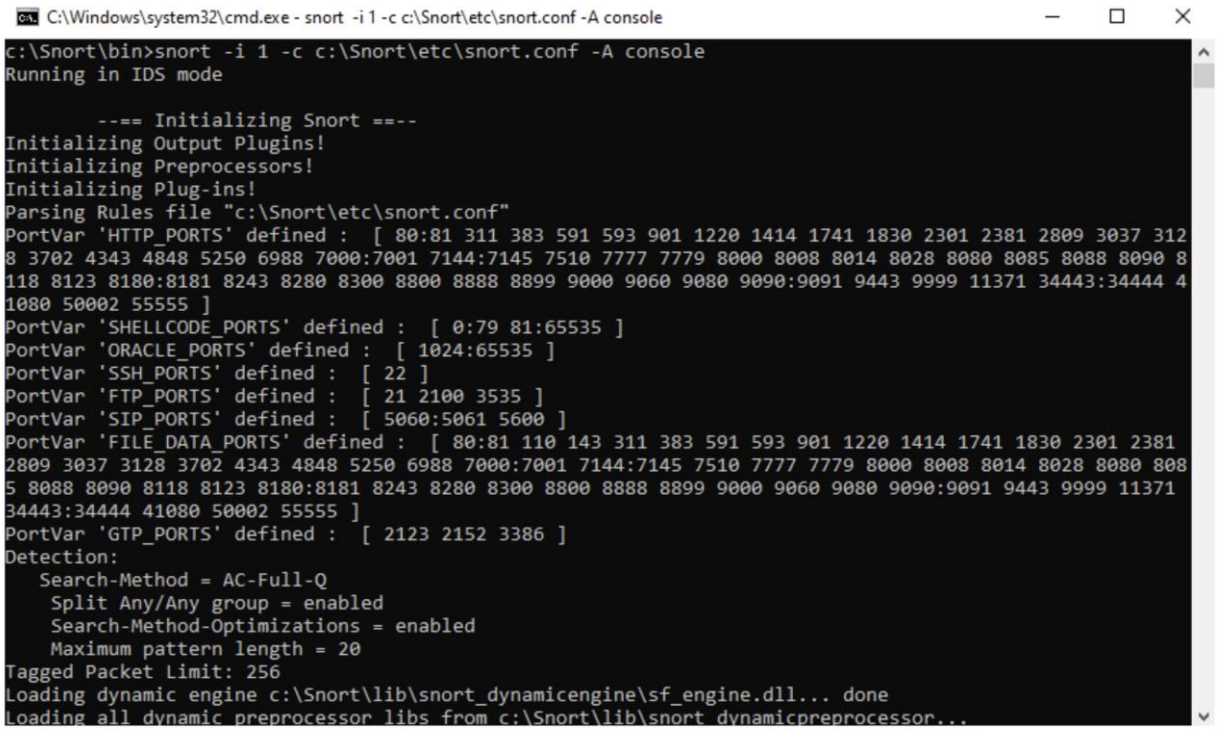

Рис. 3.20 Запуск другого тестового режиму Snort

Після запуску другого тестового режиму можна спостерігати, що всі препроцесори також були успішно ініціалізовані та працюють коректно (Рис. 3.21). Це підтверджує правильність внесених змін і стабільність роботи системи під час обробки трафіку.

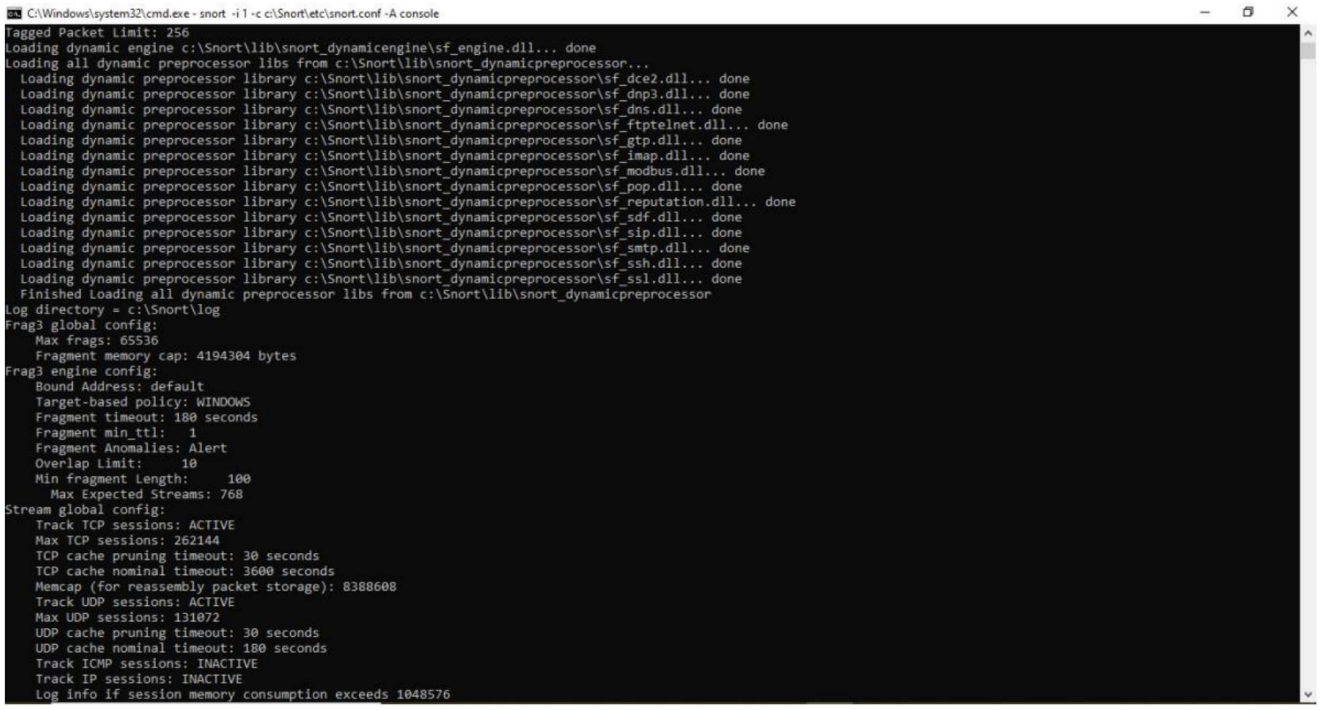

Рис. 3.21 – Успішна ініціалізація препроцесорів під час другого тестування

На рисунку 3.22 показано, що система успішно зчитала всі додані правила, а препроцесори пройшли повну верифікацію. Це свідчить про коректність конфігурації та готовність Snort до подальшого практичного використання.

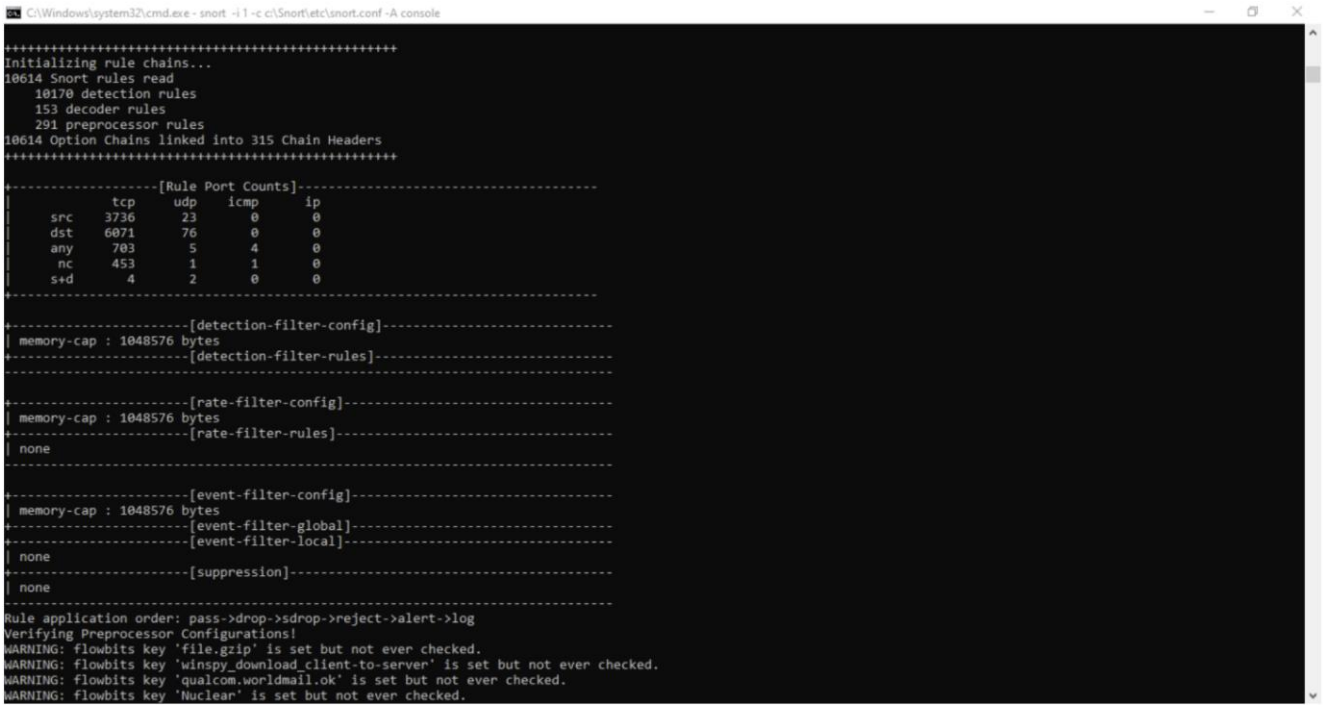

Рис. 3.22 Коректне завантаження правил та успішна верифікація препроцесорів

На цьому етапі можна спостерігати, що ініціалізація Snort пройшла успішно, і система повністю готова до виконання покладених на неї функцій (Рис. 3.23).

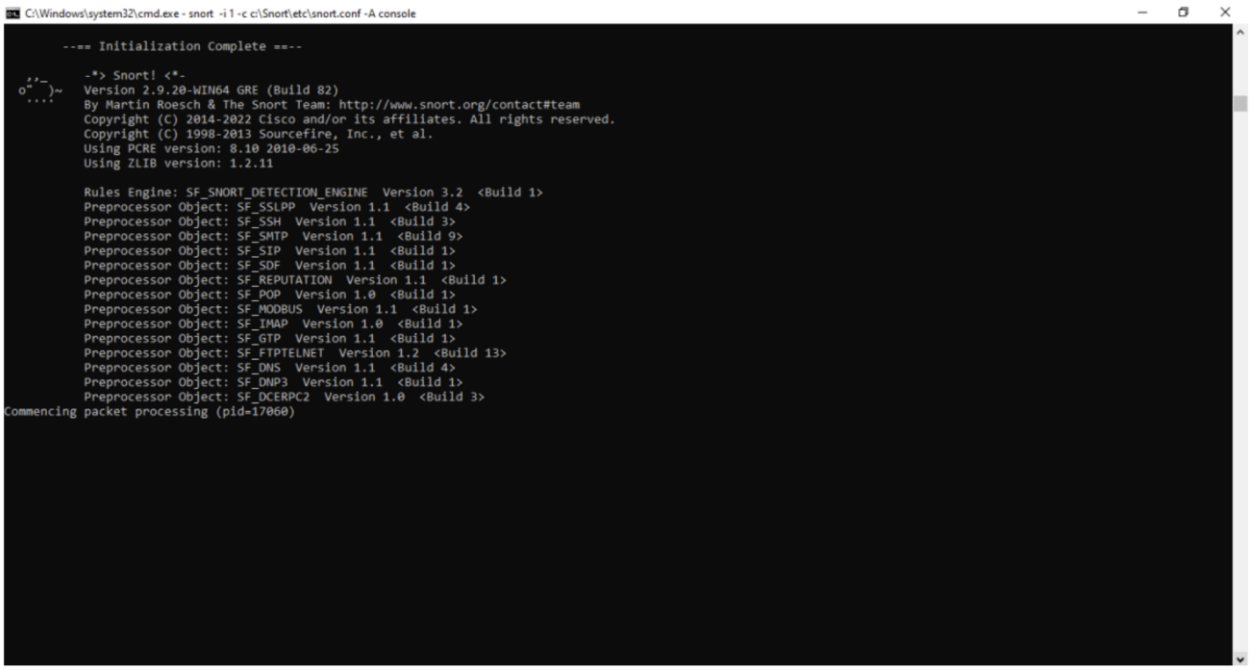

Рис. 3.23 Успішна ініціалізація системи Snort

Після завершення попередніх етапів тестування можна перейти до практичної перевірки роботи Snort під час реального мережевого трафіку. Для цього відкриваємо веб-браузер – у нашому випадку Google Chrome – і переходимо на будь-який веб-сайт, наприклад www.google.com , після чого вводимо довільний запит у пошуковому полі (Рис. 3.24).

Попри те, що жодних помилок у роботі Snort не зафіксовано, можна помітити, що процес обробки пакетів не розпочався. Це свідчить про необхідність подальшого аналізу параметрів запуску та перевірки коректності вибору мережевого інтерфейсу.

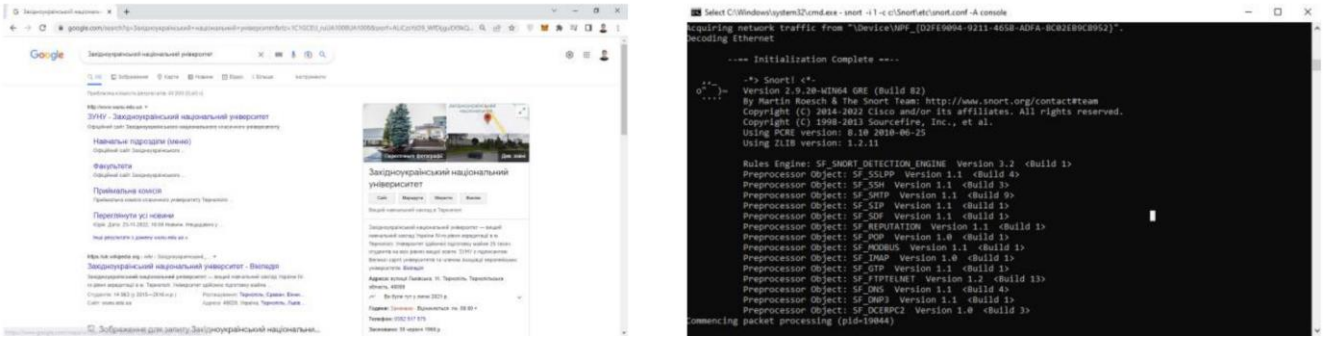

Рис. 3.24 – Невдалий запуск процесу обробки мережевих пакетів

Для вирішення виявленої проблеми необхідно повторно відкрити термінал та перейти до робочої директорії Snort за допомогою команди:

cd c:\snort\bin

Після цього слід ще раз виконати команду:

snort -W

Ця команда виведе список доступних мережевих інтерфейсів. Аналізуючи отримані дані, можна побачити, що інтерфейс, через який здійснюється підключення до Інтернету, позначено номером 6 (Рис. 3.25). Саме цей інтерфейс необхідно використовувати для коректного моніторингу трафіку Snort.

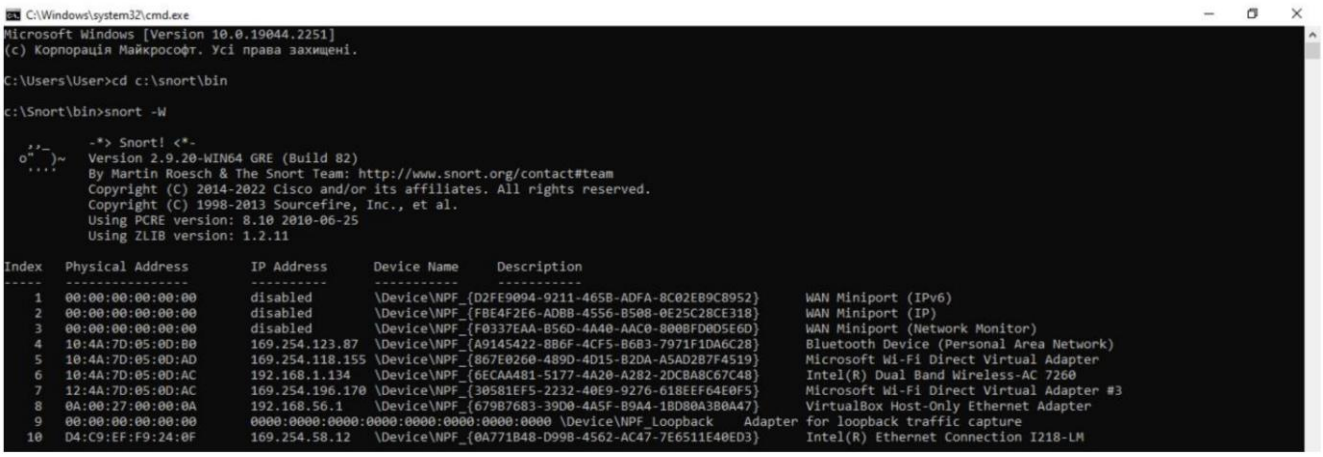

Рис. 3.25 Відображення переліку доступних мережевих інтерфейсів Snort

Після визначення коректного мережевого інтерфейсу необхідно повторно запустити Snort, вказавши інтерфейс під номером 6. Для цього у терміналі виконуємо команду:

snort -i 6 -c c:\Snort\etc\snort.conf -A console

Після запуску система починає фіксувати мережеву активність. У командному рядку з’являються відповідні сповіщення, що відображають процеси, які відбуваються під час відкриття веббраузера та завантаження вебсторінки.

Успішний результат повторного тестування показано на рисунку 3.26.

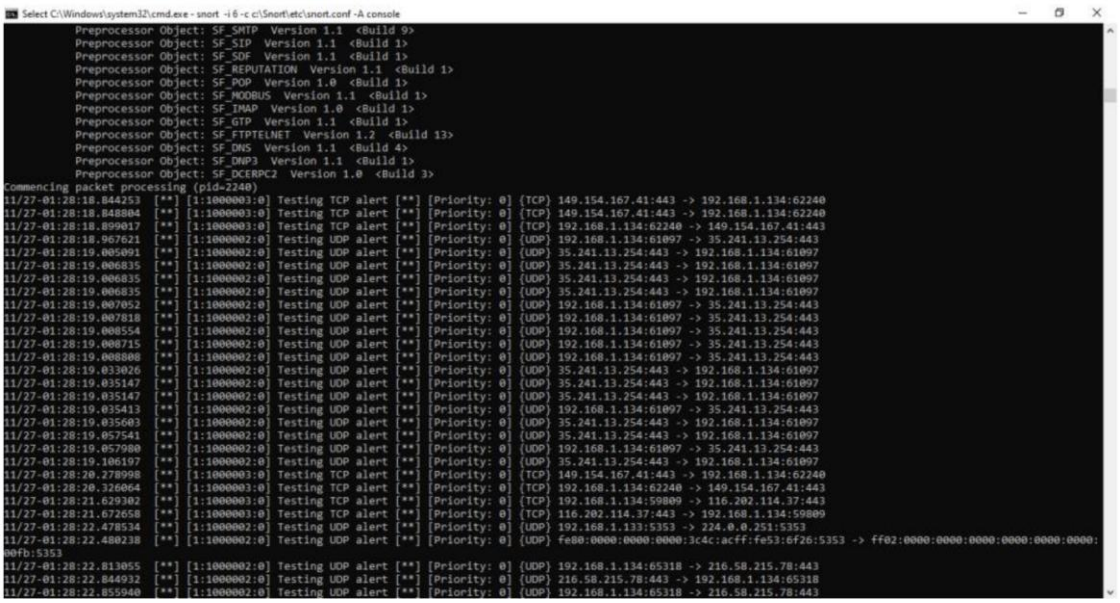

Рис. 3.26 Успішне проходження другого тестування Snort

Для перегляду зведеної статистики роботи Snort необхідно зупинити

поточний процес моніторингу. Це можна зробити, відкривши вікно термінала та натиснувши комбінацію клавіш Ctrl + C. Після завершення роботи Snort у консольному вікні буде відображено детальну статистику за всіма ключовими параметрами системи, включно з інформацією про опрацьовані пакети, спрацювання правил та активність препроцесорів (Рис. 3.27).

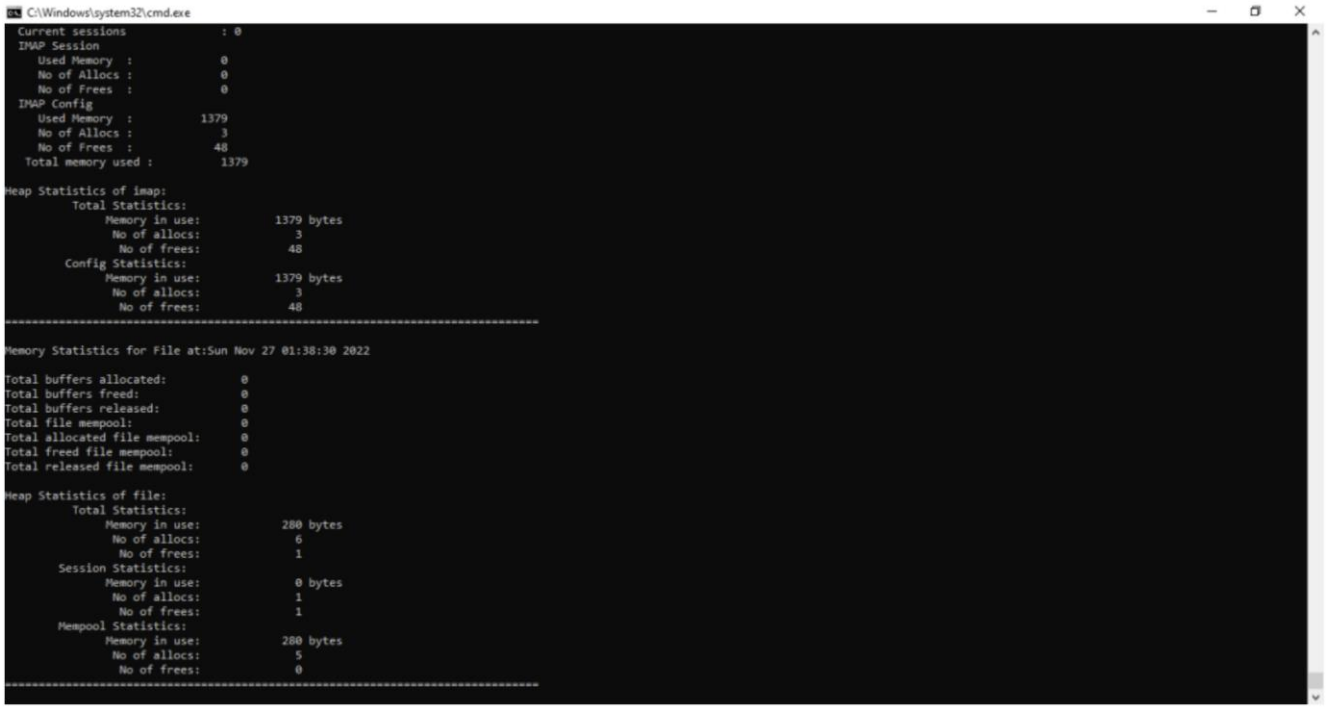

Рис. 3.27 Відображення статистики роботи системи Snort

3.4 Розробка рекомендацій щодо підвищення рівня захищеності корпоративної мережі із застосуванням IDS/IPS-рішень

Ефективність функціонування корпоративної мережі значною мірою залежить від здатності своєчасно виявляти, ідентифікувати та нейтралізувати внутрішні й зовнішні кіберзагрози. Запровадження IDS/IPS-рішень, зокрема Snort, Suricata або Zeek, суттєво підсилює систему інформаційної безпеки, однак потребує дотримання низки організаційних, технічних та оперативних рекомендацій. У цьому підпункті виокремлено ключові підходи, які дозволяють підвищити рівень захищеності корпоративної мережі та забезпечити комплексний захист інформаційних активів підприємства.

По-перше, доцільно сформувати багаторівневу архітектуру безпеки, у якій IDS/IPS відіграє роль одного з ключових елементів. Така архітектура повинна включати міжмережеві екрани, системи контролю доступу, VPN-технології, а також централізовані служби журналювання та моніторингу подій. Взаємодія між цими компонентами забезпечує своєчасне виявлення аномалій, фіксацію ознак атаки та блокування шкідливого трафіку до того, як він зможе завдати шкоди системі. Особливу увагу слід приділяти розташуванню сенсорів Snort у мережі: рекомендується встановлювати їх у точках маршрутизації трафіку, на стиках VLAN-сегментів та у зонах DMZ, що дозволяє контролювати всі критичні потоки інформації.

По-друге, важливим елементом захисту є регулярне оновлення сигнатурних правил та баз виявлення атак. Оскільки кіберзагрози постійно еволюціонують, використання застарілих сигнатур знижує ефективність IDS/IPS, збільшуючи ймовірність пропуску складних або цілеспрямованих атак. Рекомендується налаштувати автоматичне завантаження актуальних правил із репозиторіїв Emerging Threats або Snort Community Rules, а також вести власний набір корпоративних правил, розроблених на основі виявлених інцидентів, логів мережевої активності та специфічних ризиків підприємства. Це дозволяє адаптувати систему під унікальні особливості корпоративної інфраструктури.

По-третє, необхідно забезпечити оптимізацію продуктивності IDS/IPS у високонавантаженому середовищі. Застосування Snort у великих мережах потребує правильної конфігурації потоків обробки, балансування навантаження, використання апаратних прискорювачів або інтеграції з високопродуктивними мережевими інтерфейсами. Доцільно застосовувати методи відсіювання шумового трафіку (white-listing), використання порогових значень (thresholding), попередньої фільтрації пакетів та логічного групування правил, що дозволяє суттєво зменшити кількість хибних спрацювань і підвищити точність аналізу.

Важливою складовою ефективної роботи IDS/IPS є побудова системи централізованого уніфікованого моніторингу. Доцільно впровадити SIEM-рішення (Security Information and Event Management), такі як Splunk, Wazuh, ELK Stack чи

IBM QRadar, які забезпечують кореляцію подій, аналіз безпекових індикаторів та формування автоматичних звітів. Інтеграція Snort із системою моніторингу дозволяє не лише фіксувати факти вторгнення, але й виокремити тенденції, оцінити джерела загроз, визначити слабкі місця корпоративної інфраструктури та своєчасно вживати превентивні заходи. Крім того, налаштування оповіщень у режимі реального часу через електронну пошту, Telegram-боти чи внутрішні системи оповіщення забезпечує оперативне реагування на інциденти.

Окремої уваги потребує питання контролю внутрішніх загроз, оскільки значна частина кібератак походить від співробітників або скомпрометованих внутрішніх облікових записів. Рекомендується впровадити сегментацію мережі, обмеження між VLAN, використання DHCP-snooping, 802.1X-аутентифікацію, а також контроль виходу за межі дозволених зон доступу. IDS/IPS системи повинні бути налаштовані на виявлення аномальної активності, характерної для інсайдерських загроз: нетипові запити, переміщення по мережі, несанкціонований доступ до критичних сервісів або передача великих обсягів даних.

Розробка політик реагування на інциденти також є невід’ємною частиною ефективного функціонування IDS/IPS. Рекомендується створити документовані регламенти реагування, які описують порядок дій при виявленні різних типів атак, зокрема спроб сканування портів, brute force-атак, SQL-ін’єкцій, DDoS-активності та експлуатації вразливостей. Політика має включати визначення відповідальних осіб, часові рамки реагування та порядок ескалації інциденту. Це дозволяє мінімізувати людський фактор та забезпечує скоординоване вирішення проблем.

Важливою рекомендацією є також організація регулярного тестування захисних механізмів, зокрема проведення пентестів, Red Team-оцінок, моделювання атак за методологією MITRE ATT&CK та використання таких інструментів, як Metasploit або Caldera. Це дозволяє оцінити фактичний рівень стійкості системи, перевірити працездатність сигнатур Snort, протестувати реакцію IPS-модуля та перевірити відповідність політик безпеки сучасним вимогам. Періодичне тестування сприяє своєчасному виявленню вразливостей і здатне запобігти успішним атакам у майбутньому.

Не менш важливо забезпечити належну підготовку персоналу. Ефективність IDS/IPS значною мірою залежить від компетентності працівників, які здійснюють налаштування, моніторинг, аналіз журналів та реагування на інциденти. Рекомендується проводити регулярні тренінги, ознайомлення з новими техніками атак, аналізом практичних кейсів та оновленнями сигнатурних баз. Наявність кваліфікованих фахівців дозволяє значно підвищити рівень кіберзахисту та забезпечити безперервність роботи корпоративної мережі.

Узагальнюючи викладене, можна стверджувати, що підвищення рівня захищеності корпоративної мережі із застосуванням IDS/IPS-рішень можливе лише за умови комплексного підходу, який охоплює технічні, організаційні та процедурні аспекти безпеки. Застосування Snort та інших сучасних інструментів, у поєднанні з правильно налаштованою архітектурою, актуальними сигнатурами, аналітичними системами моніторингу та кваліфікованим персоналом, дозволяє ефективно протидіяти широкому спектру кібератак та забезпечує надійний захист корпоративних інформаційних ресурсів.

Висновок до розділу 3

У третьому розділі було здійснено практичне впровадження технології захисту корпоративної мережі від внутрішніх та зовнішніх кібератак із використанням сучасного IDS/IPS-рішення. На основі проведеного аналізу вимог до безпеки було обрано оптимальний інструмент для побудови системи моніторингу та реагування, після чого виконано налаштування його ключових компонентів, створення правил виявлення порушень, конфігурацію мережевих фільтрів та інтеграцію з інструментами аналізу журналів подій.

Практична реалізація дала можливість дослідити роботу системи в реальних умовах мережевого середовища підприємства, а також оцінити її ефективність під час обробки різних типів трафіку та моделювання типових сценаріїв атак. Проведені експерименти продемонстрували, що впроваджене IDS/IPS-рішення здатне своєчасно ідентифікувати спроби мережевого сканування, підбору паролів, несанкціонованого доступу, зараження шкідливим програмним забезпеченням та інші загрози. Тестування також показало значне зменшення кількості пропущених інцидентів, покращення якості фільтрації трафіку та скорочення часу реагування на події безпеки.

Проаналізовано продуктивність обраної системи, її здатності працювати з великими потоками даних та стійкості до навантажень. Результати дослідження підтвердили, що правильне налаштування IDS/IPS у комплексі з механізмами логування та моніторингу забезпечує високий рівень захисту корпоративної мережі без критичного впливу на її пропускну здатність та стабільність.

Загалом практична частина роботи довела можливість ефективного використання IDS/IPS технологій у корпоративній інфраструктурі для забезпечення виявлення та запобігання широкому спектру атак. Отримані результати підтверджують доцільність застосування розробленої конфігурації та можуть слугувати основою для подальшого удосконалення системи кібербезпеки підприємства та масштабування її функціональності.

ВИСНОВКИ

Проведений огляд щодо методів захисту корпоративних мереж дозволив зробити кілька ключових висновків. Класифікація кіберзагроз показала, що корпоративні мережі піддаються як внутрішнім, так і зовнішнім атакам, серед яких найбільш поширеними є шкідливе програмне забезпечення, фішинг, DDoS-атаки та несанкціонований доступ. Розуміння природи загроз є критичним для побудови ефективної стратегії захисту.

Оцінка вразливостей корпоративної інфраструктури виявила типові слабкі місця, такі як неправильна сегментація мережі, слабкі паролі, відсутність моніторингу та застаріле програмне забезпечення, що підкреслює необхідність регулярного аудиту та впровадження багаторівневого захисту.

Огляд сучасних технологій мережевої безпеки, включно з класичними засобами, такими як Firewall, та новітніми рішеннями, зокрема IDS, IPS, SIEM, EDR/XDR і принципами Zero Trust, показав, що комплексне поєднання різних підходів забезпечує ефективний захист корпоративних мереж. Використання політик безпеки, сегментації та багаторівневого захисту дозволяє суттєво зменшити ризик успішного впровадження атак.

Проведений аналіз підтвердив, що сучасна корпоративна мережа потребує інтегрованого підходу до кіберзахисту, який передбачає систематичну оцінку вразливостей, впровадження сучасних технологій безпеки та дотримання принципів багаторівневого захисту.

Проведено комплексний аналіз теоретичних основ функціонування систем виявлення та запобігання вторгненням (IDS/IPS), що є ключовими елементами сучасної інфраструктури кібербезпеки корпоративних мереж. Розглянуто класифікацію IDS/IPS за архітектурними принципами, функціональними можливостями та сценаріями застосування. Детально описано сигнатурний, евристичний, поведінковий та гібридний підходи до виявлення атак, що дозволило визначити їх сильні та слабкі сторони в контексті протидії сучасним кібератакам різного рівня складності.

Проведене порівняння поширених IDS/IPS-рішень – Snort, Suricata, Zeek, Cisco Secure IDS, StoneGate IPS, IBM Security NIPS та McAfee NSP – показало, що кожна система має власні переваги та сфери застосування. Snort вирізняється гнучкістю, відкритим кодом і широкою підтримкою спільноти, тоді як Suricata демонструє вищу продуктивність завдяки багатопотоковій обробці. Промислові рішення на кшталт Cisco, IBM та McAfee забезпечують розширені можливості поведінкового аналізу, кореляції подій, масштабованості та інтеграції в корпоративні екосистеми. Особливої уваги заслуговують системи класу NGIPS, орієнтовані на обробку зашифрованого трафіку, захист від AET-технік та мінімізацію хибних спрацювань.

Досліджено аспекти інтеграції IDS/IPS з платформами SIEM, що є критично важливим для формування комплексної системи моніторингу та реагування на інциденти. Встановлено, що об’єднання IDS/IPS із SIEM забезпечує повноцінну кореляцію подій з різних джерел, покращує точність виявлення атак, зменшує кількість хибнопозитивних спрацювань та підвищує ефективність автоматизованого реагування. Така взаємодія дозволяє отримати цілісне уявлення про безпековий стан корпоративної мережі та оперативно локалізувати загрози.

ПЕРЕЛІК ПОСИЛАНЬ

1. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. Conference Proceedings of 2019 IEEE Inernational Conference on Advanced Trends in Information Theory (IEEE ATIT - 2019) Dezember 18 – 20, 2019, Kyiv, Ukraine. - pp. 244-248. 23.

2. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system.

3. CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference "Information

4. Technologies and Security" (ITS 2019) Kyiv, Ukraine, November 28, 2019. Vol-2577. P.281-291. 24. Корнієнко Б.Я.

5. Кібернетична безпека – операційні системи і протоколи. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken,

6. Deutschland. − 2017. – 122 с. 25. Korniyenko B.Y., Galata L.P. Design and research of mathematical model for information security system in computer network.

7. Науковий журнал «Наукові технології». – 2017, № 2 (34), С. 114 - 118. 102 26.

8. Корнієнко Б.Я. Інформаційна безпека та технології комп’ютерних мереж: монографія.

9. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с. 27.

10. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. Sciences of Europe. – 2016. – V. 2. – No 2 (2). – P. 61 -63. 28.

11. Korniyenko B. The classification of information technologies and control systems. International scientific journal. – 2016. –№ 2. – P. 78 - 81. 29.

12. Корнієнко Б.Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив :монографія. – К.: Вид-во Аграр Медіа Груп, 2014. – 288 с. 30.

13. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources / B.

14. Korniyenko, //CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) Kyiv, Ukraine, November 27, 2018, Vol-2318, - P. 176-187, urn:nbn:de:0074-2318-4.

15. National Cyber Security Centre (NCSC) (UK) Publications. 14. NIST Cybersecurity Framework. (Version 1.1). (2018). National Institute of Standards and Technology, U.S. Department of Commerce. [Електронний ресурс]. URL: {посилання на документ}.

16. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.

17. Official documentation from network equipment vendors (e.g., Cisco, Juniper, Huawei) about configuring secure network devices.

18. RFC (Request for Comments) documents from IETF related to network security protocols and practices.

19. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.

20. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.

21. White papers and technical documentation from leading cybersecurity solution providers (e.g., Palo Alto Networks, Fortinet, Cisco, Check Point, etc.).

22. Закон України “Про захист персональних даних”. (2010). [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

23. Закон України “Про основні засади забезпечення кібербезпеки України”. (2017). [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

24. Кіберзахист компанії в умовах війни: перемагають сучасні технології [Електронний ресурс]. URL: https://hub.kyivstar.ua/news/kiberzahyst-kompaniyi-vumovah-vijny-peremagayut-suchasni-tehnologiyi/

25. Стратегія кібербезпеки України від 26 серпня 2021 року № 447/2021. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

26. Як підтримувати комплексну IT-безпеку компанії – на прикладі інструментів Microsoft [Електронний ресурс]. URL: https://dou.ua/forums/topic/40067/

27. Christopher M. Logistics and Supply Chain Management. Pearson, 2016.

28. Rushton A., Croucher P., Baker P. The Handbook of Logistics & Distribution Management. Kogan Page, 2017.

29. Waters D. Logistics: An Introduction to Supply Chain Management. Palgrave Macmillan, 2019.

30. Ghiani G., Laporte G., Musmanno R. Introduction to Logistics Systems Management. Wiley, 2013.

31. Ballou R. Business Logistics/Supply Chain Management. Pearson, 2010.

32. Bowersox D., Closs D., Cooper M. Supply Chain Logistics Management. McGraw-Hill, 2013.

33. Frazelle E. World-Class Warehousing and Material Handling. McGraw-Hill, 2016.

34. Bartholdi J., Hackman S. Warehouse & Distribution Science. Georgia Tech, 2019.

35. Tompkins J., White J. Facilities Planning. Wiley, 2014.

36. Emmett S. Excellence in Warehouse Management. Wiley, 2005.

37. Dumas M., La Rosa M., Mendling J., Reijers H. Fundamentals of Business Process Management. Springer, 2018.

38. Silver B. BPMN Method and Style. Cody-Cure Press, 2011.

39. Weske M. Business Process Management: Concepts, Languages, Architectures. Springer, 2019.

40. Jeston J., Nelis J. Business Process Management. Routledge, 2014.

41. Harmon P. Business Process Change. Morgan Kaufmann, 2018.

42. Object Management Group (OMG). Business Process Model and Notation (BPMN) 2.0 Specification. 2013.

43. Davenport T. Process Innovation: Reengineering Work Through Information Technology. Harvard Business School Press, 1993.

44. Kurbel K. Enterprise Resource Planning and Supply Chain Management. Springer, 2013.

45. Porter M. Competitive Advantage: Creating and Sustaining Superior Performance. Free Press, 2008.

46. Vom Brocke J., Rosemann M. (eds.). Handbook on Business Process Management. Springer, 2015.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ