

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

магістр

(ступінь вищої освіти)

на тему Аналіз кіберзагроз на об'єктах критичної
інфраструктури держави

(назва теми)

Виконав: студент 6 курсу, групи БК-812м

Спеціальності 125 Кібербезпека

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних і комунікаційних
мереж

ЯНКОВСЬКИЙ В.С

(ПРИЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.

(ПРИЗВИЩЕ та ініціали)

Рецензент НІКУЛІЩЕВ Г.І.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІБтаН

Андрій КОРОТУН

«___» _____ 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ЯНКОВСЬКОГО Вадима Сергійовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз кіберзагроз на об'єктах критичної інфраструктури держави

Analysis of cyber threats on critical state infrastructure facilities

керівник проєкту (роботи) к.т.н., КОРОЛЬКОВ Роман Юрійович,

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 475

2. Строк подання студентом проєкту (роботи) 10 грудня 2023 року

3. Вихідні дані до проєкту (роботи) Проаналізувати кібератаки на критичну інфраструктуру, визначити методи та інструменти для виявлення вразливостей. Розробити ряд рекомендацій для підвищення рівню безпеки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд кібератак та протоколів. Аналіз попередніх атак. Огляд методів та засобів для виявлення кібератак. Рекомендації щодо підвищення кібербезпеки критичної інфраструктури.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 15 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 4	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН	04.09.2023	05.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		08.12.2023

7. Дата видачі завдання «04» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження.	04.09.23 – 18.09.23	
2.	Відбір інформації та літератури, що відповідає отриманому завданню.	19.09.23 – 04.10.23	
3.	Аналіз кібератак на критичну інфраструктуру.	27.09.23 – 10.10.23	
4.	Опис методів та засобів для виявлення та аналізу кібератак	11.10.23 – 15.10.23	
5.	Дослідження інструментів для виявлення та протидії атакам	16.10.23 – 24.10.23	
6.	Аналіз IDS.	24.10.23 – 05.11.23	
7.	Аналіз методів виявлення слабкостей та ризиків.	05.11.23 – 14.11.23	
8.	Розроблення рекомендацій.	15.11.23 – 25.11.23	
9.	Оформлення матеріалів магістерської роботи.	25.11.23 – 05.12.23	

Студент

_____ Вадим ЯНКОВСЬКИЙ
(підпис) (Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

_____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 89 с., 2 табл., 23 рис., 30 джерел.

АНАЛІЗ РИЗИКІВ ЗАГРОЗ, ДЕРЖАВНА БЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, НАЦІОНАЛЬНА БЕЗПЕКА, СИСТЕМИ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ, СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Об'єкт дослідження – кіберзагрози критичної інфраструктури держави.

Предмет дослідження – аналіз кіберзагроз та розробка рекомендацій для їх усунення

Мета роботи – опис видів кіберзагроз та методів протидії ним. Розроблення загальних механізмів та рекомендацій, щодо поліпшення захисту критичної інфраструктури.

Метод дослідження – аналіз наявних кіберзагроз, вивчення реальних випадків кібератак. Аналіз методів захисту інфраструктури.

ABSTRACT

Explanatory note for the master's thesis: 89 pages, 2 tables, 23 figures, 30 sources.

ANALYSIS OF THREAT RISKS, NATIONAL SECURITY, CRITICAL INFRASTRUCTURE, NATIONAL SECURITY, INTRUSION DETECTION AND PREVENTION SYSTEMS, CYBERSECURITY STRATEGIES

The research object is cyber threats to the critical infrastructure of the country.

The research subject is the analysis of cyber threats for the development of recommendations for their elimination.

The aim of the study is to describe the types of cyber threats and methods to counteract them. Development of general mechanisms and recommendations to improve the protection of critical infrastructure.

Research method – analysis of existing cyber threats, study of real cases of cyber attacks. Analysis of critical infrastructure elements. Analysis of methods for protecting infrastructure.

ЗМІСТ

	С.
Перелік скорочень	9
Вступ.....	10
1 Аналіз та дослідження основних кібератак на критичну інфраструктуру.	11
1.1 Критична інфраструктура.....	11
1.2 Класифікація кіберзагроз та їх характеристики, види кібератак	12
1.3 Загрози для критичної інфраструктури держави	14
1.4 Аналіз кібератак на критичну інфраструктуру	16
1.4.1 Скоординована кібератака	16
1.4.2 Атака нульового дня	18
1.4.3 Файлова атака.....	19
1.4.4 Атака вірусом «NotPetya»	20
1.5 Оцінка наслідків кібератак для критичної інфраструктури.....	22
1.6 Аналіз ризиків і вразливостей систем критичної інфраструктури	23
1.7 Протоколи, що є критичними для функціонування критичної інфраструктури	24
1.8 Технології та методи аналізу кіберзагроз.....	25
1.9 Висновки до розділу 1	27
2 Вибір методів та засобів досліджень.....	28
2.1 Обґрунтування вибору методів аналізу кіберзагроз	28
2.1.1 Mitre ATT&CK Framework.....	29
2.1.2 Cyber Kill Chain	31
2.1.3 STRIDE.....	33
2.1.4 OWASP Risk Rating Methodology	34
2.1.5 NIST Cybersecurity Framework.....	35
2.2 Засоби моніторингу та виявлення аномальностей в мережі.....	37
2.2.1 Система виявлення аномалій в мережі (NIDS).....	37

2.2.2 Система виявлення аномалій на основі хосту (HIDS)	39
2.2.3 Гібридна система виявлення вторгнень.....	40
2.3 Використання інструментів для виявлення та аналізу кібератак.....	41
2.3.1 Snort Intrusion Detection System (IDS).....	42
2.3.2 Suricata Network IDS/IPS	46
2.3.3 Wireshark	48
2.3.4 ELK Stack	49
2.4 Методи виявлення слабкостей та ризиків у критичній інфраструктурі..	52
2.4.1 Аудит інформаційної безпеки.....	52
2.4.2 Сканування вразливостей.....	54
2.4.3 Тест на проникнення.....	55
2.4.4 Аналіз архітектури та дизайну системи.....	56
2.4.5 Моделювання загроз	57
2.4.6 Соціальний інжиніринг та освітні заходи	57
2.5 Переваги та обмеження обраних інструментів	59
2.6 Висновки до розділу 2	62
3 Розроблення загальних механізмів та рекомендацій для поліпшення захисту критичної інфраструктури.....	63
3.1 Вибір об'єкта критичної інфраструктури.....	63
3.1.1 Характеристика енергетичної системи.....	64
3.1.2 Загрози для енергетичної системи	65
3.2 Аналіз попередніх атак на об'єкт критичної інфраструктури.....	66
3.3 Вибір фреймворків та механізмів для захисту об'єкта.....	68
3.4 Створення планів навчання та тренувань персоналу	72
3.5 Переваги та обмеження розроблених механізмів	73
Висновки до розділу 3	75
4 Розробка програмного забезпечення для аналізу трафіку	76
4.1 Мета програмного забезпечення	76
4.2 Реалізація аналізатору трафіку на Python	77
4.2.1 Читання списку загрозливих IP-адрес	77

4.2.2	Визначення сигнатур загрозливих пакетів	78
4.2.3	Виявлення потенційних загроз у мережевому трафіку	79
4.2.4	Логування та зберігання інформації про шкідливі пакети	80
4.2.5	Сповіщення про виявлення загроз електронною поштою	81
4.2	Перевірка роботи програми	82
4.4	Переваги та обмеження реалізованого рішення	83
4.5	Висновки до 4 розділу	84
	Висновки	85
	Перелік джерел посилань	87

ПЕРЕЛІК СКОРОЧЕНЬ

- АПКІ – Аналіз потенційних кіберзагроз інфраструктури;
- ІТ – Інформаційні технології;
- МН – Машинне навчання;
- ПЗ – Програмне забезпечення;
- CIP - Система інцидентного реагування;
- СКЗІ – Системи захисту критичної інфраструктури;
- ІІІ – Штучний інтелект;
- DoS – Denial of Service (Атака на відмову в обслуговуванні);
- DDoS – Distributed Denial of Service (Розподілена атака на відмову в обслуговуванні);
- ICMP – Internet Control Message Protocol (міжмережевий протокол керуючих повідомлень);
- ICS – Industrial Control Systems (Промислові системи управління);
- IDS – Intrusion Detection System (Система виявлення вторгнень);
- IP – Internet Protocol address (Адрес Інтернет-протоколу);
- IoT – Internet of Things (Інтернет речі);
- Malware – Malicious Software (Шкідливе програмне забезпечення);
- RAT – Remote Access Trojan (Троян віддаленого доступу);
- SCADA – Supervisory Control and Data Acquisition (Система диспетчерського управління і збору даних);
- SMTP – Simple Mail Transfer Protocol (Простий протокол пересилання пошти);
- SNMP – Simple Network Management Protocol (Простий протокол керування мережею);
- TCP – Transmission Control Protocol (Протокол керування передачею);
- TLS – Transport Layer Security (Захист на транспортному рівні);
- UDP – User Datagram Protocol (Протокол дейтаграм користувача).

ВСТУП

У сучасному цифровому світі кібербезпека стала однією з найбільш актуальних та нагальних проблем, особливо в контексті безпеки держави та її критичної інфраструктури. Критична інфраструктура, така як енергетичні системи, транспортні мережі, телекомунікаційні системи, фінансові установи та інші, є невід'ємною складовою нашого суспільства, а її порушення може мати надзвичайно серйозні наслідки для функціонування держави та безпеки її громадян.

Зростання кількості та складності кіберзагроз створює серйозну загрозу безпеці. Вороги та кіберзлочинці постійно шукають нові способи атак на системи, які забезпечують нормальну роботу держави. Кібератаки можуть призвести до переривання енергопостачання, руйнування транспортних мереж, розколу комунікаційних систем, втрати фінансових ресурсів та витоку конфіденційної інформації. Отже, розуміння кіберзагроз, яким піддається критична інфраструктура, та розробка ефективних механізмів захисту є надзвичайно важливим завданням для забезпечення безпеки держави та її громадян.

Мета цієї роботи полягає в проведенні аналізу кіберзагроз для критичної інфраструктури, що допоможуть попереджати та мінімізувати наслідки кібератак. Дослідження таких атак допоможе визначити найбільш поширені типи загроз та їхні наслідки для критичної інфраструктури. Це включає в себе: розробку системи виявлення та попередження кібератак, розробку механізмів захисту та відновлення після кібератак. Будуть розглянуті інструменти та методи, які можна використовувати для ефективного контролю та забезпечення безпеки критичної інфраструктури.

Завершення цього дослідження сприятиме подальшому розвитку кібербезпеки та забезпеченню безпеки критичної інфраструктури.

1 АНАЛІЗ ТА ДОСЛІДЖЕННЯ ОСНОВНИХ КІБЕРАТАК НА КРИТИЧНУ ІНФРАСТРУКТУРУ

1.1 Критична інфраструктура

Критична інфраструктура є важливим фактором для стабільного функціонування будь-якої держави, включаючи Україну. Критична інфраструктура – сукупність об'єктів критичної інфраструктури [1]. Вона представляє собою сукупність систем, об'єктів і ресурсів, які мають вирішальне значення для забезпечення життєдіяльності суспільства, безпеки нації та стійкості економіки.

Критична інфраструктура України охоплює різні галузі, що включають енергетичні системи, транспортні мережі, телекомунікаційні системи, фінансові установи та інші ключові компоненти. Енергетичні системи забезпечують постачання електроенергії, газу та інших видів енергії для підтримки функціонування промисловості, житлового сектору та інших сфер господарства. Транспортні мережі, такі як дороги, залізниці, порти та аеропорти, забезпечують мобільність товарів, послуг та населення в межах країни та зовнішніх зв'язків. Телекомунікаційні системи забезпечують зв'язок і передачу інформації між людьми, органами влади, бізнесом та іншими суб'єктами. Фінансові установи здійснюють функції зберігання та переказу коштів, фінансування господарської діяльності та інших фінансових операцій.

Розуміння та оцінка критичної інфраструктури України є необхідною передумовою для розробки та впровадження ефективних заходів з кібербезпеки. Цей процес включає огляд і аналіз систем, компонентів та процесів, які є складовими критичної інфраструктури, а також визначення їхнього стратегічного значення для суспільства та економіки. Тільки зрозумівши, що вважається критичним, можна спрямувати ресурси на розробку і впровадження ефективних заходів кіберзахисту, що дозволить запобігти та мінімізувати наслідки можливих кібератак на ці важливі системи.

Аналіз критичної інфраструктури України дає можливість розпізнати уразливі місця та ідентифікувати потенційні загрози, які можуть вплинути на ці системи. Враховуючи швидкий розвиток технологій та збільшення кількості кіберзагроз, важливо визначити потенційні ризики та розробити превентивні заходи для забезпечення стійкості та надійності критичної інфраструктури.

Отже, розуміння, огляд та аналіз критичної інфраструктури України є важливими кроками для розробки стратегій та заходів з кібербезпеки. Цей процес допомагає виявити потенційні загрози, оцінити ризики та визначити пріоритети у забезпеченні безпеки та стійкості критичної інфраструктури держави.

1.2 Класифікація кіберзагроз та їх характеристики, види кібератак

Кіберебезпека є невід'ємною складовою сфери інформаційної безпеки, що зосереджується на захисті комп'ютерних систем, мереж та даних від зловмисних атак, несанкціонованого доступу, розповсюдження шкідливих програм та витоку інформації. У контексті кіберебезпеки мається на увазі комплекс заходів, які спрямовані на запобігання, виявлення та реагування на кіберзагрози з метою забезпечення конфіденційності, цілісності та доступності інформації. Це включає захист комп'ютерних систем та мереж від різних типів загроз, таких як віруси, шкідливе програмне забезпечення, атаки з метою витоку даних та інші.

Кіберзагрози можуть бути класифіковані за різними критеріями, включаючи їх характеристики та способи впровадження. Розглянемо деякі типи кіберзагроз та їх характеристики:

- віруси – це програми, які прикріплюються до інших файлів або програм та розповсюджуються, завдаючи шкоди комп'ютерній системі, включаючи втрату даних або недоступність системи;

- хробаки – це саморозповсюджувані програми, які поширюються через комп'ютерні мережі і використовують уразливості для незаконного доступу до системи або розповсюдження шкідливого коду;
- троянські програми – це програми, які приховано встановлюються на комп'ютерну систему з метою злочинної діяльності, такої як викрадення даних, шпигунство або встановлення засобів дистанційного керування;
- фішинг – це метод соціально-інженерної атаки, який включає відправку шахрайських повідомлень або веб-сторінок, що підробляють легітимні ресурси, з метою обману користувачів і отримання конфіденційних даних, таких як паролі або номери кредитних карток;
- DDoS атаки – це атаки, які спрямовані на переповнення мережевих ресурсів або послуг з метою зниження доступності системи для легітимних користувачів [2];

Це деякі приклади кіберзагроз, які можуть становити потенційну небезпеку для критичної інфраструктури держави.

Основні види кібератак можна розглядати з різних перспектив, включаючи їх мету та спосіб впровадження. Ось деякі з них:

- мережеві атаки – спрямовані на комп'ютерні мережі та інфраструктуру. Наприклад, атаки на рівень мережевого протоколу, такі як атаки "переповнення буфера" (buffer overflow), пакетні атаки або "людина-в-середині" (man-in-the-middle) атаки, де зловмисник перехоплює та змінює комунікацію між двома сторонами;
- прикладні атаки – атаки використовують вразливості у програмах та сервісах, що працюють на комп'ютері. Приклади таких атак включають атаки на веб-додатки, використання вразливостей у програмному забезпеченні, фішингові атаки через електронну пошту або соціальні мережі;
- атаки на ідентифікацію та аутентифікацію – спрямовані на отримання неправомірного доступу до системи або облікових записів шляхом обходу аутентифікаційних механізмів. Приклади включають атаки з використанням

слабких паролів, перехоплення аутентифікаційних даних або використання крадених облікових записів;

- фізичні атаки – атаки спрямовані на компоненти інфраструктури, фізичні системи або пристрої. Наприклад, фізичний доступ до серверного приміщення з метою крадіжки чутливої інформації або встановлення шпигунського обладнання;

- соціально-інженерні атаки – атаки, які використовують маніпуляцію психологічними аспектами для отримання несанкціонованого доступу до системи. Наприклад, використання соціальних мереж або телефонних розмов для впливу на людей та отримання конфіденційної інформації;

1.3 Загрози для критичної інфраструктури держави

Критична інфраструктура держави представляє собою комплекс об'єктів, систем і мереж, які є життєво важливими для функціонування суспільства, економіки та національної безпеки. Ці об'єкти включають енергетичні системи, транспортні мережі, комунікаційні інфраструктури, водопостачання, фінансові установи, системи охорони здоров'я та інші системи, які забезпечують життєдіяльність і безпеку громадян.

Об'єкт критичної інформаційної інфраструктури – об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [1].

Загрози для критичної інфраструктури держави можуть виникати з різних джерел і мати різні форми прояву. Найбільш поширеними загрозами є кібератаки, тобто злочинні дії, спрямовані на комп'ютерні системи та мережі з метою завдання шкоди, незаконного отримання інформації або переривання функціонування інфраструктури.

Кібератаки можуть бути класифіковані за різними ознаками, такими як масштаб, спосіб здійснення, мотивація зловмисника і наслідки для системи. Деякі з найпоширеніших видів кібератак включають DDoS (атака на відмову в обслуговуванні), фішинг, введення шкідливих програм (malware) на комп'ютерні системи, злам паролів, викрадення даних, саботаж, шпигунство та багато інших.

Коли мова йде про критичну інфраструктуру держави, наслідки кібератак можуть бути надзвичайно серйозними. Наприклад, атаки на енергетичні системи можуть призвести до зупинки електропостачання в широкому масштабі, порушення роботи промислових об'єктів та суттєвого впливу на економіку країни. Кібератаки на транспортні системи можуть спричинити переривання руху транспорту, зупинку міжміських комунікацій і порушення логістичних процесів. Загрози для критичної інфраструктури можуть включати атаки на енергетичні системи, транспортні мережі, комунікаційні інфраструктури, фінансові установи, системи охорони здоров'я тощо.

Для ефективного захисту критичної інфраструктури держави необхідно розробити і впровадити механізми захисту, які враховують специфіку кожного сектору. Це може включати використання сучасних систем захисту, моніторингу та виявлення інцидентів, розробку політик безпеки, тренінги персоналу, створення резервних копій і відновлення даних, а також налагодження співпраці з іншими державними органами, приватними компаніями і міжнародними організаціями.

Аналіз загроз для критичної інфраструктури держави включає оцінку потенційних сценаріїв атак, виявлення вразливостей і розробку заходів захисту. Для ефективного захисту критичної інфраструктури держави необхідно розробити комплексну стратегію, що включає технічні заходи, організаційні заходи та правові заходи.

1.4 Аналіз кібератак на критичну інфраструктуру

1.4.1 Скоординована кібератака

Кібератака росії на Україну стала першим випадком успішної кібератаки на енергетичну інфраструктуру. Випадок стався 23.12.2015 була проведена кібератака на внутрішню мережу «Прикарпаття обленерго» [2]. Внаслідок цього була порушена робота 30 станцій, 230 тисяч людей залишались без світла протягом декількох годин. Кіберзлочинці отримали доступ до мережі «Прикарпаття обленерго» завдяки зараженню комп'ютера співробітника троянській програмі «BlackEnergy».

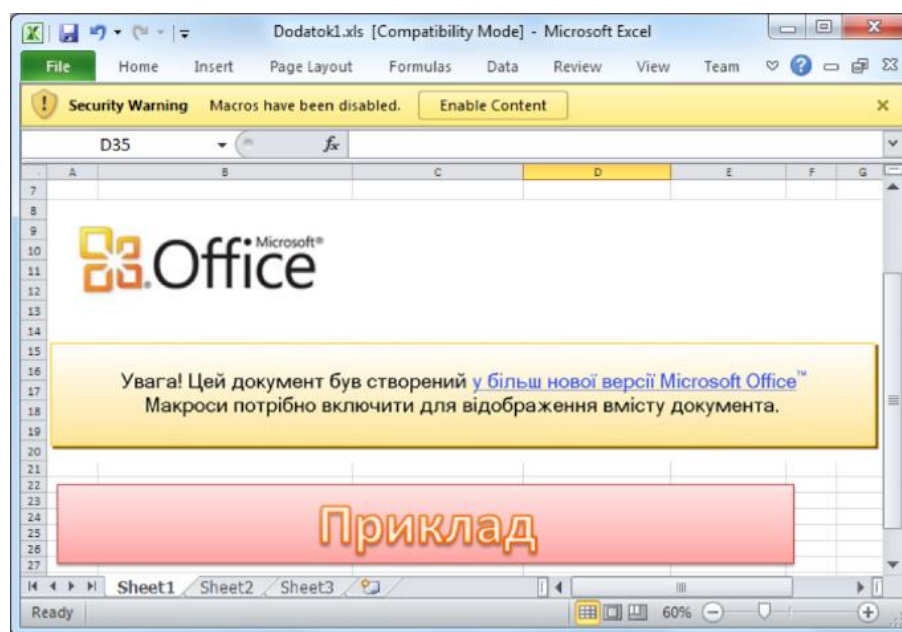


Рисунок 1.1 - Знімок екрану відкритого документу, зараженого трояном BlackEnergy [4]

Спочатку злочинці заразили головні сервери, що контролюють електропостачання, після було проникнення в мережу співробітника завдяки бекдору.

Для скидування зловмисного ПЗ було використано макрос скрипт Excel. Інфіковані таблиці були спрямованною фішинговою атакою проти ІТ-персоналу та системних адміністраторів, які відповідали за розподіл електроенергії в Україні. Було зібрано логіни та поролі, які використовували працівники для віддаленого підключення до мережі «SCADA» [3]. Зловмисникам вдалося отримати доступ до внутрішньої мережі, що дало їм змогу змінити конфігурації пристроїв безперебійного живлення, які забезпечували енергопостачання двох диспетчерських центрів. Крім того, було введено шкідливий код, який дозволяв відправляти віддалені команди та контролювати запобіжні системи. Отримання цих даних відіграло важливу роль у здійсненні зазначених злочинних дій.

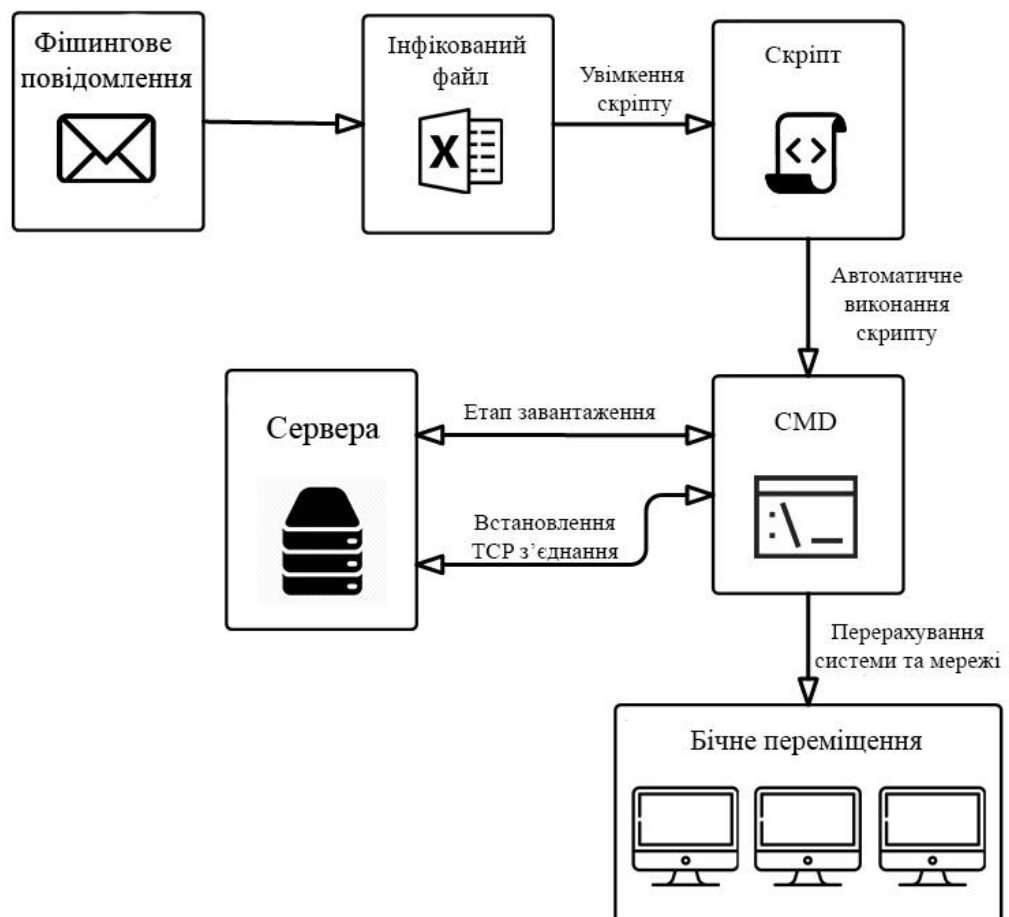


Рисунок 1.2 – Принцип роботи інфікованого макрос скрипту Excel.

В 2023 році більшість хакерів працюють в організаціях, а не самостійно, як це було раніше. Кібератаки можуть бути частиною війни, де не використовуються традиційні військові складові (наприклад важка техніка, солдати і тд.), а використовуються кібернапади, впливання на соціальні мережі, дестабілізація суспільства і т.д.

1.4.2 Атака нульового дня

Ця атака сталася 18 грудня 2016 року, на підстанцію «Північна», яка знаходиться в Києві. Наслідками цієї атаки було знеструлення північної частини правого берегу Києва і районів Київської області. В результаті успішної атаки вдалося відключити підстанцію від якої живилися підприємства, державні установи та цивільне населення [2]. Першим цю подію прокоментував очільник Укренерго Всеволод Ковальчук, 18 грудня він зробив відповідну заяву на своїй сторінці у Facebook [5]. До 11 січня 2017 р. не було відомо, що стало причиною відключення споживачів північної частини правобережжя Києва та прилеглих районів Київської області, доки не з'явилася публікація BBC [6], де з посиланням на компанію ISSP (Information Systems Security Partners) стало відомо, що це була кібератака.

Атака нульового дня – це тип кібератаки, яка використовує вразливість в програмному забезпеченні, про яку розробники ще не знають або не встигли виправити. Цей термін походить від фрази "нульовий день", що означає, що звичайній користувач або розробнику ПЗ ще не відомо про цю вразливість, тому він має "нульові" можливості попередження або захисту від атаки. Таким чином атаки нульового дня є особливо складними для виявлення і захисту.

Критична інфраструктура держави, така як енергетичні системи, транспортні мережі та комунікаційні інфраструктури, знаходяться під постійною загрозою кібератак. Зловмисники зовнішнього походження, такі як

державні хакерські групи або кіберзлочинці, можуть намагатись здійснити кібератаки на ці системи з метою завдання шкоди та викликання хаосу в державі.

1.4.3 Файлова атака

Масштабна кібератака, яка відбулась 6 грудня 2016 року на сайти Міністерства фінансів, Держказначейства, Пенсійного фонду, що призвела до знищення інформації та вимкнення обладнання, що призвело до серйозних затримок у бюджетних виплатах на суму в сотні мільйонів гривень [2]. Після цієї атаки Кабмін виділив 80 мільйонів гривень для захисту від хакерів. Щоб вимкнути сервери державних фінансових установ, злоумисники використали програму "KillDisk", яка призначена для знищення або перезапису критично важливих системних файлів, а також троянську програму "BlackEnergy", яка була використана у скоординованій атаці, яка описується в 2.1.

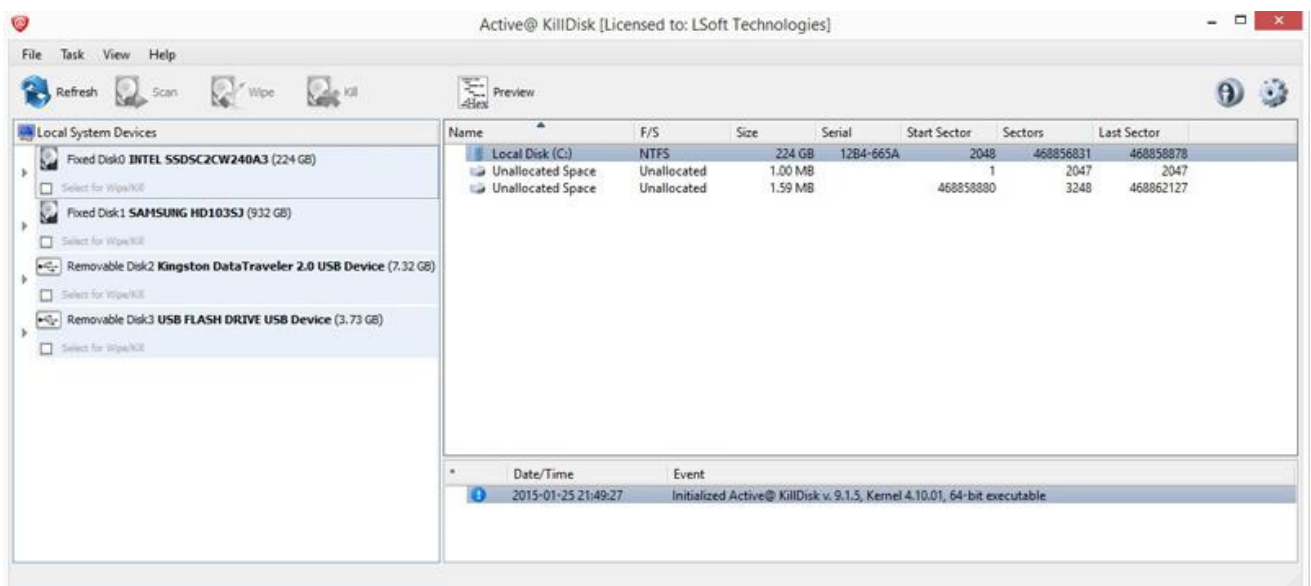


Рисунок 1.3 – Програмне забезпечення KillDisk [3]

1.4.4 Атака вірусом «NotPetya»

NotPetya, також відомий як ExPetr, Petya, GoldenEye або Nyetya, був руйнівним шкідливим програмним забезпеченням, яке з'явилося 27 червня 2017 року. Воно спрямовувалося на комп'ютери в основному в Україні, але також поширилося по всьому світу, вплинувши на численні організації та спричинивши значні розлади.

Завдяки цій кібератаці було заражено більше 12 тисяч комп'ютерів, більшість з яких належала приватним українським організаціям, а також Урядам, банкам, державним енергетичним установам, аеропортам, метрополітену [2].

Вірус поширювався за допомогою фішингового електронного листа, який містив заражений документ Microsoft Office. Коли жертва відкривала документ, то вірус запускався та зашифровував всі файли на комп'ютері, включаючи системні. Він також перезаписував головний завантажувальний запис (MBR), що робило неможливим завантаження ОС.

Атака на медичну установу. В США Sutter Davis Hospital, виявив, що її системи закривали в червні 2017 року кібератаку під назвою Notpetya, який був названий у Wired Magazine "Найбільш руйнівний кібератака в історії". Згідно з історією Енді Грінберга, частина нападу полягала в тому, щоб надсилати підроблені повідомлення про викуп на комп'ютери, і, хоча користувачі обговорювали оплату викупу, зловмисне програмне забезпечення незворотно зашифровувало свої комп'ютери [7].

NotPetya спочатку маскувався під атаку шифрувального вірусу (ransomware), подібно до оригінального вірусу Petya. Однак його головною метою було завдання масштабної шкоди, а не отримання викупу. Воно використовувало вразливості в операційній системі Windows, зокрема використовувало експлоіти EternalBlue і EternalRomance, які походили від Сполучених Штатів, але потрапили в публічний доступ.

Вірус вимагав викуп у розмірі 300 доларів США в біткоїнах за розшифровку файлі. В Україні атака призвела до закриття підприємств, банків та державних установ.

Відповідальність за атаку було покладено на російське хакерське угруповання Fancy Bear.

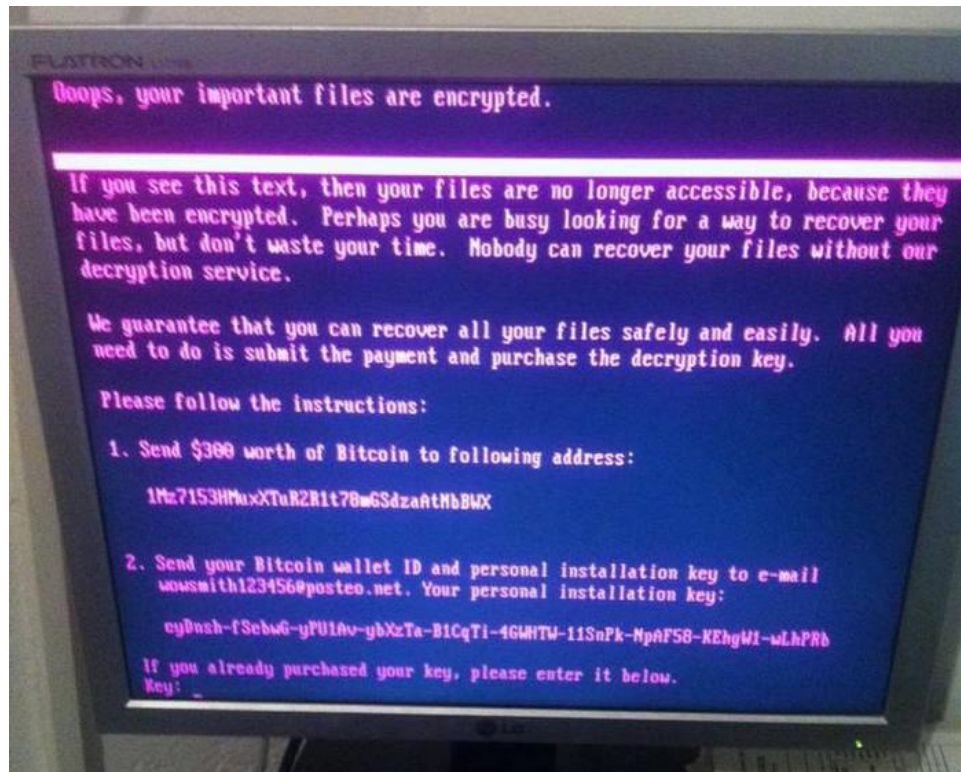


Рисунок 1.4 - Записка про викуп NotPetya відображається у зараженій системі [7]

Атака NotPetya наголошує на важливості ретельних заходів кібербезпеки, таких як своєчасне встановлення оновлень безпеки, впровадження сегментації мережі, створення резервних копій даних та навчання користувачів щодо захисту від фішингу та соціально-інженерних загроз. Це слугує нагадуванням для організацій та осіб про необхідність бути пильними та активно захищати свої системи від постійно змінюючихся кіберзагроз.

1.5 Оцінка наслідків кібератак для критичної інфраструктури

Оцінка наслідків кібератак для критичної інфраструктури передбачає аналіз потенційних наслідків, які можуть виникнути в результаті успішної атаки на системи критичної інфраструктури. Цей процес допомагає визначити масштаб і вплив можливих інцидентів на функціонування та безпеку інфраструктури, а також оцінити можливі збитки і наслідки.

Оцінка наслідків включає наступні аспекти:

- втрата функціональності. В критичній інфраструктурі атаки можуть спричинити втрату функціональності, наприклад, зупинку роботи систем, зниження продуктивності або відмову в обслуговуванні. Наслідки можуть бути особливо серйозними, якщо це стосується систем, відповідальних за життєво важливі послуги, такі як електропостачання, транспортна система чи медичні послуги;

- порушення безпеки. Кібератаки можуть призвести до порушення безпеки інфраструктури, зокрема зламу систем аутентифікації та авторизації, отримання несанкціонованого доступу до конфіденційної інформації, втрати або пошкодження даних, а також зниження довіри до системи. Це може мати серйозні наслідки для фінансової стійкості, репутації та взаємодії з користувачами інфраструктури;

- втрата даних. Критична інфраструктура зазвичай містить великі обсяги важливих даних. Успішна кібератака може призвести до втрати або пошкодження цих даних, що може мати далекосяжні наслідки. Наприклад, втрата медичних записів може загрожувати безпеці та життю пацієнтів, а втрата фінансової інформації може призвести до фінансових збитків і порушення довіри;

- фінансові збитки. Успішні кібератаки можуть мати значний вплив на фінансову стійкість організацій, що володіють та управляють критичною інфраструктурою. Вони можуть призвести до втрати прибутку, великих витрат

на відновлення систем та інфраструктури, втрати довіри партнерів та клієнтів, а також судових позовів і штрафів;

Оцінка наслідків кібератак для критичної інфраструктури вимагає використання аналітичних методів, статистичних даних, сценарійного аналізу та експертної оцінки. Вона допомагає усвідомити можливі ризики та наслідки, що виникають при атаках на критичну інфраструктуру, і сприяє прийняттю ефективних заходів з попередження та відповіді на такі загрози.

1.6 Аналіз ризиків і вразливостей систем критичної інфраструктури

Аналіз ризиків та вразливостей систем критичної інфраструктури допомагає виявити потенційні проблеми та визначити заходи з підвищення безпеки. Цей аналіз включає ідентифікацію потенційних загроз, оцінку вразливостей і розробку стратегій захисту.

Для прикладу, в разі енергетичної системи можуть існувати вразливості в мережевих комунікаціях, системах керування та моніторингу. Якщо зловмисникам вдасться скомпрометувати ці системи, вони можуть отримати контроль над енергетичними вузлами та вплинути на постачання електроенергії.

Одним із способів аналізу ризиків і вразливостей є проведення пенетраційного тестування, де експерти з етичного хакінгу спробують зламати системи, щоб виявити потенційні проблеми. Також важливо встановлювати оновлення програмного забезпечення, використовувати сильні паролі та застосовувати шифрування для захисту інформації.

Важливим елементом аналізу ризиків є ідентифікація потенційних загроз. Це можуть бути зловмисні програми, хакерські атаки, фізичні вторгнення, соціальний інжиніринг та інші види кіберзагроз. Для виявлення цих загроз можна використовувати дані з журналів подій, інцидентів безпеки,

відомостей про загрози, а також інформацію зі зовнішніх джерел, таких як спеціалізовані організації з кібербезпеки та урядові органи. Вразливості можуть бути пов'язані з програмним забезпеченням, мережевими протоколами, фізичною інфраструктурою, політиками безпеки та іншими аспектами систем. Для виявлення вразливостей можуть використовуватись автоматизовані інструменти сканування, пентестинг (тестування на проникнення) та аудит безпеки. Після виявлення вразливостей проводиться аналіз ризиків, де оцінюється потенційний вплив експлуатації цих вразливостей та імовірність їх використання зловмисниками. На основі отриманих результатів можна визначити пріоритети щодо вжиття заходів для зменшення ризиків. Це можуть бути заходи технічного захисту, вдосконалення політик безпеки, навчання персоналу або впровадження систем моніторингу та виявлення інцидентів [8].

Детальний аналіз ризиків і вразливостей систем критичної інфраструктури демонструє важливість ідентифікації потенційних загроз, оцінки їх впливу та виявлення вразливостей. Це допомагає усвідомити потенційні ризики та прийняти заходи для забезпечення безпеки та стійкості систем.

1.7 Протоколи, що є критичними для функціонування критичної інфраструктури

Критична інфраструктура використовує різні протоколи для свого функціонування, і важливо моніторити ці протоколи для забезпечення безпеки та надійності систем. Ось кілька специфічних протоколів, які можуть бути визначені як критичні для функціонування критичної інфраструктури:

- SCADA-протоколи (Modbus, DNP3, OPC). У контексті систем автоматизованого контролю та збору даних (SCADA), протоколи такі як

Modbus, DNP3 та OPC дозволяють взаємодіяти з контролерами та супервізорами, забезпечуючи ефективний моніторинг та управління фізичними процесами [9](виробництво електроенергії, хімічна промисловість, водопостачання та інші.);

- Industrial Control Systems (ICS). Протоколи, такі як OPC, EtherNet/IP та PROFINET, використовуються в системах управління промисловими процесами для ефективної автоматизації та взаємодії з різними пристроями та системами;

- IEC 61850: Стандарт IEC 61850 визначає протоколи для автоматизованих систем управління енергетичними мережами, гарантуючи надійність електропостачання та безпеку електроенергетичних систем; Серія стандартів IEC 61850 є провідною стандартною технологією регулює взаємодію в домені автоматизації [10];

- TLS/SSL (Transport Layer Security/Secure Sockets Layer). Використовується для шифрування комунікації в мережах, забезпечуючи конфіденційність та цілісність даних. Важливий для захисту інформації в критичних секторах;

- протоколи, такі як TCP, UDP та IP є основою для мережевого зв'язку та передачі даних;

- SNMP (Simple Network Management Protocol) використовується для моніторингу та управління мережевими пристроями, такими як роутери, комутатори і сервери;

1.8 Технології та методи аналізу кіберзагроз

Використання систем інтелектуального аналізу даних для виявлення загроз. Для виявлення потенційних кіберзагроз можуть використовуватись системи інтелектуального аналізу даних. Ці системи здатні автоматично

аналізувати велику кількість інформації, включаючи журнали подій, мережеві дані та інші джерела, для виявлення незвичайної активності та аномальних паттернів [11].

Наприклад, системи машинного навчання можуть використовуватись для аналізу мережевого трафіку та виявлення аномальних з'єднань або поведінки. Це дозволяє операторам інфраструктури швидко виявляти потенційні загрози та приймати відповідні заходи.

Використання розподілених сенсорних мереж для збору інформації. Розподілені сенсорні мережі можуть бути використані для збору інформації про потенційні кіберзагрози. Ці мережі складаються з різних сенсорів, розташованих в різних місцях критичної інфраструктури. Сенсори можуть виявляти зміни в мережевому трафіку, спроби несанкціонованого доступу або інші аномалії.

Наприклад, сенсори можуть бути розташовані на енергетичних підстанціях, транспортних вузлах або вузлах зв'язку. Вони можуть надсилати дані до централізованої системи, яка аналізує інформацію та виявляє загрози.

Використання системи інцидентного реагування. Система інцидентного реагування (CIR) грає важливу роль у виявленні, аналізі та реагуванні на кібератаки. CIR включає процеси, процедури та технології, які допомагають ефективно реагувати на інциденти та забезпечувати швидке відновлення послуг [12].

Це може включати автоматизовані системи виявлення інцидентів, інструменти для аналізу загроз, командний центр для координації реагування та спілкування зі зацікавленими сторонами. CIR також включає плани неперервності бізнесу та процедури відновлення після інциденту.

Цей аналіз потенційних кіберзагроз для критичної інфраструктури держави показує, що існує значна кількість загроз як зовнішнього, так і внутрішнього походження. Аналіз ризиків та вразливостей систем, використання технологій аналізу даних та розподілених сенсорних мереж, а

також впровадження системи інцидентного реагування є важливими компонентами забезпечення безпеки критичної інфраструктури.

1.9 Висновки та аналіз результатів

В цьому розділі було розглянуто комплексний погляд на проблематику кіберзагроз, спрямованих на об'єкти критичної інфраструктури держави. Ознайомившись з тим що представляє собою критична інфраструктура, було проведено аналіз кіберзагроз та виокремлено основні характеристики та види кібератак.

Загрози для критичної інфраструктури, а саме скоординовані атаки, атаки нульового дня, файлові атаки та атака вірусом «NotPetya» надають розуміння як вони впливають на функціонування та безпеку об'єктів критичної інфраструктури.

Визначено ключові протоки, які становлять велике значення для стабільної роботи критичної інфраструктури, а також представлені технології та методи аналізу кіберзагроз.

Цей аналіз може становити основу для подальшого огляду методів та засобів, які зможуть допомогти уникнути небажаних наслідків від кібератак та реалізації заходів з підвищення стійкості систем критичної інфраструктури перед сучасними кіберзагрозами.

2 ВИБІР МЕТОДІВ ТА ЗАСОБІВ ДОСЛІДЖЕНЬ

2.1 Обґрунтування вибору методів аналізу кіберзагроз

Для досягнення ефективного аналізу кіберзагроз на критичну інфраструктуру вибрані конкретні методи, які враховують унікальні властивості цього типу об'єктів та небезпеки, які їм загрожують. Вибір методів аналізу базується на:

- універсальності та адаптабельності – вибрані методи є універсальними і можуть бути адаптовані до різних видів критичної інфраструктури. Універсальність та адаптабельність є одним з найважливіх пунктів, оскільки об'єкти критичної інфраструктури включають у собі елементи енергетики, транспорту, комунікацій і т.д;

- врахуванні специфічних загроз – вибрані методи враховують специфічні загрози з якими може зіткнутися критична інфраструктура. Наприклад аналіз нульових днів може допомогти виявити нові, раніше невідомі атаки, які можуть бути використані для цілеспрямованого вторгнення;

- системному підході – за допомогою обраних методів можна провести аналіз на різних рівнях системи, тобто від окремих компонентів до цілісних мереж. Цей підхід дозволить виявити не тільки конкретні вразливості, але і аналізувати взаємодію між компонентами в контексті загальної кібербезпеки;

- моніторингу в реальному часі – однією з головних переваг обраних методів є моніторинг в реальному часі. Цей метод дозволяє оперативно реагувати та сповіщати про загрози, а також запобігати серйозним наслідкам кібератак, забезпечуючи безперервність функціонування критичної інфраструктури;

- сумісності з сучасними технологіями – обрані методи аналізу повинні бути сумісними з сучасними технологіями та інфраструктурою, яка використовується у сфері кібербезпеки. Це робить обрані методи ефективними в контексті швидкозмінюваних варіацій кіберзагроз;

– досвіді та результаті – обрані методи мають успішний досвід застосування в подібних дослідженнях та випробуваннях. Це забезпечить певний рівень вірогідності успіху в сфері кібербезпеки;

Обрані методи не лише забезпечують високий рівень об'єктивності та достовірності результатів, а також враховують специфіку критичної інфраструктури, що робить їх найкращими інструментами для аналізу кіберзагроз критичної інфраструктури.

2.1.1 Mitre ATT&CK Framework

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це база даних, яка використовується для опису дій та поведінки кіберзлочинців. Mitre ATT&CK надає відображення тактик, технік та процедур, які використовують кіберзлочинці або команда Red Team при імітації реальної кібератаки. База знань Mitre ATT&CK використовується як основа для розробки конкретних моделей загроз і методологій у приватному секторі, в уряді та в спільноті продуктів і послуг кібербезпеки [13].

Основні компоненти фреймворку Mitre ATT&CK включають:

– матричну структуру – фреймворк організований у матриці, які представляють різні платформи, такі як Enterprise, Mobile та Cloud. Матриця поділена на стовпці, де можна побачити тактику та рядки, що представляють техніки атак;

– тактика – це вискорівневі цілі, які атакуючи, тобто зловмисники або фахівці з етичного хакінгу прагнуть досягти під час атаки. Приклади тактик включають початковий доступ, виконання, постійність, підвищення привілеїв, ухилення від захисту, доступ до облікових;

– техніка – це конкретні методи, які використовують атакуючи для досягнення певної «тактичної» мети, наприклад, техніка під назвою «Виконання» може бути «Інтерфейс командного рядка»;

– процедури – це випадки технік, які були використані. Процедури надають більш конкретні приклади того, як техніка була застосована атакуючими;

– засоби пом'якшення. Фреймворк містить інформацію про рекомендовані заходи пом'якшення та оборонні стратегії для протидії визначеним методам. Це допомагає підприємствам зрозуміти, як краще захищатися від конкретних методів атак або виявляти їх;

– групи та програмне забезпечення. Фреймворк також надає інформацію про групи загроз та конкретне шкідливе програмне забезпечення або інструменти, пов'язані з певними техніками. Ця інформація допомагає приписувати спостережувану поведінку відомим суб'єктам загрози;

– відносини – Mitre ATT&CK містить інформацію про зв'язки між різними елементами, наприклад, які методи зазвичай використовуються разом або якими методами відома конкретна група учасників загрози;

Mitre ATT&CK Framework може відігравати важливу роль в сфері кібербезпеки критичної інфраструктури. Фахівці з кібербезпеки використовують структуру MITRE ATT&CK, щоб покращити своє розуміння кіберзагроз, покращити можливості виявлення загроз і реагування на них. Структура є динамічною та регулярно оновлюється, щоб відобразити мінливий ландшафт кіберза

MITRE ATT&CK допомагає аналізувати та вдосконалювати заходи безпеки для критичної інфраструктури. Розуміння загроз стає можливим завдяки визначенню тактик, технік та процедур, які використовуються кіберзлочинцями при атаках на критичну інфраструктуру, що підвищує обізнаність та сприяє вжиттю відповідних заходів забезпечення.

Фреймворк допомагає розробляти та вдосконалювати заходи безпеки, враховуючи конкретні методи, які можуть бути використані під час атак на

критичну інфраструктуру. Це може включати в себе поліпшення виявлення загроз, впровадження мітігацій та забезпечення стійкості до атак.

Mitre ATT&CK може стати основою для розробки стратегій виявлення та відгуку на інциденти. Цей фреймворк дозволяє організаціям швидше виявляти аномалії, ефективно реагувати на втручання та атаки, надаючи таку необхідну основу.

Співпраця та обмін інформацією про кіберзагрози стають стимулом завдяки Mitre ATT&CK. Фреймворк сприяє співпраці між організаціями та галузевими партнерами, що допомагає уникнути повторюваних атак та вчасно розпізнати нові загрози.

Mitre ATT&CK може використовуватися для тестування вразливостей систем критичної інфраструктури, що допомагає підвищити стійкість до атак і забезпечити ефективні заходи захисту. Застосування MITRE ATT&CK Framework у сфері критичної інфраструктури сприяє створенню більш ефективної та стійкої кібербезпеки, що має велике значення для безпеки держави та суспільства в цілому.

2.1.2 Cyber Kill Chain

Модель Cyber Kill Chain вперше була запроваджена оборонною, інформаційною та технологічною компанією Lickheed Martin, як спосіб розуміння, аналізу та зупинки ворожої активності. Cyber Kill Chain допомагає визначити, яким чином атаки можуть. Основною ціллю Cyber Kill Chain є захист від складних кібератак, під час яких кіберзлочинці витрачають багато часу на спостереження, планування та реалізації атаки. В основному такі атаки включають у собі декілька видів атак, а саме файлової атаки, програм вимагачів, троянів, спуфінгу та методів соціальної інженерії.

Cyber Kill Chain має 7 основних етапів, які включають розвідку, озброєння, доставку, експлуатацію, установку, командування і управління та дія. З плином часу фахівці з кібербезпеки розширили ці етапи, щоб включити 8 крок – монетизація, тобто отримання грошової винагороди від нападу [14].

В рамках моделі Cyber Kill Chain від Lockheed Martin, кіберзлочинці виконують кібератаки, перейшовши через кілька ключових етапів. Починаючи з етапу розвідки, зловмисники активно збирають ретельну інформацію про потенційні жертви, включаючи доменні імена, адреси електронної пошти та деталі про персонал.

На етапі озброєння зловмисники розробляють і вдосконалюють засоби атак, такі як віруси, черв'яки та інші шкідливі програми, які використовуються для інфікування системи жертви. Доставка коду відбувається через різні канали, включаючи електронну пошту та веб-сайти.

Після доставки, настає експлуатаційний етап, коли шкідливий код використовуються вразливості в системі жертви з метою отримання несанкціонованого доступу. У разі успіху на етапі експлуатації, зловмисники переходять до етапу встановлення, де вони встановлюють шкідливе програмне забезпечення на системі з метою збереження довгострокового доступу та контролю.

Після успішного встановлення, зловмисники переходять до етапу командування та управління, який надає їм здатність взаємодіяти та керувати інфікованою системою віддалено. На завершальному етапі, дії, зловмисники реалізують свої основні цілі, які можуть включати крадіжку конфіденційних даних, завдання шкоди або інші кіберзлочинні дії.

Додатковим етап є монетизація, тобто кіберзлочинці вимагають викуп за розшифрування даних, відновлення нормальної роботи сайту або запобіганню витоку інформації.

Ця модель надає організаціям можливість розуміти та виявляти атаки на ранніх етапах, дозволяючи ефективно реагувати та запобігати серйозним наслідкам кіберзагроз.

2.1.3 STRIDE

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) – це методологія аналізу ризиків у сфері кібербезпеки, яка була розроблена в рамках Microsoft. Ця методологія дозволяє ідентифікувати та аналізувати загрози безпеці інформаційних систем, а також визначати заходи для їх запобігання чи пом'якшення. Вона може бути використана як частина процесу проектування безпечних систем або під час аудиту безпеки інформаційних технологій. STRIDE є аббревіатурою, що вказує на шість основних класів загроз безпеці інформаційних систем.

Основні класи загроз STRIDE включають:

- spoofing (підробка) – це загроза пов'язана з можливістю атаки, при якій зловмисник намагається підробити або маскувати свою ідентичність, щоб представлятися як інша особа або система;
- tampering (втручання) – ця загроза виникає, коли зловмисник намагається змінити або порушити цілісність даних або програмного забезпечення;
- repudiation (заперечення) – це стосується можливості відмови від відповідальності за виконані дії, коли суб'єкт системи (користувач або система) відмовляється визнавати свою відповідальність за вчинені дії;
- information disclosure (розголошення інформації) – ця загроза виникає, коли зловмисник отримує несанкціонований доступ до конфіденційної інформації та може її розголошувати;
- denial of service (відмова в обслуговуванні) – це включає загрози, спрямовані на перешкоджання нормальному функціонуванню системи, завдяки чому вона стає недоступною для легітимних користувачів;

– elevation of privilege (підняття привілеїв) – ця загроза полягає в тому, що атакуючий намагається отримати більше привілеїв або доступу, ніж йому дозволено;

Аналізуючи систему за допомогою цих шести класів загроз, фахівці кібербезпеки можуть ідентифікувати потенційні ризики і вживати заходів безпеки для їх запобігання чи пом'якшення. Вона може бути використана як частина процесу проектування безпечних систем або під час аудиту безпеки інформаційних технологій.

2.1.4 OWASP Risk Rating Methodology

OWASP (Open Web Application Security Project) Risk Rating Methodology — це методологія для оцінки ризиків в області кібербезпеки, розроблена OWASP, некомерційною організацією, яка спрямована на поліпшення безпеки програмного забезпечення. Ця методологія допомагає фахівцям в області кібербезпеки визначати та оцінювати різноманітні ризики, пов'язані з веб-додатками та іншими програмними системами. Оцінка ризиків є важливою частиною стратегії кібербезпеки, оскільки вона дозволяє приділяти увагу та ресурси тим аспектам, які можуть мати найбільший вплив на безпеку.

OWASP Risk Rating Methodology використовується для призначення рейтингів ризиків на основі різних факторів, таких як вразливості, загрози, можливість виникнення атаки та наслідки. Вона може бути використана для визначення пріоритетів у впровадженні заходів з покращення безпеки та розробці стратегій реагування на ризики.

Ця методологія допомагає організаціям вирішувати, які кроки вони повинні зробити для зменшення ризиків і підвищення рівня безпеки своїх програмних продуктів та систем.

При використанні OWASP Risk Rating Methodology для оцінки кібербезпеки критичної інфраструктури, оцінка ризиків може враховувати такі аспекти:

- визначення джерел загроз;
- ідентифікація загроз, які можуть бути створені ціми джерелами;
- визначення вразливих місць, які можуть бути використані для атаки;
- визначення несприятливих наслідків, що включаючи економічні, соціальні та безпекові аспекти [15];
- визначення ризиків;
- важливість активів. Врахування важливості окремих компонентів інфраструктури для відновлення та продовження її функціонування;

Оцінка ризиків може допомогти організаціям приймати обґрунтовані рішення щодо вдосконалення кібербезпеки критичної інфраструктури, впровадження ефективних заходів безпеки та планування відновлення в разі атаки чи інших подій. Враховуючи розмаїття вразливостей у критичній інфраструктурі, ця методологія допомагає виокремити найбільш критичні аспекти для подальшого вивчення та запобігання.

2.1.5 NIST Cybersecurity Framework

NIST Cybersecurity Framework (National Institute of Standards and Technology Cybersecurity Framework) – це набір рекомендацій та вказівок, розроблений Національним інститутом стандартів і технологій (NIST) Сполучених Штатів Америки. Цей фреймворк був створений для покращення кібербезпеки в організаціях та інших інфраструктурних системах. NIST є важливим інструментом для захисту критичної інфраструктури. Критична інфраструктура включає у себе системи та об'єкти, які визначаються як

ключові для функціонування суспільства та економіки, і їхнє пошкодження чи знищення може мати серйозні наслідки.

Основний принцип (Framework Core) визначає п'ять функцій кібербезпеки: ідентифікацію, захист, виявлення, реагування та відновлення [16]. Кожна з цих функцій взаємодіє з ризиками та допомагає організаціям розробляти стратегії забезпечення кібербезпеки.



Рисунок 2.1 – Функції кібербезпеки NIST Framework

Рівні впровадження (Framework Implementation Tiers) допомагають визначити ступінь впровадження фреймворку, що відповідає конкретним потребам та можливостям організацій.

Профіль фреймворку (Framework Profile) визначає конкретні цілі та процеси, обрані для впровадження в організаціях на основі їхніх унікальних потреб і обставин.

Цей фреймворк дозволяє організаціям розробляти та впроваджувати стратегії кібербезпеки, враховуючи їхні специфічні умови і виклики. Такий підхід стає особливо важливим в умовах швидко змінюючогося кіберзлочинного середовища, де важливо постійно удосконалювати та підтримувати заходи забезпечення кібербезпеки.

2.2 Засоби моніторингу та виявлення аномальностей в мережі

Сучасні кіберзагрози створюють серйозні проблеми для безпеки критичних об'єктів інфраструктури, акцентуючи увагу на важливості ефективного моніторингу та виявлення аномалій в мережі.

Враховуючи розвиток технологій та постійного збільшення кількості кібератак, важливо визначити найкращі інструменти для моніторингу мережі та виявлення потенційно небезпечних аномалій. В даному розділі будуть розглянуті ключові аспекти вибору та застосування систем виявлення вторгнень (IDS), систем виявлення аномалій (ADS) та інших засобів, які допоможуть забезпечити надійний рівень безпеки критичної інфраструктури.

Впровадження таких засобів стає необхідністю для швидкого реагування на виклики, які завдають кіберзлочинці та попередження про можливі кібератаки.

Важливо враховувати, що кожен обраний інструмент повинен не лише реагувати на наявні кіберзагрози, а й повинен виявляти нові форми атак і аномальностей.

Буде проведено огляд засобів моніторингу мережі та розглянуто їхні основні характеристики

2.2.1 Система виявлення аномалій в мережі (NIDS)

Системи виявлення мережевих атак – це тип системи виявлення вторгнень (IDS) (Network-based Intrusion Detection Systems) – це тип системи виявлення вторгнень (IDS), метою якої є виявлення зловмисних активностей. Основними функціями системи виявлення мережевих атак (NIDS) є аналіз мережевого трафіку, виявлення патернів та сигнатур, які можуть свідчити про

несанкціонований допуск або кібератаку. Деякі системи виявлення мережевих атак можуть взаємодіяти з іншими засобами захисту, такими як системи запобігання вторгнень (Intrusion Prevention Systems). Системи виявлення мережевих атак грають важливу роль у забезпеченні безпеки мережі та допомагають вчасно реагувати на потенційні загрози.

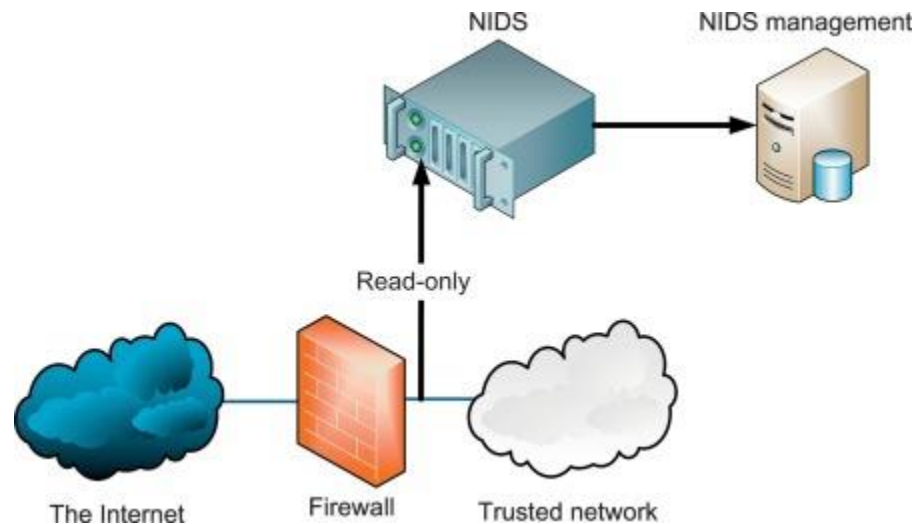


Рисунок 2.2 – Архітектура NIDS [17]

Основні функції NIDS:

- аналіз пакетів. Система виявлення мережевих атак аналізує пакети, що пересилаються по мережі, для виявлення аномалій, що вказують на потенційні атаки;
- сигнатурний аналіз. Система використовуючи базу сигнатур, які представляють відомі патерни атак аналізує сигнатури, які представляють патерни атак;
- аномалійний аналіз. Система підозрілу мережеву активність, яка може свідчити про атаки, що не входять до бази відомих сигнатур. Аномалійний аналіз дозволяє виявляти нові атаки;
- аналіз аномальних з'єднань та підключень. Система моніторить за підозрілими та небажаними мережевими з'єднаннями;

NIDS можуть бути розташовані в різних точках мережі, таких як мережеві вузли, сегменти, периметр мережі чи навіть на рівні провайдерів Інтернет-послуг. Це дозволяє їм ефективно виявляти та реагувати на мережеві загрози.

2.2.2 Система виявлення аномалій на основі хосту (HIDS)

Системи виявлення вторгнень на основі хосту (Host-based Intrusion Detection) – це тип системи виявлення вторгнень (IDS) окремих комп'ютерів або серверів. Основною метою цієї системи є моніторинг активності на окремому хості та виявлення аномалій та ознак несанкціонованого доступу. Популярні приклади систем виявлення інтраверсійних атак включають Tripwire, OSSEC, Snort, Suricata та інші. Ці системи можуть бути встановлені на серверах, робочих станціях та інших критичних хостах для постійного моніторингу їхньої безпеки. Система виявлення вторгнень на основі хосту (HIDS) була першим типом програмного забезпечення для виявлення вторгнень, яку було розроблено, спочатку її використовували на мейнфреймах, де зовнішні вторгнення відбувалися рідко [18].

Основні функції HIDS:

- моніторинг файлів. Система вивчає файли та директорії на хосту та шукає зміни, модифікації до системних ресурсів;
- системні журнали. Система проводить аналіз журналів для виявлення підозрілої активності, такої як несподівані зупинки служб, помилки входу та інші події, які можуть свідчити про несанкціонований доступ;
- мережева активність. Система аналізує мережеву активність на надмірні запити та підозрілі з'єднання;
- моніторинг процесів. Система виявляє зміни конфігурації системи, так як скоріш за все це може свідчити про несанкціоновані дії;

- спостереження за спробами аутентифікації. Система виявляє невдалі спроби входу, обходу системи та інші атаки на функції аутентифікації;

HIDS може використовувати деякі методи для виявлення вторгнень, а саме сигнатурний аналіз, аномалійний аналіз та інші. HIDS може визначити ресурси, що використовуються програмами і оцінити поточний стан системи. Однак він стикається з проблемами, пов'язаними з виконанням у реальному часі [19].

Сигнатурний аналіз використовує заздалегідь визначені шаблони для виявлення відомих атак, в той час як аномалійний аналіз виявляє незвичайну активність, що може бути ознакою нових атак або змін в системному стані.

2.2.3 Гібридна система виявлення вторгнень

Гібридні системи виявлення інцидентів (Hybrid Intrusion Detection System) – це системи, які об'єднують в собі системи виявлення атак на основі хосту (HIDS) та системи виявлення мережевих інцидентів (NIDS). Обидві системи працюють спільно за для забезпечення більш якісного виявлення потенційно небезпечних активностей в інформаційній системі. Ці системи дозволяють компаніям та організаціям ефективно виявляти інциденти, швидко реагувати на них та мінімізувати їх наслідки. Вони також можуть бути використані для виявлення аномалій в різних системах, включаючи мережі зв'язку та системи електронних платежів

Основні функції HIDS:

- комплексний аналіз. Гібридні системи використовують внутрішні та мережеві підходи для комплексного аналізу даних. Це дозволяє глибше розпізнавати атаки, які можуть виявляти аномалії на різних рівнях системи;

- спільна обробка інцидентів – гібридні системи можуть поєднувати інформацію, зібрану з різних джерел, наприклад лог файли і дані мережевих датчиків, щоб отримати цілісну картину потенційних загроз;

- системи виявлення по відхиленнях – HIDS встановлює поведінкові шаблони для нормальної діяльності системи та спостерігає за будь-якими відхиленнями від цих шаблонів. Вони виявляють аномалії, які можуть бути знаком потенційного вторгнення;

- реагування на інциденти – HIDS може надавати рекомендації щодо реагування на виявлені загрози, включаючи автоматичне виведення системи з дії або автоматичне сповіщення адміністраторів про потребу втручання;

Загалом, гібридні системи виявлення інцидентів поєднують в собі різні методи та підходи з метою забезпечення комплексного та ефективного виявлення та реагування на потенційні загрози для безпеки інформаційних систем.

2.3 Використання інструментів для виявлення та аналізу кібератак

Проведення аналізу кіберзагроз на об'єктах критичної інфраструктури вимагає вдосконалених інструментів, які забезпечують надійність, швидкість та глибокий рівень деталізації. Увесь час мережі піддаються великому великому обсягу різноманітних атак.

Далі буде проведено обґрунтування вибору конкретних інструментів для виявлення та аналізу кібератак на критичну інфраструктуру. Кожен обраний інструмент висвітлений з позиції його функціональних можливостей, переваг, а також обмежень. Це допоможе створити повноцінну систему моніторингу та реагування, спрямовану на забезпечення високого рівня кібербезпеки об'єктів критичної інфраструктури.

2.3.1 Snort Intrusion Detection System (IDS)

Snort Intrusion Detection System (далі Snort) – це система виявлення вторгнень (IDS), яка виявляє, ідентифікує та упереджує атаки в комп'ютерних мережах. Основним призначенням Snort є виявлення аномалій та зловживань в мережевому трафіку, допомагаючи забезпечити безпеку систем та баз даних.

До функцій Snort IDS відносяться виявлення вторгнень, система підписів, аналіз пакетів, логування та повідомлення та підтримка протоколів.

Виявлення вторгнень, тобто Snort аналізує мережевий трафік і виявляє потенційно шкідливі або аномальні дії;

Система підписів. Система підписів у Snort IDS використовується для виявлення відомих патернів атак, які вже були ідентифіковані та описані розробниками або спільнотою кібербезпеки. Ця система також називається системою сигнатур або сигнатурним движком.

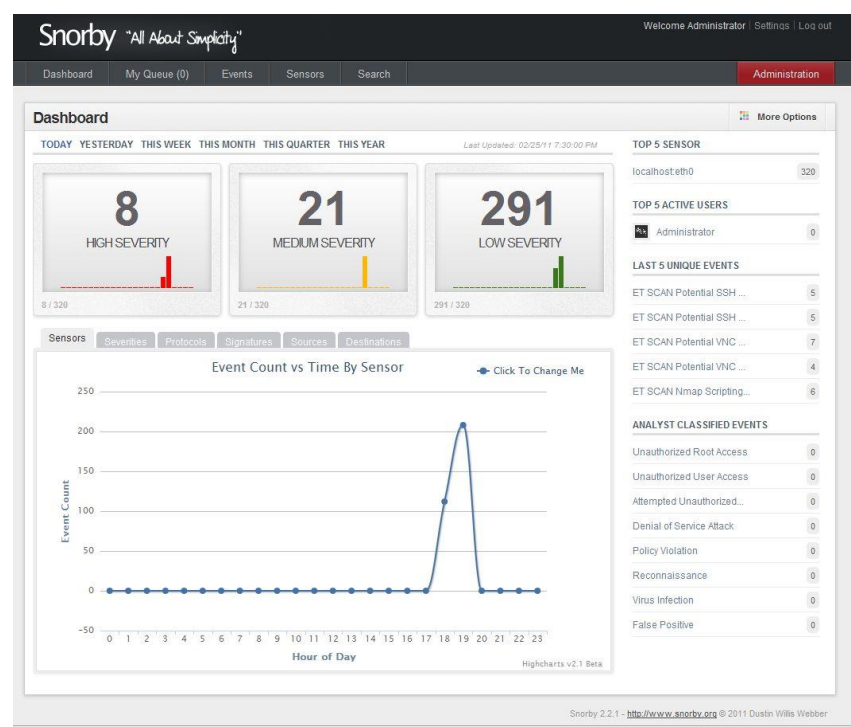


Рисунок 2.3 – Інтерфейс Snort, реалізований завдяки Snorby [20]

Основна ідея полягає в тому, що кожна атака або тип атаки має унікальний «сигнатурний» патерн або характеристику, яку Snort може виявити в мережевому трафіку. Ці сигнатури базуються на відомих вразливостях, характеристиках атак, або конкретних рядках коду, які є характерними для конкретної загрози.

Приклад сигнатури виглядає наступним чином:

```
alert tcp any any -> any 80 (content: "GET /malicious"; msg:"Potential HTTP Attack")
```

У цьому прикладі:

- content:"GET /malicious" – вказує на те, що система буде шукати підстроку "GET /malicious" в HTTP-запитах;
- msg:"Potential HTTP Attack" – текстове повідомлення, яке виводиться, коли виявляється відповідна сигнатура;
- sid:10001 – унікальний ідентифікатор сигнатури.

Коли Snort спостерігає, що мережевий трафік відповідає заданому сигнатурному патерну, він спрацьовує та вживає визначені дії (наприклад, логування, блокування або сповіщення адміністратора).

Аналіз пакетів. Snort IDS використовує систему аналізу пакетів для глибокого розгляду мережевого трафіку та виявлення потенційно шкідливих або аномальних активностей. Система аналізу пакетів у Snort грає ключову роль у виявленні атак, а також в моніторингу та логуванні подій у мережі.

Основні елементи аналізу пакетів Snort включають:

- розпізнавання протоколів. Snort вміє розпізнавати різні мережеві протоколи, такі як TCP, UDP, IP, ICMP, HTTP і інші. Це дозволяє системі аналізувати різні рівні мережевого стеку;
- розділення пакетів. Пакети, які надходять у мережевий інтерфейс, розбиваються на окремі компоненти для подальшого аналізу. Це включає розділення на заголовки та дані, що допомагає Snort отримати доступ до ключових частин пакетів;

- аналіз заголовків. Snort аналізує заголовки пакетів для отримання інформації про джерело та призначення, тип протоколу, порти та інші параметри, що допомагають визначити характеристики мережевого трафіку;
- аналіз даних. Глибокий аналіз реальних даних у мережевих пакетах дозволяє Snort виявляти аномалії або відомі патерни атак, які можуть бути використані для ідентифікації загроз;
- застосування правил. На основі аналізу пакетів і використання системи підписів (сигнатур), Snort застосовує визначені правила для виявлення потенційних вторгнень або аномалій;
- реакції на події. Залежно від встановлених правил та конфігурації, Snort може реагувати на виявлені атаки або аномалії, включаючи логування, сповіщення адміністраторів, або навіть блокування певного трафіку;

Логування та повідомлення у Snort IDS – це процес фіксації та документування виявлених подій та потенційних загроз у мережі. Ці механізми допомагають адміністраторам мережі або кібербезпеки слідкувати за діяльністю мережі, а також реагувати на виявлені атаки чи аномальні ситуації. У Snort IDS це реалізується за допомогою різних методів, таких як лог-файли та повідомлення.

Лог файли:

- alert log. Snort використовує лог-файл для записування виявлених атак або аномалій. Цей файл часто називається alert.log або подібним чином. Він містить інформацію про кожну виявлену загрозу, таку як час, джерело, призначення, тип атаки та інші релевантні дані;
- packet log Цей лог-файл містить записи про весь мережевий трафік, який пройшов через Snort. Це може включати заголовки пакетів та інші деталі, які можуть бути корисними для аналізу та виявлення загроз;

Ці механізми логування та повідомлень в Snort допомагають адміністраторам ефективно виявляти та реагувати на потенційні загрози мережевої безпеки, що сприяє забезпеченню високого рівня безпеки для системи.

Snort IDS підтримує широкий спектр мережевих протоколів, що робить його універсальним інструментом для виявлення атак у різних мережевих середовищах. Серед основних протоколів, які підтримуються Snort, включають:

- TCP (Transmission Control Protocol). TCP є одним з основних мережевих протоколів, і Snort може аналізувати та виявляти атаки, що використовують цей протокол. Визначення TCP-пакетів дозволяє Snort виявляти аномалії та підозрілу активність;

- UDP (User Datagram Protocol). Snort також підтримує UDP, і це важливо для виявлення атак, які використовують цей протокол. UDP використовується для передачі даних без встановлення з'єднання, і атаки через UDP можуть виявлятися на рівні пакетів;

- IP (Internet Protocol). Snort аналізує IP-пакети, що дозволяє виявляти атаки на рівні мережі. Враховуючи IP-адреси та інші характеристики, Snort може виявляти потенційні загрози;

- ICMP (Internet Control Message Protocol). ICMP використовується для передачі повідомлень про помилки та іншої інформації мережевими пристроями. Snort може виявляти атаки або аномалії, пов'язані з використанням ICMP;

- HTTP (Hypertext Transfer Protocol). Для аналізу веб-трафіку Snort підтримує HTTP. Це дозволяє виявляти атаки, спрямовані на вразливості в веб-додатках, а також інші загрози через HTTP;

- DNS (Domain Name System). Snort може виявляти атаки, пов'язані з DNS, такі як DNS-спуфінг, DNS-відповіді з підробленими IP-адресами та інші атаки, які використовують DNS;

- FTP (File Transfer Protocol). Підтримка FTP дозволяє Snort виявляти атаки на протокол передачі файлів, такі як невірні аутентифікації чи спроби несанкціонованого доступу;

- SMTP (Simple Mail Transfer Protocol). Для виявлення загроз, пов'язаних з електронною поштою, Snort підтримує аналіз пакетів SMTP;

Перевагами Snort IDS є відкритий код, що дозволяє користувачам вносити свої модифікації та адоптувати його до конкретних потреб ефективність, підтримка спільноти. До недоліків можна віднести відсутність автоматичного відновлення та підвищений ризик помилкових спрацювань.

2.3.2 Suricata Network IDS/IPS

Suricata є системою для виявлення вторгнень (IDS) та системою для запобігання вторгнень (IPS), яка використовується в мережах для виявлення та захисту від потенційно шкідливих дій та вторгнень. Основною метою Suricata є аналіз мережевого трафіку з метою виявлення аномалій, підозрілих патернів чи вторгнень.

Основні можливості Suricata включають:

- сигнатурний аналіз. Suricata використовує сигнатури (патерни або правила), щоб виявляти відомі види атак або шкідливий код;
- аналіз аномалій: Suricata виявляє незвичайні або аномальні патерни трафіку, що може вказувати на вторгнення або атаки;
- підтримка протоколів. Suricata підтримує різні мережеві протоколи, такі як TCP, UDP, ICMP, HTTP, DNS і т.д.;
- модульний підхід. Має модульну архітектуру, що дозволяє додавати розширення та плагіни для розширення функціональності;
- захист в реальному часі; Suricata може виявляти та реагувати на атаки в реальному часі, що робить його ефективним інструментом для захисту мереж;
- ведення журналів. Suricata здатний вести подій, що дозволяє фахівцям з кібербезпеки аналізувати та реагувати на виявлені атаки;

Рисунок 2.4 – Розширений звіт та аналітика Suricata Network IDS [21]

Suricata Network IDS/IPS є широко використовуваним інструментом по всьому світу для виявлення та запобігання вторгнень. Країни, компанії та організації впроваджують Suricata як складову своїх кібербезпечних стратегій. Наприклад, у Сполучених Штатах, Suricata використовується в різних галузях, включаючи урядові агентства, корпорації та інші організації. В Європейських країнах багато урядових та приватних секторів використовують Suricata для захисту своїх мереж від кіберзагроз. Країни в Азії також впроваджують Suricata у своїх програмах кібербезпеки для захисту критичної інфраструктури та інших важливих систем. У країнах Латинської Америки Suricata використовується для мережевого моніторингу та виявлення вторгнень.

Отже, Suricata Network IDS/IPS представляє собою важливий інструмент у сфері кібербезпеки, який знаходить широке застосування у всьому світі. Здатний виявляти та запобігати вторгненням, Suricata стає необхідністю для багатьох країн, компаній та організацій, особливо в контексті захисту критичної інфраструктури.

Його здатність аналізувати різноманітний мережевий трафік, виявляти відомі та нові загрози, реалізувати реакцію в реальному часі та інтегруватися з системами управління інцидентами роблять його потужним інструментом для захисту від кіберзагроз. Suricata є прикладом того, як відкритий код може стати важливим фактором у сфері кібербезпеки, сприяючи спільноті розробників та користувачів у вдосконаленні та адаптації інструменту до зростаючих вимог у сфері кіберзахисту. З його допомогою організації можуть забезпечити надійний захист своїх мереж та інфраструктури, що є ключовим елементом в епоху все зростаючих кіберзагроз.

2.3.3 Wireshark

Wireshark є безкоштовним і відкритим програмним забезпеченням для аналізу мережевого трафіку. Він використовується для захоплення, аналізу та відображення пакетів даних, які пересилаються через мережу. Основні функції Wireshark включають:

- захоплення пакетів – Wireshark може записувати трафік мережі з різних джерел, таких як мережеві інтерфейси, файлові потоки або навіть за допомогою віддалених з'єднань;
- аналіз пакетів – програма надає можливості для розгляду і аналізу окремих пакетів даних, включаючи їх заголовки та вміст;
- фільтрація трафіку – користувач можете використовувати фільтри для відображення або приховування конкретного мережевого трафіку за різними критеріями;
- статистика мережі – Wireshark забезпечує різноманітні статистичні дані та графіки, що дозволяють вам отримати уявлення про трафік мережі;

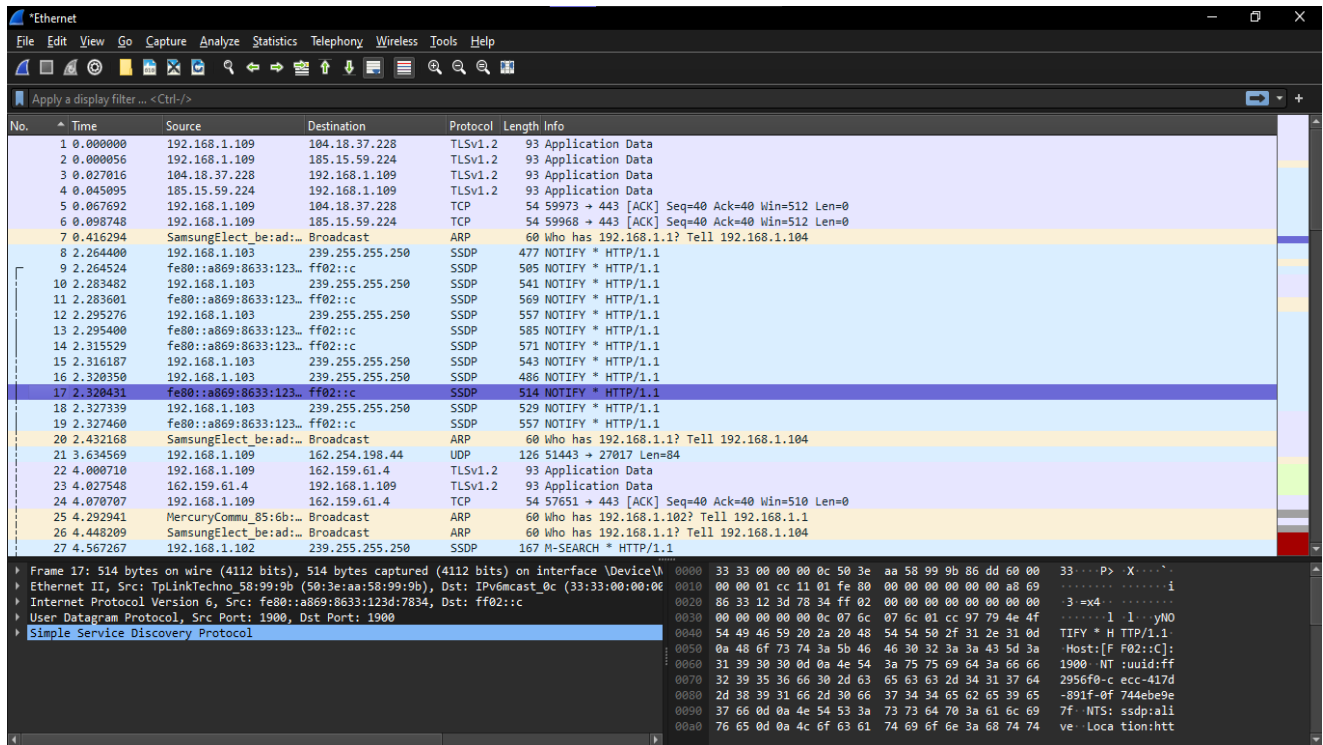


Рисунок 2.5 – Інтерфейс програми Wireshark

Wireshark це непоганий інструмент для аналізу мережевого трафіку, який надає можливість виявляти проблеми та вразливості. Цей інструмент забезпечує безпечний та ефективний спосіб моніторингу та аналізу мережі, що робить його важливим для ряду сфер інформаційно-комунікаційних технологій. Wireshark використовується для глибокого розуміння того, як відбувається обмін даними в мережі, що є критичним для виявлення вразливостей та атак.

2.3.4 ELK Stack

ELK Stack – це аббревіатура, яка вказує на три відкритих програмних продукти: Elasticsearch, Logstash і Kibana [22]. Ці компоненти працюють разом

для забезпечення потужного і ефективного аналізу та візуалізації лог-файлів та інших видів структурованих та неструктурованих даних.

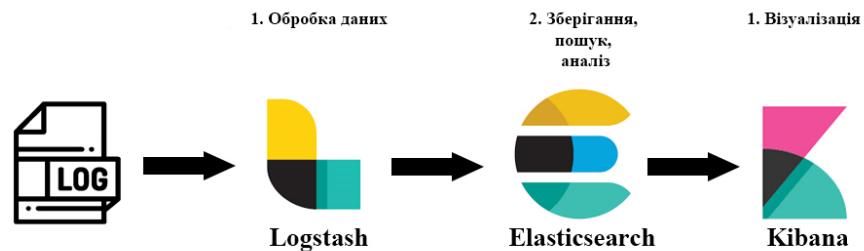


Рисунок 2.6 – Архітектура ELK Stack

Elasticsearch є розподіленою системою управління пошуковою аналітикою, побудованою на основі Apache Lucene (Apache Lucene – безкоштовна бібліотека пошукової системи, яка написана на мові програмування Java [24]). Вона призначена для зберігання, пошуку та аналізу великих обсягів даних в реальному часі. До основних функцій відносяться:

- індексація даних;
- пошук та агрегація;
- розподілена архітектура (дозволяє масштабувати систему горизонтально для обробки великого обсягу даних);
- RESTful API;

Logstash є важливою складовою ELK Stack і використовується для збору, обробки та передачі різноманітних даних з різних джерел до Elasticsearch для індексації та аналізу. Основна ідея полягає в тому, щоб робити дані доступними та придатними для пошуку та аналізу, враховуючи їх різноманітні формати та джерела. До основних функцій відносяться:

- збір даних;
- інтеграція з різними вихідними системами, тобто Elasticsearch, бази даних для подальшого зберігання та використання, зовнішні API;
- фільтрація та обробка;

- підтримка різних форматів даних, тобто JSON, CSV, XML;

Загалом, Logstash грає ключову роль у створенні ефективного процесу обробки та передачі даних

Kibana надає інтерфейс користувача для візуалізації, аналізу та розуміння даних, які зберігаються в Elasticsearch. Завдяки Kibana, користувачі можуть легко створювати різноманітні графіки, діаграми, таблиці та інші візуальні елементи, щоб легше вивчати та взаємодіяти зі своїми даними. До основних функцій відносяться:

- візуалізація даних;
- дашборди;
- інтерактивний пошук та фільтрація;
- сповіщення про виникнення певних подій;
- рольовий доступ;

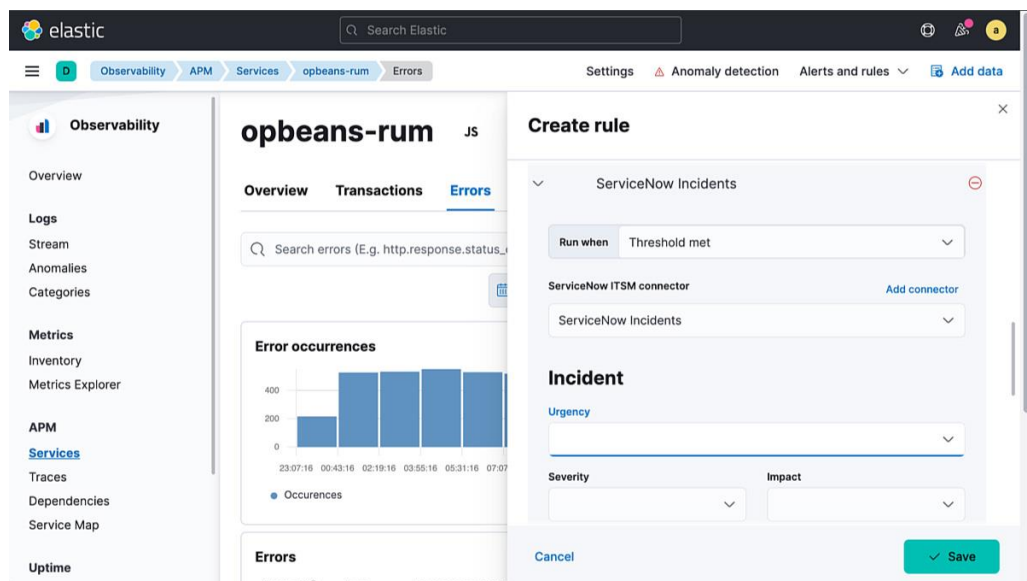


Рисунок 2.7 – Інтерфейс Kibana [26]

Kibana використовується для швидкого та зручного аналізу своїх даних, зрозуміння трендів, виявлення аномалій та створення інформативних звітів. Комбінуючи Kibana з Elasticsearch та Logstash, користувачі отримують повний стек для збору, обробки та аналізу даних в реальному часі.

2.4 Методи виявлення слабкостей та ризиків у критичній інфраструктурі

Сучасні технологічні виклики та загрози вимагають високого рівня уваги до забезпечення безпеки об'єктів, які мають велике соціальне та економічне значення для суспільства. Тому важливо розглянути методи виявлення слабкостей та ризиків у контексті критичної інфраструктури.

Забезпечення безпеки критичної інфраструктури потребує вивчення та розуміння різноманітних методів, які виявляють слабкості та ризики в системах. У цьому розділі буде розглянуто такі ключові аспекти, як аудит безпеки, сканування вразливостей, аналіз журналів подій, пентестінг та інші методи, які спрямовані на ефективне виявлення можливих загроз.

Не менш важливим є включення соціального інжинірингу та освітніх заходів, оскільки люди стають фокусом сучасних кібератак. Ми розглянемо аспекти соціального інжинірингу, такі як фішинг та різні техніки маніпуляцій, і розглянемо заходи з підвищення обізнаності та здатностей персоналу.

Мета цього розділу полягає не лише в розкритті методів виявлення ризиків, а й розробку комплексної стратегії безпеки, яка враховує технічні, організаційні та соціальні виміри, необхідні для забезпечення надійної захисту критичної інфраструктури.

2.4.1 Аудит інформаційної безпеки

Аудит інформаційної безпеки – це систематичний та об'єктивний процес оцінки, перевірки та аналізу безпеки інформаційних систем, мереж та компонентів критичної інфраструктури. Цей метод виявлення ризиків передбачає глибокий аналіз конфігурацій, налаштувань та процесів з метою ідентифікації потенційних слабкостей та вразливостей.

Він спрямований за для підвищення або забезпечення високого рівня інформаційної безпеки та виявлення можливих загроз для безпеки критичної інфраструктури. Цей процес дозволяє:

- визначити слабкі місця в системах та мережах, що можуть стати об'єктами кібератак;
- перевірити відповідності існуючих заходів безпеки стандартам та внутрішнім політикам для забезпечення високого стандарту безпеки;
- запобігати потенційним атакам, завдяки прийнятим заходам для попередження можливих атак;

Етапи аудиту безпеки:

- планування – визначення об'єктів аудиту, мети та обсягу розроблення плану дій, основною метою планування є забезпечити чіткість та структурованість аудиту, визначивши основні завдання;
- збір даних – збір та аналіз конфігурацій, налаштувань, журналів подій. На цьому етапі здійснюється оцінка технічних параметрів та збір необхідних даних для подальшого аналізу;
- оцінка вразливостей – аналіз виявлених слабкостей та вразливостей систем та мереж, оцінка потенційних загроз та ризиків;
- розроблення рекомендацій – визначення заходів для покращення безпеки, створення конкретних рекомендацій, які можуть включати технічні зміни, впровадження нових політик безпеки;
- подання звіту – підготовка документації з результатами аудиту та рекомендаціями для вдосконалення безпеки, звіт повинен бути прозорим та зрозумілим для технічних та нетехнічних спеціалістів;

Організації повинні реагувати на висновки аудиту інформаційної безпеки, розробляючи план для вирішення проблем, які були виявлені під час аудиту. Цей план повинен мати у собі конкретні вирішення проблем для кожної виявленої слабкості та графік за яким будуть впроваджені зміни [22]. Аудит інформаційної безпеки повинен бути неперервним процесом, оскільки кіберзагрози постійно змінюються. Регулярне проведення аудитів дозволяє

адаптувати стратегії безпеки до нових викликів та зберегти або покращити рівень захисту критичної інфраструктури.

2.4.2 Сканування вразливостей

Сканування вразливостей є ефективним методом для виявлення вразливостей у програмному та апаратному забезпеченні систем. Використання автоматизованих сканерів дозволяє швидко ідентифікувати вразливі точки та надавати рекомендації щодо їх виправлення. Цей метод виявлення ризиків дозволяє знайти можливі точки доступу для потенційних загроз. Сканування вразливостей є ефективним інструментом для:

- визначення потенційних атак – ідентифікація слабкостей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу;
- оцінка рівня загроз – визначення потенційних наслідків вразливостей для безпеки всієї системи та даних;
- покращення систем безпеки, тобто надання рекомендацій для усунення виявлених слабкостей їх реалізація;

Етапи сканування вразливостей:

- визначення цілей сканування – об'єктів, мети проведення сканування;
- вибір програмних засобів, які використовуються для сканування (були розглянуті у розділі 2.2);
- проведення сканування;
- аналіз результатів – оцінка виявлених вразливостей, визначення їх критичної інфраструктури та потенційних наслідків;
- визначення заходів для усунення виявлених вразливостей та запобігання можливим атакам;

Сканування вразливостей є динамічним процесом, оскільки нові загрози виникають з часом. Регулярне проведення сканування дозволяє тримати

систему або мережу під постійним контролем та вчасно реагувати на зміни, забезпечуючи стабільний та високий рівень безпеки.

2.4.3 Тест на проникнення

Пентест є ключовим етапом аудиту безпеки, спрямованим на імітацію реальної кібератаки або кібератак для виявлення та усунення вразливостей в системах та мережах. Цей метод виявлення ризиків дозволяє випробувати реакцію системи на різноманітні загрози та атаки. Звіти з тестування на проникнення можуть надати оцінку потенційного впливу на організацію і запропонувати контрзаходи для зменшення потенційного ризику [25]. Тест на проникнення включає в себе моделювання реальних атак, виявлення слабкостей та оцінки реакції на загрози.

До етапів пентесту відносяться:

- планування – визначення об'єкта тестування, визначення завдань та підготовка фахівців з етичного хакінгу;
- збір інформації – збір інформації про об'єкт тестування, ідентифікація потенційних цілей;
- пошук вразливостей – використання сканерів та аналіз для виявлення вразливостей в системі;
- експлуатація вразливостей – спроба отримання несанкціонованого доступу чи здійснення інших атак при виявлених вразливостях;
- аналіз результатів – оцінка виявлених вразливостей та потенційних наслідків для системи;
- підготовка звіту з результатами тестування та рекомендаціями для усунення виявлених слабкостей;

Пентестінг є необхідним для забезпечення високого рівня безпеки. Цей метод не лише виявляє потенційні загрози, а й допомагає розробити та вдосконалити стратегії захисту для запобігання майбутнім кібератакам.

2.4.4 Аналіз архітектури та дизайну системи

Аналіз архітектури та дизайну системи є одним з етапів аудиту інформаційної безпеки, який визначає наскільки добре система побудована для виявлення та запобігання та виправлення можливих кіберзагроз.

Аналіз архітектури та дизайну враховує виявлення слабкостей в проектування, тобто наскільки система враховує принципи безпеки на етапі проектування, оцінку ефективності архітектурних рішень та як вона сприяє безпеці і забезпеченні відповідності стандартам безпеки.

Етапи аналізу архітектури та дизайну:

- збір даних – визначення архітектурних систем, дизайну та документації;
- аналіз дизайну – оцінка вибору технологій, використання шифрування, механізмів аутентифікації та авторизації;
- оцінка доступності та відмовостійкості;
- аналіз наявних засобів виявлення та реагування на інциденти;
- оцінка взаємодії компонентів системи в реальному часі та виявлення потенційних атак;
- підготовка звіту з результатами аналізу;

Цей етап дозволяє побудувати систему стійку до кіберзагроз ще на етапі розробки.

2.4.5 Моделювання загроз

Моделювання загроз є ефективним методом аналізу та оцінки потенційних загроз. Цей підхід дозволяє імітувати різноманітні сценарії атак та визначити, як система чи мережа підготовлена та може реагувати на ці атаки в реальному часі.

Етапи моделювання загроз включають:

- визначення цілей та об'єктів моделювання;
- розроблення сценаріїв загроз, які враховують різні типи кібератак;
- моделювання загроз, завдяки спеціалізованих програм для імітації сценаріїв атак та вивчення їхнього впливу;
- аналіз результатів;
- підготовка звіту з запропонованими рекомендаціями для підвищення безпеки системи чи мережі;

Цей метод дозволяє ефективно впливати на безпеку критичної інфраструктури, надаючи можливість побачити, реакцію систему на потенційну атаку, аналізувати та усувати виявлені слабкості, до того, як вони будуть використані кіберзлочинцями при реальній атаці.

2.4.6 Соціальний інжиніринг та освітні заходи

Соціальний інжиніринг визначається, як маніпулювання людьми з метою отримання конфіденційної інформації або здійснення інших дій, що можуть загрожувати безпеці. Соціальний інжиніринг є одним з найважливіших ризиків, оскільки в основному саме люди стають слабким ланцюжком у системах безпеки, як ми могли побачити це у розділі 1.4.

Фішинг – це форма соціальної інженерії та шахрайства, коли зловмисник обманом, тобто маскуючись під конкретну особу або організацію змушує розкрити людей конфіденційну інформацію або встановити зловмисне програмне забезпечення.

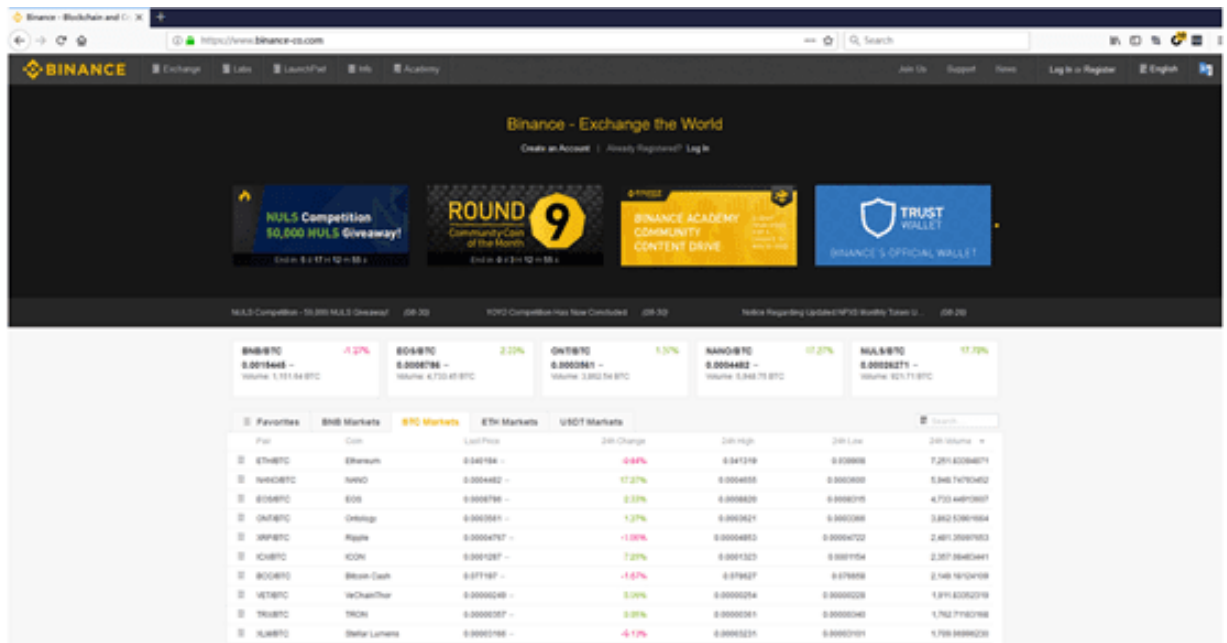


Рисунок 2.7 – Приклад фішингового сайту Binance [27]

Організація лекцій та навчань для фахівців, які працюють на критичній інфраструктурі, а особливо технічних спеціалістів стане важливим елементом стратегії забезпечення безпеки. Ці лекції можуть включати в себе:

- ідентифікацію та усунення загроз соціального інжинірингу, тобто навчання співробітників розпізнавати та уникати його;
- регулярні тренінги та тести, навчання персоналу важливості захисту конфіденційної інформації та здорового підходу до обміну даними;
- лекції та практичні завдання з фахівцями з кібербезпеки для підвищення рівня знань та навичок;

Після впровадження освітніх заходів важливо провести оцінку їхньої ефективності. Визначення ефективності освітніх заходів та визначення змін у рівні соціального інжинірингу стане основою для подальших покращень.

Резюмуючи, у розділі 2.3 було розглянуто різноманітні методи виявлення вразливостей та слабкостей у критичній інфраструктурі. Кожен обговорений пункт пропонує специфічні підходи та інструменти, які можна використовувати для ефективного аналізу та запобігання можливим кіберзагрозам.

На основі аналізу різноманітних методів було виявлено, що комплексний підхід до кібербезпеки включає в себе технічні, соціальні та освітні аспекти.

Важливо враховувати, що кіберзагрози постійно еволюціонують і відповідного до цього стратегії кібербезпеки повинні постійно вдосконалюватися.

2.5 Переваги та недоліки обраних інструментів

Розгляд переваг та недоліків використовуваних інструментів допоможе визначити ефективність та обмеження кожного обраного засобу.

Таблиця 2.1 - Переваги та недоліки обраних методів та інструментів

Інструменти	Переваги	Недоліки
Snort Intrusion Detection System	Відкритий та безкоштовний код.	Вимагає значних зусиль для конфігурації та налаштування.
	Підтримка різноманітних протоколів.	Може бути вразливим до обхідних методів для деяких атак.
	Присутнє інтегрування з іншими системами безпеки.	Може вимагати значних ресурсів для великих мереж.

Продовження таблиці 2.1

Інструменти	Переваги	Недоліки
	Активна спільнота та широкий функціонал.	Може генерувати велику кількість хибнопозитивних сигналів.
		Оновлення правил може бути не таким оперативним, як потрібно.
Suricata Network IDS/IPS	Підтримка мережевого виявлення вторгнень та запобігання атакам.	Великий обсяг даних може вимагати значних ресурсів.
	Підтримка протоколів та широкий функціонал.	Споживає багато ресурсів CPU при великій швидкості мережі.
	Можливість використання у режимі IDS або IPS.	Не завжди підтримує всі функції Snort.
	Відкритий код.	Може вимагати технічного експерта для налаштування та управління.
		Специфічний для мережевого виявлення вторгнень, не покриває всі аспекти безпеки.

Кінець таблиці 2.1

Інструмент	Переваги	Недоліки
Wireshark	Інтуїтивний інтерфейс та можливість перегляду пакетів даних.	Може генерувати велику кількість даних, яку важко обробляти.
	Підтримка протоколів та фільтрація даних.	Вимагає ресурсів для аналізу великих потоків даних.
	Відкритий код.	Потребує високого рівня технічної експертизи.
	Можливість аналізу пакетів на різних рівнях мережи.	
ELK Stack	Інтеграція з різноманітними даних.	Вимагає значних зусиль для розгортання та конфігурації.
	Розширена можливість візуалізації даних та створення звітів.	Вимагає потужних ресурсів при великих обсягах даних.
	Підтримка моніторингу та аналізу в реальному часі.	
	Система безпеки та журналювання подій.	
	Відкритий код та активна спільнота.	

2.6 Висновки та аналіз результатів

В даному розділі здійснено обґрунтування вибору методів аналізу кіберзагроз і розглянуто ключові фреймворки та методології такі, як Mitre ATT&CK Framework, Cyber Kill Chain, STRIDE, OWASP Risk Rating Methodology та NIST Cybersecurity Framework. Це надає можливість систематизувати та структурувати аналіз кіберзагроз для критичної інфраструктури, забезпечуючи повний огляд векторів атак та етапів.

Також було розглянуто засоби моніторингу та виявлення аномалій в мережі, а саме система виявлення аномалій в мережі (NIDS), систему виявлення аномалій на основі хосту (HIDS) та гібридні системи виявлення вторгнень (HIDS), які поєднують в собі систему виявлення аномалій на основі хосту та гібридних систем.

Окремий акцент було зроблено на виборі інструментів для виявлення та аналізу кібератак. Snort IDS, Suricata Network IDS/IPS, Wireshark, ELK Stack та NIST Cybersecurity Framework є найкращими системами для аналізу та реагування на кіберзагрози на критичні інфраструктури.

Подальший аналіз виявлення слабкостей та ризиків включає аудит інформаційної безпеки, сканування вразливостей, тести на проникнення, аналіз архітектури, соціальний інжиніринг та освітні заходи. Всі ці методи допомагають виявити та усунути слабкості, зменшуючи ризик того, що наступна кібератака буде вдалою.

Також було проведено критичний огляд обраних інструментів і визначено їх переваги та обмеження. Загальною метою цього огляду є відбір інструментів, які забезпечать надійний рівень захисту об'єктів критичної інфраструктури.

3 РОЗРОБЛЕННЯ ЗАГАЛЬНИХ МЕХАНІЗМІВ ТА РЕКОМЕНДАЦІЙ ДЛЯ ПОЛІПШЕННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Вибір об'єкта критичної інфраструктури

Об'єктом критичної інфраструктури для подальшого аналізу обрано енергетичну систему як об'єкт, що є основою для функціонування економіки, соціальних служб та інших критичних об'єктів держави.

Енергетична система відіграє ключову роль у забезпеченні енергією всіх галузей економіки, починаючи від промисловості та закінчуючи побутовими споживачами. Її неперервна робота є життєво важливою для забезпечення сталого розвитку та безпеки держави.

Важливість енергетичної системи полягає в наступних аспектах:

- економічне значення полягає в тому, що енергетична система є серцем економіки, надаючи необхідну електроенергію для виробництва та функціонування підприємств. Переривання роботи може викликати серйозні економічні збитки, зупинку або закриття підприємства;

- соціальне значення полягає в тому, що наявність стабільного електропостачання є важливим фактором забезпечення комфорту та безпеки громадян, починаючи від опалення та освітлення до функціонування лікарень та навчальних закладів;

- енергетична система має ключове значення для національної безпеки, оскільки вона забезпечує роботу інших об'єктів критичної інфраструктури, а також надає змогу відповідати на різні виклики, такі як надзвичайні ситуації;

Отже, енергетична система є стратегічно важливою для економіки, соціальної стабільності та національної безпеки. Забезпечення надійного рівня безпеки є необхідним завданням для нормального функціонування держави.

3.1.1 Характеристика енергетичної системи

Енергетична система – це сукупність електростанцій, електричних і теплових мереж, інших об'єктів електроенергетики, які об'єднані спільним режимом виробництва, передачі та розподілу електричної і теплової енергії при централізованому управлінні цим режимом [28]. Енергетична система є динамічною системою, яка постій змінюється. Ці зміни можуть створити нові загрози для безпеки.

Енергосистема є складною структурою, яка включає в себе різні компоненти та підсистеми. Кожен з цих елементів грає важливу роль у забезпеченні стійкості та ефективності електропостачання.

Електростанції є центральним елементом енергетичної системи. В залежності від типу електростанції вона буде використовувати різні джерела енергії, такі як вугілля, газ, вітер, ядерне паливо чи сонце. Кожен тип має свої унікальні технічні характеристики та системи керування.

Передача та розподіл електроенергії забезпечується мережами передачі і розподілу, що складаються з високовольтних та низьковольтних ліній, трансформаторів та підстанцій.

Системи управління та моніторингу є ключовим елементом енергетичної інфраструктури. Вони регулюють виробництво, передачу, розподіл та споживання електроенергії. Забезпечення надійного рівня захисту цих систем є критично важливим для запобігання несанкціонованого доступу та втручання в роботу енергосистеми.

Впровадження сучасних технологій, таких як смарт-мережі роблять систему більш підключеною, але в той же час вразливою до кіберзагроз, Що вимагає ретельного кіберзахисту.

3.1.2 Загрози для енергетичної системи

Енергетична система, як ключовий елемент критичної інфраструктури стикається з непростими викликами у сфері кібербезпеки. З кожним кроком у напрямку цифрової трансформації та автоматизації зростає потенційна небезпека з боку кіберзагроз, що може негативно впливати на її ефективність та безпеку.

В контексті цього дослідження виявлено низку серйозних кіберзагроз для енергетичних систем. Віруси та шкідливі програми є потенційною загрозою, інфікуючи інформаційні системи. Атаки нульового дня, використовують раніше невідомі вразливості і можуть порушити стійкість енергетичних систем.

Соціальний інжиніринг та фішинг виступають як методи, які використовують людський фактор для отримання несанкціонованого доступу та конфіденційної інформації. Далі, DoS та DDoS атаки можуть переповнювати ресурси серверів енергетичних компаній, ламаючи їхню доступність та завдавати збитків.

Файлові атаки використовують вразливості у обробці файлів для введення шкідливого коду, що може призвести до втрати даних або руйнування програмного забезпечення. Несанкціонований доступ та витік даних стають загрозою для конфіденційності та цілісності інформації.

Ці різноманітні атаки вимагають комплексного підходу до захисту інформаційних систем, спрямованого на виявлення, усунення та запобігання можливим атакам за для забезпечення стабільності та безпеки енергетичних систем.

3.2 Аналіз попередніх атак на об'єкт критичної інфраструктури

Починаючи з 2014 року Україна знаходиться у постійному протистоянні кібератакам з боку росії. Перші кібератаки на державні установи було зафіксовано ще під час Революції гідності у 2013 році.

Кібератаки, що спрямовані на критичні галузі, такі як енергетика, фінансові установи, медицина загрожують не лише конфіденційності інформації, але стають потенційною зброєю в руках учасників сучасних конфліктів та війн. Ця загроза особливо актуальна в контексті кібергеополітики, де держави та кіберзлочинці обирають критичну інфраструктуру, як об'єкт для стратегічних атак.

Україна є однією з країн, яка найбільше постраждала від кібератак на критичну інфраструктуру. Ці атаки були здійснені російськими урядовими хакерськими групами з метою дестабілізувати ситуацію в Україні і нашкодити українській економіці.

Попередні кібератаки, які були розглянуті у першому розділі мають спільні риси та характеристики. Давайте визначимося з техніками атак та методами доступу.

Кібератака на «Прикарпаття обленерго»:

- техніка атаки: використання троянської програми «BlackEnergy» та макрос скрипта Excel для зараження системи;
- метод доступу: фішингова атака на ІТ персонал та системних адміністраторів, збір логінів та паролів для віддаленого підключення до мережі «SCADA»;

Атака на підстанцію «Північна»:

- техніка атаки: використання програми «KillDisk», яка використовувало вразливість в ПЗ Simatic S7-400H, яке використовується для управління підстанціями. Вразливість була в протоколі Modbus, вона дозволила отримати доступ до систем управління підстанцією;

– метод доступу: вразливість в ПЗ системі автоматизації Simatic S7-400H;

Атака на сайти Міністерства фінансів, Держказначейства та Пенсійного фонду:

– техніка атаки: атака здійснена за допомогою шкідливого ПЗ «KillDisk», яка призначений для знищення або перезапису критично важливих системних файлів;

– метод доступу: фішингова атака для зараження комп'ютерів співробітників державних фінансових установ;

Атака вірусом «NotPetya»:

– техніка атаки: вразливість в операційній системі Windows, яка називається EternalBlue;

– метод доступу: фішингова атака для зараження комп'ютерів;

Усі ці атаки мають спільні риси, а саме вони були здійснені на критичну інфраструктуру. Це означає, що вони були спрямовані на системи, які є життєво важливими для суспільства, такі як енергетична інфраструктура, транспортна мережа та комунікаційні інфраструктури. Атаки були здійснені з використанням шкідливого ПЗ. Ці атаки були здійснені російськими урядовими хакерськими групами з метою дестабілізувати ситуацію в Україні і нашкодити українській економіці. Вони були добре сплановані і здійснені. Зловмисники, які здійснювали і планували ці атаки мали глибокі знання про критичну інфраструктуру України, а також про її вразливості. Також ці атаки призвели до значних економічних збитків і дестабілізації ситуації в Україні.

Застосовані техніки вимагають комплексних заходів з кібербезпеки для запобігання подібним інструментам у майбутньому.

Російські хакери продовжують проникати в мережі об'єктів критичної інфраструктури як через комп'ютери керівників (які використовували неліцензійні

Необхідно надавати велику увагу кібербезпеці та розробці заходів захисту для об'єктів критичної інфраструктури. Захист від кібератак повинен

бути комплексним з впровадженням новітніх технологій та підвищенням обізнаності персоналу.

3.3 Вибір фреймворків та механізмів для захисту об'єкта

Всі розглянуті фреймворки у 2.1, а саме Mitre ATT&CK, Cyber Kill Chain, STRIDE, OWASP, NIST Cybersecurity Framework є важливими інструментами для захисту критичної інфраструктури, зокрема енергетичної системи. Вони допомагають організаціям зрозуміти загрози, оцінити ризики та розробити ефектні заходи безпеки.

Mitre ATT&CK є найбільш всеосяжним і детальним фреймворком, який описує татики, техніки та процедури, що використовуються кіберзлочинцями. Цей фреймворк стане найкращим варіантом для розуміння атак на критичну інфраструктуру, розробки заходів пом'якшення та підвищення ефективності виявлення та реагування на інциденти.

Cyber Kill Chain є більш спрощеним фреймворком, який описує етапи кібератаки. Цей фреймворк може бути використаний для розуміння загального процесу атаки, виявлення ранніх ознак атаки та розробки заходів пом'якшення.

Вибір найкращого фреймворку для захисту критичного об'єкту енергетичної системи залежить від таких факторів, як:

- складність інфраструктури. Критичні об'єкти енергетичної системи часто є складними інфраструктурами, що складаються з різноманітних систем і компонентів, а саме системи управління, системи безпеки, підстанції, системи управління, центри керування енергосистемою, систему зв'язку і тд. Це вимагає використання фреймворку, який може враховувати ці особливості;

- рівень загроз. Критичні об'єкти є бажаною ціллю для кіберзлочинців. Це вимагає використання фреймворку, який має ефективно протистояти сучасним кіберзагрозам;

- фінансові та людські ресурси. Впровадження та підтримка фреймворку вимагає фінансових та людських ресурсів для його підтримки та використання. Цей фактор слід враховувати при виборі;

На основі цих факторів можна зробити висновок, що найкращим фреймворком для захисту критичного об'єкту енергосистеми є Mitre ATT&CK. Цей фреймворк є найбільш всеосяжним і детальним, що дозволяє організаціям отримати глибоке розуміння загроз і розробити ефективні заходи безпеки.

До його переваг відносяться:

- деталізація – фреймворк забезпечує детальний опис тактик, технік і процедур, що використовуються;

- аналіз атак – дозволяє зрозуміти та аналізувати реальні атаки, що відбуваються в різних секторах;

- гнучкість – може бути використаний як для великих корпорацій, так і для менших організацій;

Але також є і недоліки, до яких відносяться складність та обсяг, тобто фреймворк може бути складним для розуміння і впровадження.

Однак, якщо організація має обмежені ресурси, то вона може розглянути можливість використання Cyber Kill Chain. Цей фреймворк є «спрощеною» версією Mitre ATT&CK, але все одно він може забезпечити ефективний захист критичної інфраструктури.

До переваг Cyber Kill Chain відноситься:

- системність, тобто Cyber Kill Chain розбиває атаку на етапи, що полегшує аналіз та реакцію на всі фази атаки;

- виявлення атаки на ранніх етапах;

Недоліки:

- менш ефективний проти більш високорозвинених атак, тобто ботнети, мережі проникнень, використання соціальної інженерії;

Mitre ATT&CK є всеосяжним і детальним фреймворком, який описує понад 300 тактик, технік і процедур, які використовуються кіберзлочинцями. Він може бути використан для опису кібератак на будь-яку систему або інфраструктуру, в той час Cyber Kill Chain орієнтований на опис кібератак на комп'ютерні системи та описує лише етапи кібератаки.

Для підвищення ефективності захисту можна розглянути можливість застосування двох фреймворків разом. Наприклад Mitre ATT&CK для розуміння загроз і розробки заходів безпеки, а Cyber Kill Chain для впровадження та підтримки цих заходів. Такий підхід дозволить отримати найкращі якості від кожного фреймворку.

Розглянуті IDS у розділі 2.4 є одними з найкращих інструментів для виявлення атак на комп'ютерні системи. Для захисту енергетичної системи найкращим вибором стане ELK Stack. Ось конкретні приклади того, як ELK Stack може бути використаний для захисту енергетичної системи.

- виявлення атак на мережеві пристрої. ELK Stack може використовуватися для виявлення атак на мережеві пристрої, такі як маршрутизатори, комутатори та сервери. Це може допомогти в захисті від вторгнення та крадіжки даних. Наприклад для виявлення атак на протоколи управління мережею (SNMP), які використовуються для атаки на мережеві пристрої;

- виявлення атак на програмне забезпечення. ELK Stack справляється з виявленням атак на програмне забезпечення, таке як операційні системи, веб-додатки та промислові контролери;

- виявлення атак в мережевому трафіку. ELK Stack може використовуватися для виявлення аномалій в мережевому трафіку, які можуть вказувати потенційну загрозу. Це допоможе при виявленні нових атак або загроз, які ще не були виявлені сигнатурами Snort. Наприклад, це можна

використати для виявлення аномалій між промисловими контролерами, виявлення яких може вказувати на атаку на промислову систему;

– виявлення вразливостей. ELK Stack може бути використаний для виявлення вразливостей у системах і мережах. Для цього потрібно використовувати аналіз журналів, аналіз даних про мережу активність, які є у ELK Stack;

ELK Stack є потужним і всебічним інструментом, який може бути використаний для захисту енергетичної системи від широкого спектру кіберзагроз.

ELK Stack має ряд переваг перед іншими фреймворками:

- потужні можливості для пошуку та аналізу даних;
- гнучкість – він є масштабованим і гнучким рішенням, яке може бути адаптованим до потреб конкретного об'єкта;
- легкість використання;
- відкритість коду;

Але також існують деякі недоліки, такі як витрати та відповідальність. Організації, які використовують ELK Stack несуть відповідальність за забезпечення та конфіденційність даних, які зберігаються в Elasticsearch.

Таблиця 3.1 – Функції безкоштовної та платної версії ELK Stack [30]

Безкоштовна версія	Платна версія
Elasticsearch 7.10	Elasticsearch 8
Logstash 7.10	Logstash 8
Kibana 7.10	Kibana 8
1000 індексів	Необмежена кількість індексів
10 ГБ зберігання	Необмежене зберігання
100 000 запитів на день	Необмежена кількість запитів на день
	Підтримка Elastic Cloud

Кінець таблиці 3.1

Безкоштовна версія	Платна версія
	Підтримка Elastic Stack Security
	Підтримка Elastic Stack Machine Learning

В цілому ELK Stack є найкращим варіантом для захисту критичного об'єкту енергетичної системи. Він забезпечує потужні можливості для збору обробки, аналізу та візуалізації даних, що дозволяє фахівцям з кібербезпеки швидко виявляти та реагувати на кіберзагрози.

3.4 Створення планів навчання та тренувань персоналу

Проаналізувавши попередні атаки на критичну інфраструктуру стає зрозуміло, що основною проблемою вразливості в системах кібербезпеки є людина. Людський фактор включає в себе не лише можливість внутрішньої недбалості або зловживання, але й слабкість перед соціальним інжинірингом. Саме тому створення комплексного плану навчання та тренувань працівників є критичним аспектом забезпечення високого рівня кібербезпеки об'єктів критичної інфраструктури держави. Цей план повинен охоплювати різні рівні персоналу, враховуючи як технічних, так і не-технічних працівників. Високий рівень захищеності вимагає активної участі всього персоналу. Здійснення кампаній з підвищення кваліфікації щодо кібербезпеки є ключовим кроком до цього.

Крок 1 – оцінка потреб. Першим етапом є проведення аналізу потреб персоналу у навчанні інформаційній гігієні та кібербезпеки. Це може включати оцінку рівня технічної підготовки, аналіз попередніх інцидентів та індивідуальних компетенцій.

Крок 2 – розробка курсів та тренувань. На основі виявлених потреб розробляються спеціалізовані курси та тренування. Не-технічний персонал може отримати навчання основ з інформаційної гігієни та правил корпоративної безпеки, а технічний окрім цього буде навчатися виявленню та реагуванню на загрози. Співробітникам буде надаватися інформація про різновиди фішингу, методи його виявлення та його вплив.

Крок 3 – соціальна інженерія. Навчання включає в себе аспекти соціальної інженерії, які допоможуть зрозуміти як атаки можуть використовувати психологічні та соціально методи для обману.

Крок 4 – симуляція. Важливо включити в план навчання симуляцію фішингових атак, щоб персонал міг випробувати свої отримані навички у реальних або схожих на реальні умови. Це допоможе підготувати співробітників до реальних ситуацій та вдосконалити їх реакцію на кіберзагрози. Найкращі результати можна виявити, якщо не попереджати персонал про симуляцію цих атак та подивитися, як персонал буде вести себе в умовах, коли він цього не очікує.

Крок 5 – взаємодія зі сторонніми ресурсами або експертами. Впровадження експертів з кібербезпеки або використання освітніх майданчиків (курсів) може допомогти у наданні високоякісної інформації персоналу. Це може включати в себе воркшопи, лекції, вебінари.

Ці рекомендації є основою для розробки стратегії з підвищення та обізнаності персоналу, спрямованих на конкретні виклики, що виникають у контексті кібербезпеки критичної інфраструктури держави.

3.6 Переваги навчань та тренувань персоналу

У цьому розділі розглядається необхідність визначення та врегулювання людського фактору у контексті кібербезпеки, а також пропонуються конкретні

рекомендації для створення планів навчання, спрямованих на підвищення рівня компетентності та усвідомленості персоналу. Висвітлюється роль інформаційної освіти у формуванні культури кібербезпеки в організації та надається аналіз переваг такого підходу до захисту інформаційних систем.

До переваг тренувань персоналу відноситься:

- підвищення свідомості – інформаційна освіта дозволяє підняти рівень свідомості серед працівників, щодо кіберзагроз та правил безпеки. Зрозумілі засоби комунікації допомагають зробити складні концепції доступними для широкого кола співробітників, включаючи не-технічний персонал;

- зниження ризиків фішингу та соціального інжинірингу – працівники, які розуміють схеми атак та пройшли симуляцію атак мають менше шансів стати жертвами фішингових атак;

- підвищення компетентності технічного персоналу – технічний персонал, що проходить це навчання отримує глибокі знання та навички, які необхідні для виявлення, аналізу та реагування на існуючі загрози;

- активна участь всього персоналу – інформаційна освіта залучає всі рівні персоналу до активної участі у забезпеченні кібербезпеки, кожен зможе вносити свій вклад у створення безпечного робочого середовища;

- здатність ефективно реагувати – тренування і симуляції допомагають персоналу ефективно реагувати на кібератаки, вони зможуть швидко та правильно визначати, характеризувати та контролювати інциденти;

- мінімізація людської помилки – навчальні курси допомагають зменшити ризик людської помилки, таких як випадкові витoki конфіденційної інформації, незахищене оброблення важливих даних і тд.;

Інформаційна освіта відіграє важливу роль у створенні організації, що свідомо відноситься до кібербезпеки та забезпечує збалансований підхід до захисту від кіберзагроз.

Висновки до 3 розділу

У третьому розділі були розроблені загальні механізми та рекомендації для поліпшення захисту критичної інфраструктури. Для цього було обрано енергетичну систему, як об'єкт критичної інфраструктури, оскільки вона є однією з найважливіших для суспільства.

Енергетична система є складною інтегрованою системою, яка включає в себе різні компоненти, такі як електростанції, електромережі, підстанції та споживачі електроенергії. Ці компоненти взаємодіють один з одним, і порушення в роботі одного з них може призвести до збоїв у роботі всієї системи.

Аналіз попередніх атак на енергетичну систему показав, що найпоширенішими типами атак є фішинг і злом паролів. Ці атаки дозволяють зловмисникам отримати доступ до облікових даних працівників енергетичної компанії, які потім можуть бути використані для проведення інших атак, таких як шпигунство або викрадання даних.

На основі проведеного аналізу було обрано фреймворки та механізми для захисту енергетичної системи

Підвищення свідомості щодо кібербезпеки серед працівників є важливим компонентом будь-якої програми захисту критичної інфраструктури. Працівники повинні бути обізнані про існуючі кіберзагрози та про те, як їх можна запобігти.

Загалом, розроблені механізми є ефективним способом підвищення рівня захисту енергетичної системи від кіберзагроз. Однак, для досягнення максимального ефекту ці механізми повинні бути належним чином впроваджені та підтримувані.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ ТРАФІКУ

У цьому розділі представлено програмне забезпечення для аналізу мережевого трафіку, яке розроблено для виявлення потенційних кіберзагроз. Розділ охоплює огляд основних аспектів та функціональних можливостей реалізованого аналізатору трафіку.

4.1 Ціль програмного забезпечення

Ціллю цієї програми є виявлення та аналіз загрозових пакетів у мережевому трафіку. Програма здатна ідентифікувати потенційні загрози за допомогою сигнатур та аналізу мережевих пакетів, а також повідомляти про них через електронну пошту. Розглянемо ключові аспекти розробленого програмного продукту:

- читання списку шкідливих IP-адрес – програма може зчитувати списки IP-адрес, які вважаються потенційно небезпечними з файлу для подальшого використання у виявленні загроз;
- визначення сигнатур шкідливих пакетів – використовуючи визначені сигнатури програма може ідентифікувати пакети, які можуть представляти загрозу;
- виявлення потенційних загроз у мережевому трафіку – програма проводить аналіз мережевого трафіку та визначає чи містить він загрозові елементи відповідно до визначених сигнатур;
- логування та зберігання інформації про шкідливі пакети – у випадку виявлення загроз програма логує необхідну інформацію та зберігає її для подальшого аналізу та вивчення;

– сповіщення про виявлення загроз електронною поштою – після виявлення потенційної загрози програма може вислати повідомлення електронною поштою для реагування на інциденти;

4.2 Реалізація аналізатора трафіку на Python

4.2.1 Читання списку загрозових IP-адрес та портів

Для забезпечення гнучкості та можливості оновлення потенційно небезпечних IP-адрес та портів, програма реалізує функціонал читання цих адрес з файлу.

```
def read_malicious_ips(file_path):
    try:
        with open(file_path, "r") as file:
            malicious_ips = [line.strip() for line in file if line.strip()]
        return malicious_ips
    except FileNotFoundError:
        logger.error(f"Файл не знайдено: {file_path}")
        return []

def read_malicious_ports(file_path):
    try:
        with open(file_path, "r") as file:
            malicious_ports = [line.strip() for line in file if line.strip()]
        return malicious_ports
    except FileNotFoundError:
        logger.error(f"Файл не знайдено: {file_path}")
```

Рисунок 4.1 – Функція для читання загрозових IP-адрес

Використання:

```
malicious_ips_file = "malicious_ips.txt"
malicious_ports_file = "malicious_ports.txt"
threat_signature = {
    "malicious_ip": read_malicious_ips(malicious_ips_file),
    "malicious_port": read_malicious_ports(malicious_ports_file),
}
```

Рисунок 4.2 – Завантаження списку шкідливих IP-адрес та портів

Пояснення:

- функція `read_malicious_ips` отримує шлях до файлу з IP-адресами;
- вона відкриває файл, читає його рядок за рядком та створює список загрозливих IP-адрес;
- якщо файл не знайдений генерується помилка і повертається пустий список;
- отримані IP-адреси використовуються, як частина сигнатури для подальшого виявлення загроз у мережевому трафіку;

4.2.2 Визначення сигнатур загрозливих пакетів

Для виявлення шкідливих пакетів у мережевому трафіку програма використовує сигнатури, що визначають характеристики, типи або параметри, які є характерними для кіберзагроз.

```
threat_signature = {
    "malicious_ip": read_malicious_ips(malicious_ips_file),
    "malicious_port": read_malicious_ports(malicious_ports_file),
}
```

Рисунок 4.3 – Використання сигнатур для аналізатору трафіку

Пояснення:

- `threat_signature["malicious_ip"] = read_malicious_ips(malicious_ips_file)`
- ця стрічка коду викликає функцію `read_malicious_ips()` зі шляхом до файлу `malicious_ips_file`. Ця функція призначена для читання IP адрес з файлу і повертає список цих адрес;
- `threat_signature["malicious_port"] = read_malicious_ports(malicious_ports_file)`: Ця стрічка коду викликає ту ж функцію `read_malicious_ips`, але для файлу

malicious_ports_file. Файл містить інформацію про шкідливі порти. Отриманий список портів також заноситься у словник threat_signature під ключем "malicious_port".

4.2.3 Виявлення потенційних загроз у мережевому трафіку

У цьому підпункті буде розглянуто алгоритм виявлення шкідливих пакетів у мережевому трафіку. Програма використовує визначені сигнатури для аналізу кожного пакеті та визначення його потенційної небезпеки

```
def is_threat(packet):
    if IP in packet and TCP in packet:
        src_ip = packet[IP].src
        dst_ip = packet[IP].dst
        src_port = packet[TCP].sport
        dst_port = packet[TCP].dport

        malicious_ports = list(map(int, threat_signature["malicious_port"]))

        # Перевірка наявності загрози у пакеті
        return (
            (src_ip in threat_signature["malicious_ip"]
             and dst_port in malicious_ports)
            or (dst_ip in threat_signature["malicious_ip"] and src_port in threat_signature["malicious_port"])
        )
    else:
        return False
```

Рисунок 4.4 – Функція для визначення чи є пакет потенційною загрозою

```
def analyze_packet(packet):
    if is_threat(packet):
        logger.warning("Виявлено потенційну загрозу:")
        logger.warning(packet.summary())
        threat_packets.append(packet)
        send_email(f"Виявлено потенційну загрозу:\n{packet.summary()}")
```

Рисунок 4.5 – Використання функції під час аналізу мережевого трафіку

Пояснення:

- функція `is_threat()` визначає чи є переданий пакет потенційною загрозою на основі визначених сигнатур, вона перевіряє чи присутній в пакеті IP та TCP шари і якщо так, то отримує їхні IP-адреси та порти;

- функція `analyze_packet()` викликає функцію `is_threat()` для аналізу кожного мережевого пакету та викликає відповідні дії у випадку виявлення загрози;

Цей розділ описує механізм виявлення потенційних загроз у мережевому трафіку та прийняття відповідних заходів у разі їх виявлення.

4.2.4 Логування та зберігання інформації про шкідливі пакети

Визначемо механізми для логування та зберігання інформації про потенційно шкідливі пакети, які були виявлені під час аналізу мережевого трафіку.

У програмі використовується модуль `logging` для ведення журналу подій. Логер ініціалізується з рівнем `WARNING`, щоб логувати тільки серйозні події, пов'язані з загрозами.

```
logging.basicConfig(level=logging.INFO)
logger = logging.getLogger("NetworkAnalyzer")
```

Рисунок 4.6 – Використання модуля `logging`

Коли виявляється потенційно загрозливий пакет, то він логується для подальшого аналізу та виводу інформації користувачу.

```
logger.warning("Виявлено потенційну загрозу:")
logger.warning(packet.summary())
```

Рисунок 4.7 – Логування та вивід інформації

Шкідливі пакети зберігаються у списку `threat_packets` для подальшого аналізу та виводу користувачу. Цей список оголошений поза основною функцією `main()` та доступний для інших частин програми. Кожен раз, коли виявляється потенційно шкідливий пакет, він додається до цього списку.

4.2.5 Сповіщення про виявлення загроз електронною поштою

У програмі використовується дані користувача для налаштування електронної пошти, такі як адреса відправника (`email_sender`), пароль (`email_password`), адреса отримувача (`email_recipient`), сервер SMTP (`email_smtp_server`) та порт SMTP (`email_smtp_port`). Ці дані використовуються для аутентифікації на сервері та надсилання електронної пошти.

```
load_dotenv('.env')

email_sender = os.getenv("EMAIL_SENDER")
email_password = os.getenv("EMAIL_PASSWORD")
email_recipient = os.getenv("EMAIL_RECIPIENT")
email_subject = "Виявлено зловмисну IP-адресу"
email_smtp_server = "smtp.gmail.com"
email_smtp_port = 587
```

Рисунок 4.8 – Налаштування електронної пошти

Формування повідомлення. При виявленні загрози формується текстове повідомлення, яке містить інформацію про виявлену загрозу. Це повідомлення

включає заголовок та текстовий вміст, який містить короткий опис виявленої потенційної загрозової дії.

Для відправлення електронної пошти використовується бібліотека `smtpplib`. Спочатку здійснюється спроба встановлення з'єднання з сервером SMTP, а після успішної аутентифікації відправляється електронне повідомлення.

Також реалізовано механізм обробки помилок, щоб уникнути відключення програми в разі невдалої спроби надіслати електронне повідомлення. Якщо спроба відправлення не вдається, то виводиться відповідне повідомлення.

Після вдалого відправлення електронного листа генерується лог повідомлення, яке підтверджує успішну доставку.

```
def send_email(message):
    try:
        # Налаштування MIMEText
        msg = MIMEText(message)
        msg["Subject"] = email_subject
        msg["From"] = email_sender
        msg["To"] = email_recipient

        # Налаштування SMTP server
        with smtpplib.SMTP(email_smtp_server, email_smtp_port) as server:
            server.starttls()
            server.login(email_sender, email_password)
            server.sendmail(email_sender, [email_recipient], msg.as_string())

        logger.info("Сповіщення електронною поштою надіслано.")
    except Exception as e:
        logger.error(
            f"Не вдалося надіслати сповіщення на електронну пошту: {e}")
```

Рисунок 4.9 – Функція `send_email()`

4.3 Перевірка роботи програми

Для перевірки роботи аналізатору мережевого трафіку варто внести шкідливу IP-адресу до файлу `malicious_ips`. У цьому випадку використано IP-адресу 192.168.1.109.

```

PS D:\Programming\traffic-analyzer> python traffic_analyzer.py
• WARNING:NetworkAnalyzer:Виявлено потенційну загрозу:
WARNING:NetworkAnalyzer:Ether / IP / TCP 192.168.1.109:49645 > 74.125.131.84:https PA / Raw
INFO:NetworkAnalyzer:Сповіщення електронною поштою надіслано.
WARNING:NetworkAnalyzer:Виявлено потенційну загрозу:
WARNING:NetworkAnalyzer:Ether / IP / TCP 192.168.1.109:49748 > 142.250.186.195:https PA / Raw
INFO:NetworkAnalyzer:Сповіщення електронною поштою надіслано.
INFO:NetworkAnalyzer:Сканування завершено. Перевірте наявність індикаторів загрози.
INFO:NetworkAnalyzer:Виявлені загрози:
INFO:NetworkAnalyzer:Ether / IP / TCP 192.168.1.109:49645 > 74.125.131.84:https PA / Raw
INFO:NetworkAnalyzer:Ether / IP / TCP 192.168.1.109:49748 > 142.250.186.195:https PA / Raw

```

Рисунок 4.10 – Виявлені шкідливі IP-адреси

Програма виявила потенційні загрози у мережі. Зокрема, виявлено два мережевих пакети з IP-адресою 192.168.1.109 (яку було додано у файл `malicious_ips`), що взаємодіють з різними зовнішніми IP-адресами на портах HTTPS.

Після виявлення цих загроз програма автоматично відправила сповіщення електронною поштою. Після завершення сканування програма вивела повідомлення про завершення та інформацію про всі виявлені загрози.

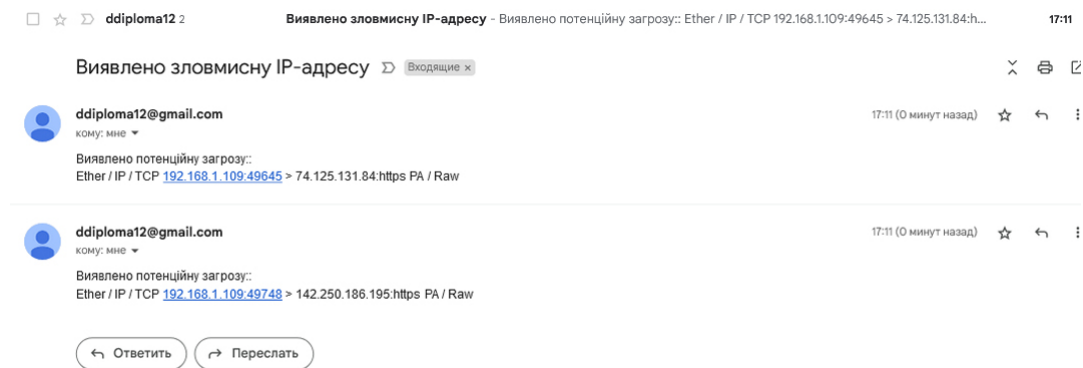


Рисунок 4.11 – Надіслані повідомлення

4.4 Переваги та обмеження реалізованого рішення

До переваг можна віднести ефективність виявлення загроз, гнучкість конфігурації за рахунок того, що кожен може сам настроїти параметри

аналізатора, включаючи файли сигнатур та тривалість сканування. Легкість розширення дозволяє додавати нові функціональності у майбутньому, що робить програму придатну для змін.

Однак, варто врахувати і обмеження до яких відноситься залежність від сигнатур, яка може привести до пропуску нових атак або виявлення фальшивих позитивів. До обмежень також відноситься область виявлення, яка спрямована лише на мережевий трафік.

4.5 Висновки до 4 розділу

Цей розділ є ключовим в цій дипломній роботі, оскільки саме тут здійснено практичну реалізацію засобу для виявлення кіберзагроз у мережевому трафіку.

Аналізатор трафіку відзначається простотою конфігурації, можливістю розширення, можливістю визначення сигнатур загрозливих пакетів, логуванні та зберіганні інформації про них та сповіщенні про виявлення загроз електронною поштою.

Щодо подальших досліджень та розвитку рекомендується акцентувати увагу на кількох ключових напрямках. Перше, це можливість розширення сигнатур та алгоритмів, використання додаткових методів аналізу. Друге, це вдосконалення механізму сповіщення про виявлені загрози, наприклад через телеграм бот. Також важливо зазначити про можливість застосування ІІІ та МН для автоматизації усіх процесів та виявлення нових типів атак.

Загалом, розроблене програмне забезпечення є ефективним та простим інструментом для виявлення кібератак. Воно може використовуватися для моніторингу мережі організації та реагуванню на атаки.

ВИСНОВКИ

В даній роботі були розглянуті питання захисту критичної інфраструктури від кібератак. Аналізуючи різні аспекти цієї проблеми, було виявлено, що кібератаки на критичну інфраструктуру стають все більш поширеними і серйозними загрозами для суспільства.

У першому розділі було проведено класифікацію кіберзагроз та описані їх характеристики. Це дозволило зрозуміти різноманітність і складність кібератак, які можуть спрямовуватись на критичну інфраструктуру. Розглянуто скоординовані кібератаки, атаки нульового дня, файлові атаки та атаку вірусом "NotPetya". Ці приклади продемонстрували, наскільки серйозними можуть бути наслідки кібератак для критичної інфраструктури.

Другий розділ роботи було присвячено вибору методів та засобів протидії кібератакам. Обрані фреймворки, такі як Mitre ATT&CK Framework, Cyber Kill Chain, STRIDE, OWASP Risk Rating Methodology та NIST Cybersecurity Framework забезпечують комплексний підхід до виявлення, аналізу та управління кіберзагрозами. Використання інструментів виявлення та аналізу кібератак, такі як ELK Stack, Snort IDS, Suricata Networ IDS/IPS, дозволяють вчасно виявити аномалії та оперативно реагувати на загрози. Було не лише обрано методи та інструменти, але й розглянуто їх переваги та обмеження. Розглянута інформація є базовим фундаментом для вдосконалення та оптимізації систем аналізу кіберзагроз, який дозволяє забезпечити більш ефективний та стійкий захист об'єктів критичної інфраструктури. Використання цих фреймворків та IDS допоможе виявити та запобігти кібератакам на ранніх стадіях.

Третій розділ роботи спрямований на розроблення загальних механізмів та рекомендацій для поліпшення захисту критичної інфраструктури. На основі аналізу попередніх кібератак були вибрані фреймворки та засоби, які найкраще підійдуть для захисту критичної інфраструктури. Розроблені плани

навчання та тренуванню сприятимуть підвищенню обізнаності персоналу, що знизить ризик того, що наступна атака буде вдалою. Обрані механізми є ефективним способом підвищення рівня захисту енергетичної системи від кіберзагроз.

Нарешті, у четвертому розділі було розроблено програмне забезпечення на Python, яке здатне аналізувати мережевий трафік та виявляти потенційні загрози, що базуються на сигнатурах. Важливою частиною є сповіщення про виявлення загроз електронною поштою, що дозволяє своєчасно реагувати на потенційні атаки. Також слід зазначити можливість інтеграції цього інструменту у вже існуючі системи моніторингу та управління безпекою. В цілому, четвертий розділ вносить важливий внесок у створення комплексного підходу до кіберзахисту критичної інфраструктури, дозволяючи виявляти та реагувати на потенційні загрози у режимі реального часу.

Усі вищезгадані елементи створюють комплексний підхід до кібербезпеки, який враховує різноманітність загроз та захисних методів. Запропоновані рекомендації та розроблені механізми можуть слугувати основою для подальшого вдосконалення систем кіберзахисту об'єктів критичної інфраструктури.

Отже, на основі проведеної роботи можна зробити висновок, що захист критичної інфраструктури є надзвичайно важливим завданням для забезпечення стабільності та безпеки держави. Основною метою цього проєкту було визначення ефективних технологій та стратегій, які зможуть забезпечити надійний рівень безпеки критичній інфраструктурі. Результати дослідження досягли поставленої мети, розроблені рекомендації є значним внеском у розвиток галузі кібербезпеки критичної інфраструктури.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX : станом на 5 груд. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 10.09.2023).
2. Кібератаки російської федерації. Хронологія. Міністерство оборони України. URL: <https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html> (дата звернення: 17.09.2023).
3. How to delete multiple drives with Active@ KillDisk?. KillDisk: Disk Eraser, Wiper & Sanitizer - Erase HDD/SSD/USB/NVMe Securely. URL: <https://www.killdisk.com/blog-text2.htm> (дата звернення: 18.09.2023).
4. Учасники проєктів Вікімедіа. BlackEnergy – Вікіпедія. Вікіпедія. URL: <https://uk.wikipedia.org/wiki/BlackEnergy> (дата звернення: 20.09.2023).
5. Ковальчук В. 5. Заява очільника Укренерго про збій в автоматизації керування. URL: https://www.facebook.com/permalink.php?story_fbid=1798082313797621&id=100007876094707 (дата звернення: 20.09.2023).
6. Відключення електроенергії в Україні було хакерською атакою - BBC News Україна. BBC News Україна. URL: <https://www.bbc.com/ukrainian/news-38585587> (дата звернення: 20.09.2023).
7. Petya (malware family). Wikipedia. URL: https://en.wikipedia.org/wiki/Petya_and_NotPetya (date of access: 25.09.2023).
8. How Does Baldrige Cyber Work with the NIST Cyber Framework?. NIST. URL: <https://www.nist.gov/blogs/blogrige/how-does-baldrige-cyber-work-nist-cyber-framework> (дата звернення: 30.09.2023).
9. SCADA Networking Protocols and Basics. Nor-Cal Controls Blog. URL: <https://blog.norcalcontrols.net/scada-networking-protocols-and-basics> (дата звернення: 01.10.2023).
10. IEC 61850. IEC 61850. Вид. офіц. URL: <https://iec61850.dvl.iec.ch/what-is-61850/> (дата звернення: 01.10.2023).

11. Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA. Home Page | CISA. URL: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience> (date of access: 08.10.2023).
12. Баранов О. А. Про тлумачення та визначення поняття "кібербезпека". Правова інформатика. 2014. № 2 (42). С. 54–62.
13. Strom B. ATT&CK 101. Medium. URL: <https://medium.com/mitre-attack/att-ck-101-17074d3bc62> (дата звернення: 15.10.2023).
14. Lenaerts-Bergmans B. What is the Cyber Kill Chain? Introduction Guide - CrowdStrike. URL: <https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain> (дата звернення: 27.10.2023).
15. Guide for Conducting Risk Assessments. NIST SP 800-30 Rev. 1. 2012. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> (дата звернення: 29.10.2023).
16. Stouffe K., Zimmerman T., Tang C. Cybersecurity Framework Manufacturing Profile. NIST. 2017. URL: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf> (дата звернення: 29.10.2023).
17. Eleventh Hour CISSP®. Elsevier, 2017. URL: <https://doi.org/10.1016/c2016-0-00637-x> (дата звернення: 06.12.2023).
18. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems. IBM Research Division. 1999. (дата звернення: 06.12.2023).
19. Signature-Anomaly based Intrusion Detection Algorithm. м. National Institute of Technology, Kurukshetra, 15 берез. 2018 р (дата звернення: 06.12.2023).
20. Snorby: Modern Snort IDS frontend. Help Net Security. URL: <https://www.helpnetsecurity.com/2010/12/07/snorby/> (дата звернення: 10.11.2023).
21. Suricata (software). Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/Suricata_\(software\)](https://en.wikipedia.org/wiki/Suricata_(software)) (дата звернення: 19.12.2023).

22. What is ELK stack? - Elasticsearch, Logstash, Kibana Stack Explained - AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/what-is/elk-stack/?nc1=h_ls (дата звернення: 20.11.2023).
23. Apache Lucene. URL: <https://lucene.apache.org/> (дата звернення: 21.11.2023).
24. Responding to IT Security Audits: Improving Data Security Practices. Protecting Student Privacy | U.S. Department of Education. URL: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/issue-brief-responding-to-security-audits_0.pdf (дата звернення: 22.11.2023).
25. Alharbi M. Writing a Penetration Testing Report. White Paper. 200. URL: <https://sansorg.egnyte.com/dl/yNfjHOQix8> (дата звернення: 24.11.2023).
26. Elastic Stack. URL: <https://www.elastic.co/kibana> (дата звернення: 10.11.2023).
27. Examples of Phishing Sites | Binance. Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins. URL: <https://www.binance.com/en/support/faq/examples-of-phishing-sites-360020550592> (дата звернення: 25.11.2023).
28. Про електроенергетику : Закон України від 16.10.1997 р. № 575/97-ВР : станом на 1 лип. 2019 р. URL: <https://zakon.rada.gov.ua/laws/show/575/97-вр#Text> (дата звернення: 06.12.2023).
29. Ворожі хакери атакують критичну інфраструктуру України: працювати над посиленням захисту треба постійно. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/vorozhi-khakeri-atakuyut-kritichnu-infrastrukturu-ukrayini-pracyuvati-nad-posilennyam-zakhistu-treba-postiino>.(30.11.2023)
30. Signature-Anomaly based Intrusion Detection Algorithm. м. National Institute of Technology, Kurukshetra, 15 безез. 2018 р.