Державний торговельно-економічний університет
Кафедра інженерії програмногозабезпечення та кібербезпеки

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захист соціотехнічних систем від кібератак»

Студента 2м курсу, 8 групи,
спеціальності 125 «Кібербезпека»
освітньої програми
«Безпека систем електронних комунікацій в економіці» _____ Криворота Максима Ростиславовича
підпис студента

Науковий керівник
старший викладач кафедри
інженерії програмного
забезпечення та кібербезпеки _____ Костюк Юлія Володимирівна
підпис керівника

Гарант освітньої програми
кандидат технічних наук,
доцент кафедри інженерії
програмного забезпечення та
кібербезпеки _____ Савченко Тетяна Віталіївна
підпис гаранта

КИЇВ – 2023

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки
Освітній ступінь магістр
Освітня програма «Безпека систем електронних комунікацій в економіці»

Затверджую
Зав. кафедри інженерії програмного забезпечення та кібербезпеки
Криворучко О. В.
«16» листопада 2022 р.

Завдання
на випускну кваліфікаційну роботу студентові

Кривороту Максиму Ростиславовичу

(прізвище, ім'я, по батькові)

Тема випускної кваліфікаційної роботи «Захист соціотехнічних систем від кібератак»

Затверджена наказом ректора від «06» грудня 2022 р. № 3287

2. Строк здачі студентом закінченої роботи 15 листопада 2023 р.

3. Цільова установка та вихідні дані до роботи

Мета роботи полягає в забезпеченні безпеки та надійності комплексних систем, які об'єднують соціальні та технічні компоненти для забезпечення ефективного захисту соціотехнічних систем від кібератак.

Об'єктом дослідження є процес дослідження та впровадження заходів для покращення процесу ідентифікації та аутентифікації, які є складовою стратегії кібербезпеки.

Предмет дослідження: методи забезпечення безпеки соціотехнічних систем з метою розробки ефективних стратегій та інструментів для захисту соціотехнічних систем від кібератак.

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1 АНАЛІЗ ЗАГРОЗ СОЦІОТЕХНІЧНИХ СИСТЕМ

1.1. Огляд основних типів кібератак, спрямованих на соціотехнічні системи

1.2. Аналіз випадків кібератак на соціотехнічні системи

1.3 Виявлення загроз та ризиків для соціотехнічних систем

Висновки до розділу 1

РОЗДІЛ 2 МЕТОДИ ЗАХИСТУ СОЦІОТЕХНІЧНИХ СИСТЕМ

2.1. Огляд існуючих методів та технологій захисту соціотехнічних систем

2.2. Класифікація методів захисту залежно від типу кібератак

2.3. Дослідження сучасних рішень для виявлення та запобігання кібератакам на соціотехнічні системи

Висновки до розділу 2

РОЗДІЛ 3 РОЗРОБКА СТРАТЕГІЇ ЗАХИСТУ СОЦІОТЕХНІЧНИХ СИСТЕМ

3.1. Аналіз поточного стану захисту соціотехнічних систем

3.2. Вибір архітектури системи

3.3. Реалізація функціональності системи

Висновки до розділу 3

РОЗДІЛ 4 ДОСЛІДЖЕННЯ ТА РЕЗУЛЬТАТИ

4.1. Опис методики тестування та моделювання кібератак на соціотехнічні системи

4.2. Аналіз результатів розробки системи захисту

Висновки до розділу 4

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

6. Календарний план виконання роботи

№ пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1.	*Вибір теми випускної кваліфікаційної роботи*	*05.11.2022*	*05.11.2022*
2.	*Розробка та затвердження завдання на роботу магістра (стаціонар)*	*16.11.2022*	*16.11.2022*
3.	*Вступ та перелік літературних джерел*	*25.02.2023*	*25.02.2023*
4.	*Розробка технічного завдання*	*18.03.2023*	*18.03.2023*
5.	*Розділ 1. Аналіз загроз соціотехнічних систем – (ось так має бути скрізь*	*15.04.2023*	*15.04.2023*
6.	*Розділ 2. Методи захисту соціотехнічних систем*	*27.05.2023*	*27.05.2023*
7.	*Розділ 3. Розробка стратегії захисту соціотехнічних систем*	*24.06.2023*	*24.06.2023*
8.	*Розділ 4. Дослідження та результати*	*27.08.2028*	*27.08.2028*
9.	*Розробка системи захисту соціотехнічних систем*	*17.10.2023*	*17.10.2023*
10.	*Написання наукової статті*	*20.05.2023*	*20.05.2023*
11.	*Висновки та пропозиції*	*23.10.2023*	*23.10.2023*
12.	*Здача випускної кваліфікаційної роботи на кафедру (перша перевірка)*	*01.11.2023*	*01.11.2023*
13.	*Підготовка автореферату та презентації доповіді*	*04.11.2023*	*04.11.2023*
14.	*Попередній захист випускної кваліфікаційної роботи*	*09.11.2023 – 14.11.2023*	*14.11.2023*
15.	*Здача зброшурованої випускної кваліфікаційної роботи*	*15.11.2023*	*15.11.2023*
16.	*Зовнішнє рецензування випускної кваліфікаційної роботи*	*15.11.2023*	*15.11.2023*
17.	*Підготовка до публічного захисту випускної кваліфікаційної роботи*	*за розкладом роботи ЕК*	

7. Дата видачі завдання «16» листопада 2022 р.

8. Науковий керівник випускної кваліфікаційної роботи Костюк Ю.В.

(прізвище, ініціали, підпис)

9. Гарант освітньої програми Савченко Т.В.

(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент Криворот М.Р.

(прізвище, ініціали, підпис)

11. Відгук керівника випускної кваліфікаційної роботи

Науковий керівник випускної кваліфікаційної роботи

_____

(підпис, дата)

Відмітка про попередній захист _____

(ПІБ, підпис, дата)

12. Висновок про випускну кваліфікаційну роботу

Випускна кваліфікаційна робота студента_____ Криворота М.Р.

(прізвище, ініціали)

може бути допущена до захисту в екзаменаційній комісії.

Гарант освітньої програми _____ Савченко Т.В.

(прізвище, ініціали, підпис)

Завідувач кафедри _____ Криворучко О. В.

(підпис, прізвище, ініціали)

«_____»_____2023 р.

АНОТАЦІЯ

Відповідно до мети дослідження робота присвячена розробці системи захисту соціотехнічних систем. В результаті порівняльного аналізу аналогічних рішень визначено оптимальний набір технологій та підходів для забезпечення високого рівня захисту. Розробка серверної частини виконана в середовищі, що враховує сучасні тенденції та вимоги до безпеки. Використані передові технології для забезпечення ефективності та надійності системи захисту. Реалізація серверної частини відповідає високим стандартам безпеки та враховує специфіку соціотехнічних систем. Проведені дослідження та експерименти свідчать про те, що розроблена система забезпечує ефективний захист від різноманітних кібератак та інших загроз.

Ключові слова: кібератака, кіберзагрома, система захисту, соціотехнічні системи, цілісність даних, шифрування.

ABSTRACT

In accordance with the research objective, the work is dedicated to the development of a protection system for sociotechnical systems. As a result of a comparative analysis of similar solutions, an optimal set of technologies and approaches has been identified to ensure a high level of protection. The development of the server-side has been carried out in an environment that takes into account modern trends and security requirements. Advanced technologies have been utilized to ensure the efficiency and reliability of the protection system. The implementation of the server-side adheres to high security standards and considers the specifics of sociotechnical systems. Research and experiments conducted indicate that the developed system provides effective protection against various cyberattacks and other threats.

Keywords: cyber attack, cyber threat, security system, sociotechnical systems, data integrity, encryption.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КІБЕРАТАКА – кібернетична атака

СТС – соціотехнічна система

БЗ – безпека

ІТ – інформаційні технології

ЗБС – заходи безпеки

МСЗ – мережева безпека

ЗМД – загрози мережевої безпеки

ІС – інформаційна система

СЗЗ – соціальна захищеність засобів зв'язку

КВС – кібернетичні вразливості систем

РС – ризики кібербезпеки

АІС – антивірусні інструменти та програми

ОТП – одноразовий пароль

ІНС – інформаційна безпека

ЗМП – заходи моніторингу та превентивного реагування

БМПД – бездротова мережа передачі даних

КМ – комп’ютерна мережа

					ДТЕУ 125-07-09.МР			
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*				
Зав. каф.		Криворучко О.В.		25.02.23	*Захист соціотехнічних систем від кібератак*	*Стадія*	*Аркуш*	*Аркушів*
Керівник		Костюк Ю.В.		25.02.23		*ПС*	*2*	*60*
Гарант		Савченко Т.В.		25.02.23		*Факультет інформаційних технологій 2м курс, 7 група*		
Розробив		Криворот М.Р.		25.02.23	*Перелік умовних позначень,символів,одиниць,скорочень і термінів*			

ЗМІСТ

ВСТУП

Актуальність теми полягає в постійно зростаючій загрозі кібератак та кіберзагроз, яка насувається на різні сфери суспільства. Запитання безпеки цифрових даних та інформаційних систем стає важливим завданням для бізнесу, урядових установ, медичних організацій та приватних осіб. Зростання технологічних можливостей супроводжується високим рівнем вразливості перед кіберзагрозами, що підкреслює необхідність ефективних заходів з кіберзахисту. Використання технології блокчейну є одним із можливих шляхів підвищення рівня кібербезпеки через її характеристики, такі як децентралізація та невідкладність.

Мета дослідження полягає в забезпеченні безпеки та надійності комплексних систем , які об'єднують соціальні та технічні компоненти для забезпечення ефективного захисту соціотехнічних систем від кібератак.

Об'єктом дослідження є процес дослідження та впровадження заходів для покращення процесу ідентифікації та аутентифікації, які є складовою стратегії кібербезпеки.

Предметом дослідження є методи забезпечення безпеки соціотехнічних систем з метою розробки ефективних стратегій та інструментів для захисту соціотехнічних систем від кібератак.

					ДТЕУ 125-07-09.МР		
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*			
Зав. каф.		Криворучко О.В.		25.02.23	*Захист соціотехнічних систем від кібератак*	*Стадія*	*Аркуш*	*Аркушів*
Керівник		Костюк Ю.В.		25.02.23		*В*	*4*	*60*
Гарант		Савченко Т.В.		25.02.23		*Факультет інформаційних технологій 2м курс, 7 група*		
Розробив		Криворот М.Р.		25.02.23	*Вступ*			

Завдання дослідження:

- дослідити поточний стану сфери кібербезпеки соціотехнічних систем;

- проаналізувати програмне забезпечення, апаратне забезпечення;

- проаналізувати можливі кібератаки, які можуть впливати на безпеку соціотехнічних систем;

- розробити систему для запобігання кібератак;

- розробити конкретні рекомендації для підвищення рівня безпеки соціотехнічних систем від кібератак.

Наукова новизна полягає в розробці нових інструментів, алгоритмів захисту, які допомагають у забезпеченні ефективного захисту від кіберзагроз, а також в дослідженні новітніх технологій та їхній інтеграції в системи кіберзахисту для соціотехнічних систем.

Методи дослідження. Під час написання роботи були використані такі методи, як аналіз кіберзагроз, метод моделювання та симуляція, аналіз вимог безпеки, аналіз інформаціної системи та аналіз регулятивного середовища, дослідження соціальних аспектів: розгляд впливу кібератак на людей та соціальні системи, оцінка взаємодії між технічними та соціальними аспектами.

Практична цінність полягає в розробці конкретних та ефективних стратегій захисту від кіберзагроз у сучасних соціотехнічних системах. Дослідження може допомогти визначити конкретні вразливості, ризики та методи атак, що можуть бути спрямовані на такі системи.

РОЗДІЛ 1.АНАЛІЗ ЗАГРОЗ СОЦІОТЕХНІЧНИХ СИСТЕМ

1.1 Огляд основних типів кібератак, спрямованих на соціотехнічні системи

Для початку, варто зазначити, що кібератака — це спроба кіберзлочинців, хакерів або інших цифрових супротивників отримати доступ до комп'ютерної мережі або системи, як правило, з метою зміни, викрадення, знищення або розкриття інформації. При цьому кібератаки можуть бути спрямовані на широке коло жертв як на окремих користувачів, так і на підприємства і навіть уряди. Коли хакер націлюється на підприємства чи інші організації, мета хакера — отримати доступ до конфіденційних і цінних ресурсів компанії, таких як інтелектуальна власність (IP), дані клієнтів або платіжні деталі. Тому задля створення надійного захисту системи від кібератак, необхідно розглянути типи атак і їх характерні особливості [12].

Загально, шкідливе програмне забезпечення — це будь-яка програма або код, створений з метою завдати шкоди комп'ютеру, мережі чи серверу. Зловмисне програмне забезпечення охоплює багато підгруп, таких як програми-вимагачі, трояни, шпигунські програми, віруси, хробаки, клавіатурні шпигуни, боти, криптозлом та будь-які інші типи атак шкідливих програм, які використовують програмне забезпечення зловмисним чином. Програми-вимагачі, коли під час якої зловмисник шифрує дані жертви та пропонує надати ключ розшифровки в обмін на оплату. Атаки програм-вимагачів зазвичай здійснюються через шкідливі посилання, які надсилаються через фішингові електронні листи, але також

використовуються невиправлені вразливості та неправильні налаштування політики.

В сучасному цифровому світі соціотехнічні системи відіграють ключову роль у функціонуванні суспільства та організацій. Проте, їх важливість також робить їх привабливою мішенню для різноманітних кібератак. Основні типи кібератак, які можуть бути спрямовані на соціотехнічні системи (табл.1.1).

Таблиця 1.1

Основні типи кібератак

Тип	Опис
Віруси	Ці програмні загрози можуть розповсюджуватися через мережу та заражати комп'ютерні системи, використовуючи їх для незаконного доступу, поширення шкідливого програмного забезпечення або інших кіберзлочинних дій.
Фішинг	Фішингові атаки спрямовані на злам користувачів шляхом надання дезінформації або маніпуляції з метою вибору особистих або фінансових даних.
ДДОС-атаки	Ці атаки спрямовані на перевантаження серверів чи мережі, щоб недоступним ставав веб-сайт чи інші сервіси, що працюють в мережі.
Внутрішні загрози	Коли внутрішні працівники організації, навмисно чи ненавмисно, надають несанкціонований доступ до конфіденційної інформації або здійснюють інші дії, що можуть вразити безпеку системи.
Соціальна інженерія	Цей тип атаки використовує маніпуляцію психологічними чинниками, щоб змусити людей виконувати небезпечні дії або розкривати конфіденційну інформацію.
Зломування паролів	Злом паролів може стати першим кроком для отримання несанкціонованого доступу до системи або даних [15].

Розуміння цих типів кібератак є важливим для ефективного захисту соціотехнічних систем від потенційних загроз. Розгляд цих атак у вашій

дипломній роботі може допомогти ідентифікувати стратегії та заходи для покращення кібербезпеки соціотехнічних систем.

Троян− це зловмисне програмне забезпечення, яке виглядає як законне програмне забезпечення, замасковане під рідні програми операційної системи або нешкідливі файли, наприклад безкоштовні завантаження. Трояни встановлюються за допомогою методів соціальної інженерії, таких як фішинг або сайти-приманки.

Хробак− це автономна програма, яка розмножується та поширює свої копії на інші комп'ютери. Хробак може заразити свою ціль через уразливість програмного забезпечення або він може бути доставлений через фішинг чи смішинг. Вбудовані хробаки можуть змінювати та видаляти файли, впроваджувати більше шкідливого програмного забезпечення або розмножуватися на місці, доки цільова система не закінчить ресурси.

Безфайлове зловмисне програмне забезпечення – це тип зловмисної діяльності, яка використовує власні законні інструменти, вбудовані в систему, для здійснення кібератаки. На відміну від традиційного зловмисного програмного забезпечення, безфайлове зловмисне програмне забезпечення не вимагає від зловмисника встановлення будь-якого коду в системі цілі, що ускладнює його виявлення [24].

Шпигунське програмне забезпечення – це тип шкідливого програмного забезпечення, яке заражає комп’ютер або інший пристрій і збирає інформацію про веб-активність користувача без його відома чи згоди.

Рекламне програмне забезпечення − це тип шпигунського програмного забезпечення, яке спостерігає за діяльністю користувача в Інтернеті, щоб визначити, яку рекламу йому показувати. Хоча рекламне програмне забезпечення за своєю суттю не є шкідливим, воно впливає на продуктивність пристрою користувача та погіршує взаємодію з користувачем. Іншим видом атаки, пов’язаним з рекламою, є шкідливі

атаки, коли зловмисник, маючи доступ до серверу третьої сторони, впроваджує шкідливий код у медійну рекламу чи деякі її елементи, такі як рекламний банер, креативні зображення чи відеовміст. Після відкриття відвідувачем веб-сайту, зловмисний код в оголошенні встановлює на комп'ютер користувача зловмисне або рекламне програмне забезпечення. [10, с. 79-85]

Зловмисне програмне забезпечення Rootkit — це набір програмного забезпечення, призначеного для надання зловмисникам контролю над комп'ютерною мережею або програмою. Після активації шкідлива програма встановлює бекдор-експлойт і може доставити додаткові зловмисні програми. Експлойт — це частина програмного забезпечення або даних, яка випадково використовує дефект операційної системи або програми для надання доступу неавторизованим особам. Експлойт може бути використаний для встановлення нових шкідливих програм або викрадення даних. Scareware – це залякувальна програма, що змушує користувачів повірити, що їхній комп'ютер заражений вірусом. Як правило, користувач бачить програмне забезпечення як спливаюче вікно з попередженням про те, що його система заражена. Ця тактика залякування спрямована на те, щоб переконати людей встановити підроблене антивірусне програмне забезпечення, щоб видалити «вірус». Після завантаження підробленого антивірусного програмного забезпечення ваш комп'ютер може заразитися зловмисним програмним забезпеченням. Кейлоггери — це інструменти, які записують те, що людина вводить на пристрої. Незважаючи на те, що їх використання законне, багато з них є зловмисними. Під час атаки кейлоггера програмне забезпечення кейлоггера записує кожне натискання клавіші на пристрої жертви та надсилає його зловмиснику [27].

Ботнет є мережею комп'ютерів, заражених шкідливим програмним забезпеченням, якими керує пастух ботів (рис.1.1). Пастух ботів — це особа,

яка керує інфраструктурою бот-мережі та використовує скомпрометовані комп'ютери для здійснення атак, спрямованих на збій у цільовій мережі, ін'єкцію зловмисного програмного забезпечення, збір облікових даних або виконання завдань із інтенсивним навантаженням на ЦП.

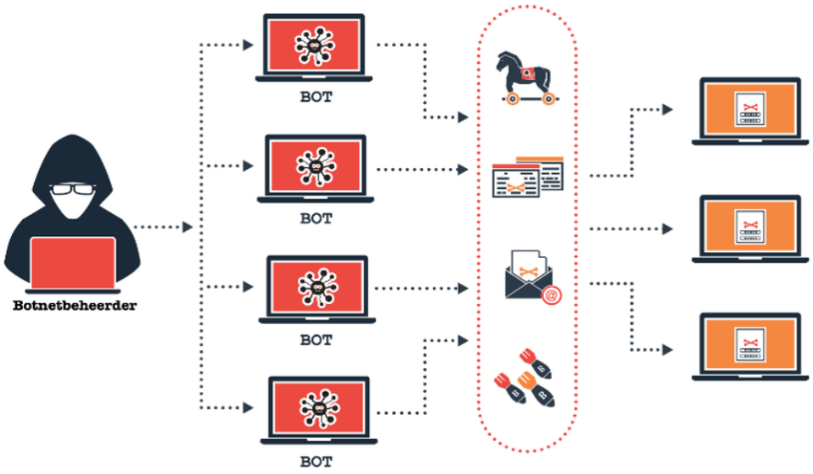


Рис. 1.1 Як працює Ботнет

Атака «Відмова в обслуговуванні» (DoS) – це зловмисна цілеспрямована атака, яка заповнює мережу помилковими запитами, щоб порушити бізнес-операції. Під час DoS-атаки користувачі не можуть виконувати звичайні та необхідні завдання, такі як доступ до електронної пошти, веб-сайтів, облікових записів в Інтернеті чи інших ресурсів, якими керує скомпрометований комп'ютер або мережа. Хоча більшість DoS-атак не призводять до втрати даних і, як правило, усуваються без виплати викупу, вони коштують організації часу, грошей та інших ресурсів для відновлення критичних бізнес-операцій. Різниця між атаками DoS і розподіленою відмовою в обслуговуванні (DDoS) пов'язана з походженням атаки. DoS-атаки походять лише з однієї системи, тоді як DDoS-атаки запускаються з кількох систем. DDoS-атаки є швидшими та складнішими для блокування, ніж DOS-атаки, оскільки для припинення атаки необхідно ідентифікувати та нейтралізувати кілька систем.

Фішинг − є різновидом кібератаки, яка використовує електронну пошту, SMS, телефон, соціальні мережі та методи соціальної інженерії, щоб спонукати жертву поділитися конфіденційною інформацією, як-от паролі чи номери облікових записів, або завантажити шкідливий файл, який інсталює віруси на їхній комп'ютер. або телефон. Підробка домену − це форма фішингу, коли зловмисник видає себе за відому компанію чи особу з підробленим веб-сайтом або доменом електронної пошти, щоб обдурити людей, щоб вони довіряли їм. Як правило, на перший погляд домен здається законним, але при ближчому розгляді можна виявити тонкі відмінності. Вішинг − голосова фішингова атака, являє собою шахрайське використання телефонних дзвінків і голосових повідомлень, видаючи себе за авторитетні організації, щоб переконати людей розкрити особисту інформацію, таку як банківські реквізити та паролі [18].

Спуфінг − це техніка, за допомогою якої кіберзлочинець маскується під відоме або надійне джерело. Таким чином зловмисник може вступити в ціль і отримати доступ до його систем або пристроїв з кінцевою метою викрадення інформації, вимагання грошей або встановлення зловмисного або іншого шкідливого програмного забезпечення на пристрої. Підробка протоколу ARP (Address Resolution Protocol, ARP) або отруєння ARP − це форма спуфінгу, яку хакери використовують для перехоплення даних. Хакер здійснює атаку ARP-спуфінгу, обманом змусивши один пристрій надіслати повідомлення хакеру замість передбачуваного одержувача. Таким чином хакер отримує доступ до комунікацій вашого пристрою, включаючи конфіденційні дані.

Підробка електронної пошти – це тип кібератаки, яка спрямована на бізнес за допомогою електронних листів із підробленими адресами відправників. Оскільки одержувач довіряє передбачуваному відправнику,

він, швидше за все, відкриє електронний лист і перегляне його вміст, наприклад шкідливе посилання чи вкладення [20].

Атака «Людина посередині» - це тип кібератаки, під час якого зловмисник підслуховує розмову між двома цілями з метою збору особистих даних, паролів або банківських реквізитів та/або переконати жертву вжити такі дії, як як зміна облікових даних для входу, завершення транзакції або ініціювання переказу коштів.

Атака передачі хешу — це тип атаки, під час якої зловмисник викрадає «хешовані» облікові дані користувача та використовує їх для створення нового сеансу користувача в тій самій мережі. Зловмиснику не потрібно знати або зламувати пароль, щоб отримати доступ до системи. Навпаки, він використовує збережену версію пароля для початку нового сеансу [21].

Атаки з використанням облікових даних — атаки, що працюють на основі того, що люди часто використовують той самий ідентифікатор користувача та пароль для кількох облікових записів. Тому, володіючи обліковими даними для одного облікового запису, можна надати доступ до іншого, не пов’язаного облікового запису.

Брутфорс — це використання методу систематичного вгадування інформації для входу, облікових даних і ключів шифрування. Зловмисник надсилає комбінації імен користувачів і паролів, поки вони нарешті не підійдуть.

Атаки з впровадженням коду - це впровадження зловмисником шкідливого коду у вразливий комп’ютер або мережу, щоб змінити курс дій. Існує кілька типів атак із впровадженням коду:

- SQL Injection, що використовує вразливі місця системи для введення зловмисних інструкцій SQL у керовану даними програму, яка потім дозволяє хакеру отримувати інформацію з бази даних. Хакери використовують

методи впровадження SQL, щоб змінити, викрасти або стерти дані бази даних програми.

- XSS(Міжсайтовий скриптинг), під час якої зловмисник вставляє шкідливий код на веб-сайті. Потім код запускається як інфікований сценарій у веб-браузері користувача, що дозволяє зловмиснику викрасти конфіденційну інформацію або видати себе за користувача. Веб-форуми, дошки оголошень, блоги та інші веб-сайти, які дозволяють користувачам публікувати власний вміст, найбільш сприйнятливі до атак XSS [28].

Атака на ланцюжок поставок − це тип кібератаки, спрямований на надійного стороннього постачальника, який пропонує послуги або програмне забезпечення, життєво важливі для ланцюга поставок. Атаки на ланцюг поставок програмного забезпечення вводять шкідливий код у програму, щоб заразити всіх користувачів програми, тоді як атаки на ланцюг поставок апаратного забезпечення компрометують фізичні компоненти з тією ж метою.

APT − це довготривалі, складні кібератаки, організовані кваліфікованими супротивниками. Вони включають кілька векторів атаки, в тому числі соціальну інженерію, шкідливе програмне забезпечення та використання вразливостей "нульового дня". APT-атаки часто націлені на урядові установи, об'єкти критичної інфраструктури та великі організації [9].

1.2.Аналіз відомих випадків кібератак на соціотехнічні системи

Розглянемо більш детальний аналіз кількох кібератак, що відбулися в період з 2022 по 2023 роки та методи, які були використані.

1. Одним з найвідомих випадків є атака «нульового дня» на Twitter, що відбулася у 2022 році. За підсумками, зловмисники отримали доступ до особистої інформації 5,4 мільйонів облікових записів. Вразливість дозволяла будь-кому надіслати електронну адресу або номер телефону, перевірити, чи вона пов'язана з обліковим записом Twitter, і отримати пов'язаний ідентифікатор облікового запису. З технічної точки зору, ця вразливість дозволяє будь-якій стороні без автентифікації отримати ідентифікатор Twitter (який практично рівносильний імені користувача облікового запису) будь-якого користувача, навіть якщо користувач заборонив цю дію в налаштуваннях конфіденційності.

За офіційними заявами Twitter, ця помилка сталася внаслідок оновлення їх коду в червні 2021 року. Коли вони дізналися про це, вони одразу провели розслідування та виправили це. В той час компанія не мала доказів, які свідчили б, що хтось скористався цією вразливістю. І для всіх користувачів, які працюють під псевдонімом на обліковому записі Twitter, вони рекомендували не додавати відомий публічно номер телефону або адресу електронної пошти до облікового запису Twitter, щоб зберегти свою ідентичність як можна більше в прихованому вигляді [1].

2. Починаючи від 14 січня 2022 року і до поточного часу, Україна знаходиться на першому місці за кількістю кібератак. Причиною цьому є вторгнення росії в кіберпростір шляхом DDoS-атак, атак на ланцюжки постачання та фішингу. Варто зазначити, що хоча серйозних наслідків ці атаки не завдали, велика кількість як фізичних, так і юридичних осіб залишились постраждалими. У фокусі уваги зловмисників – телеком-провайдери, компанії, що забезпечують зв’язок і розробляють програмне забезпечення та логістичні компанії.

Доволі поширена проблема в тому, що в Україні досі не всі адміністратори онлайн-систем вчасно оновлюють програмне забезпечення, і навіть не всі використовують ліцензійне ПЗ [2].

3. 15 вересня 2022 року відбулась атака на компанію Uber, в наслідок якої зловмисник отримав повні права доступу до внутрішніх систем. За даними, хакер отримав контроль над внутрішніми системами компанії, використовуючи техніки соціальної інженерії, що призвели до компрометації облікового запису співробітника в Slack. Хакер відправив текстове повідомлення співробітнику Uber, яке видавалося як лист від відділу IT Uber. Співробітник вважав його легітимним повідомленням від власного відділу і поділився своїм паролем. Хакер здобув доступ до особистої інформації 57 мільйонів користувачів Uber, включаючи їх імена, електронні адреси і номери телефонів. Компанія виплатила хакерові 100 000 доларів за знищення доказів і зберігання таємниці щодо того, що сталося [3].

Це лише декілька прикладів визначених кібератак, які відбулися з 2022 по 2023 рік. Вони демонструють різноманітність тактик, від використання соціальної інженерії до компрометації ланцюга постачання та використання вразливостей програмного забезпечення. Кібербезпека залишається критично важливою галуззю, і організації продовжують інвестувати у покращення захисту від зростаючих загроз.

1.3.Виявлення загроз та ризиків для соціотехнічних систем

Виявлення загроз і ризиків у соціотехнічних системах є критично важливим аспектом забезпечення їхньої безпеки та стійкості. Соціотехнічні системи є складними, взаємопов'язаними середовищами, які поєднують

людські та технологічні компоненти, що робить їх вразливими до широкого спектру загроз.

Ефективне виявлення цих загроз і ризиків вимагає комплексного і проактивного підходу із залученням різних стратегій і технологій, а саме:

- Розвідка та моніторинг загроз, збір та аналіз інформації про потенційні загрози, зловмисників та їхню тактику. Організації можуть використовувати канали розвідки загроз, рекомендації з безпеки та моніторинг даркнету, щоб бути в курсі нових загроз і вразливостей, які можуть вплинути на їхні соціотехнічні системи [16].
- Використання рішень SIEM, що збирають та аналізують дані журналів з різних джерел, таких як мережеві пристрої, сервери та додатки. Співставляючи ці дані та застосовуючи поведінкову аналітику, SIEM допомагає виявляти аномалії та потенційні інциденти безпеки в режимі реального часу, забезпечуючи швидке реагування та розслідування відхилень від нормальних шаблонів. Незвичайні дії, такі як спроби несанкціонованого доступу або неочікувана передача даних, можуть викликати сповіщення для подальшого розслідування.
- Проведення аналізу мережевого потоку та глибокої перевірки пакетів задля ретельного вивчення мережевого трафіку, допомагаючи виявити підозрілі дії, передачу шкідливого програмного забезпечення або несанкціоновану витоку даних.
- Відстеження і запис активності кінцевих точок за допомогою інструментів EDR, дозволяючи проводити ретроспективне розслідування і надаючи контекст для реагування на інциденти. Вони можуть виявляти шкідливі процеси, модифікації файлів та інші ознаки компрометації на окремих пристроях [26].
- Регулярне сканування вразливостей і тестування на проникнення, що допоможе виявити потенційні слабкі місця в соціотехнічних системах

моделюючи реальні сценарії атак, організації можуть визначати пріоритети та усувати недоліки безпеки до того, як вони будуть використані.

- Планування та навчання з реагування на інциденти при регулярному проведенні допоможе забезпечити готовність команд до швидкого та ефективного реагування в разі реального порушення безпеки.

Виявлення та зменшення загроз і ризиків у соціотехнічних системах є багатогранним процесом, що поєднує технології, людський досвід та співпрацю. Впроваджуючи комплексний підхід до безпеки, організації можуть підвищити свою стійкість до кіберзагроз, що розвиваються, і захистити свої критичні активи і дані. Регулярна оцінка, постійне вдосконалення та адаптивність є ключовими факторами для підтримання сильних позицій захисту в сучасному динамічному ландшафті загроз.

Висновки до розділу 1

Перший розділ висвітлює проблему розвитку кіберзагроз та кібератак. Це стає зростаючою загрозою для різних сфер, включаючи корпоративний сектор, урядові установи, медичні установи та приватних осіб. Цей тренд посилюється зростанням технологічних можливостей, а разом з тим і вразливість перед кіберзагрозами. Забезпечення безпеки інформації та захист від кібератак набуває визначального значення для всіх, хто оперує цифровими даними та системами. Враховуючи різноманітні типи атак, такі як спуфінг, підробка електронної пошти, атака "Людина посередині" та атака передачі хешу, важливо наголосити на необхідності розвитку комплексних стратегій кіберзахисту та посилення свідомості користувачів щодо соціального інжинірингу.

Аналізуючи кібератаки з 2022 по 2023 рік, видно кілька ключових тенденцій. Перш за все, атаки "нульового дня" продовжують

використовуватися для отримання несанкціонованого доступу до систем. Крім того, Україна стає активним об'єктом кібератак, з великим навантаженням на телекомунікаційні компанії та розробників програмного забезпечення. Атаки з використанням соціальної інженерії, як випадок з Uber, вказують на важливість кіберосвідомості серед персоналу. Кібербезпека залишається важливим аспектом, інвестиції в який є критичними для захисту від різноманітних загроз.

Забезпечення безпеки соціотехнічних систем вимагає комплексного підходу, об'єднуючи розвідку, моніторинг, використання SIEM, аналіз мережевого потоку, інструменти EDR, сканування вразливостей та планування реагування на інциденти. Постійна оцінка та адаптація ключові для зміцнення захисту у сучасному ландшафті кіберзагроз.

РОЗДІЛ 2.МЕТОДИ ЗАХИСТУ СОЦІОТЕХНІЧНИХ СИСТЕМ

2.1 Огляд існуючих методів та технологій захисту соціотехнічних систем

Сучасний ландшафт соціотехнічних систем постійно розвивається і вдосконалюється, що накладає великий акцент на важливість заходів забезпечення їхньої безпеки та надійності. Огляд існуючих методів та технологій захисту є кроком у напрямку розуміння цього складного завдання. У цьому контексті важливо ретельно розглянути різні аспекти та можливості, які пропонуються сучасною індустрією безпеки та дослідницькими групами [14].

По-перше, необхідно розглянути технологічний підхід до захисту соціотехнічних систем. Наприклад, використання сучасних антивірусних програм, які постійно оновлюють свої бази даних для виявлення нових загроз, може служити ефективним заходом захисту від шкідливих програм. Наприклад, встановлення відомого антивірусного рішення, такого як Norton або McAfee, допомагає у вчасному виявленні інфікованих файлів та їхньому ізоляції перед спричиненням можливих шкідливих наслідків.

По-другу, соціальний аспект важливий у сфері захисту соціотехнічних систем. Наприклад, освічені користувачі можуть стати першими ланками в ланцюзі захисту. Правильна навчаність співробітників може запобігти атакам, коли зловмисники використовують маніпуляцію або обман, щоб отримати доступ до системи. Наприклад, співробітники фінансових установ можуть бути навчені

розпізнавати телефонні або електронні атаки, де аферисти намагаються отримати конфіденційну інформацію, видаючи себе за авторитетних осіб.

По-третє, важливо розглянути питання апаратної безпеки. Наприклад, сучасні системи використовують біометричні методи для аутентифікації, такі як відбитки пальців або розпізнавання обличчя. Ці технології можуть бути впроваджені для забезпечення фізичного захисту об'єктів та даних. Наприклад, смартфони, які використовують розпізнавання обличчя, стають все більш поширеними, оскільки ця технологія надає додатковий рівень безпеки для особистих даних користувачів.

По-четверте, однією з ключових складових сучасного захисту соціотехнічних систем є моніторинг та виявлення вторгнень. Системи моніторингу дозволяють постійно відслідковувати активність в мережі та виявляти незвичайні або підозрілі події. Наприклад, система виявлення вторгнень, яка аналізує великі обсяги мережевого трафіку, може спостерігати за змінами в звичайному зразку активності та автоматично сповіщати адміністраторів про потенційні загрози.

По-п'яте, важливим аспектом є аналіз загроз та ризиків для соціотехнічних систем. Наприклад, в банківській галузі, де конфіденційність та фінансова безпека є критичними, здійснюється постійний аналіз потенційних атак і їхніх наслідків. На основі цього аналізу розробляються стратегії та заходи забезпечення безпеки, які допомагають запобігти можливим загрозам [25].

Щоб забезпечити конфіденційність, цілісність і доступність інформації(рис. 2.1), організації можуть вибирати з безлічі інструментів. Кожен із цих інструментів можна використовувати як частину загальної політики інформаційної безпеки, про яку йтиметься в наступному розділі.

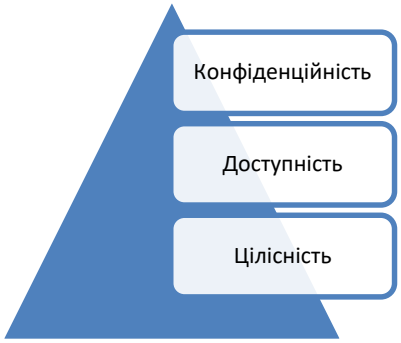


Рис. 2.1 Тріада кібербезпеки

Варто зазначити, що контроль доступу складається з усіх політик і процедур, які використовує компанія для запобігання неправомірному доступу до систем неавторизованих інсайдерів і сторонніх осіб. Саме для цього використовується процес аутентифікації – перевірки на те, що людина є тим, за кого себе видає.

Інструменти аутентифікації використовуються для того, щоб переконатися, що особа, яка отримує доступ до інформації, справді є тією, за кого себе представляє. Її можна здійснити шляхом ідентифікації людини за одним або декількома з трьох факторів: те, що вони знають, те, що вони мають, або те, чим вони є.

Наприклад, найпоширенішою формою аутентифікації сьогодні є ідентифікатор користувача та пароль. У цьому випадку аутентифікація виконується шляхом підтвердження того, що користувач знає (його ідентифікатор та пароль). Але цю форму аутентифікації легко скомпрометувати, і іноді потрібні більш надійні форми аутентифікації. Ідентифікувати когось лише за тим, що у нього є, наприклад, за ключем чи карткою, також може бути проблематично. Якщо ідентифікаційний маркер втрачено або викрадено, ідентифікаційну інформацію можна легко вкрасти. Набагато важче сфальсифікувати останній фактор, яким ви є. Цей фактор ідентифікує користувача за допомогою фізичних характеристик, таких як сканування ока або відбиток пальця. Ідентифікація людини за її фізичними характеристиками називається біометрією [25].

Також зустрічається більш безпечний спосіб аутентифікації користувача — багатофакторна аутентифікація. Поєднуючи два чи більше факторів, перерахованих вище, комусь стає набагато важче представити себе в оманливій формі. Прикладом цього може бути використання маркера RSA SecurID . Пристрій RSA — це те, що у вас є, і він генеруватиме новий код доступу через кожний фіксований проміжок часу. Щоб увійти на інформаційний ресурс за допомогою пристрою RSA, ви поєднуєте відомий вам чотиризначний PIN-код із кодом, згенерованим пристроєм.

Після аутентифікації користувача наступним кроком є переконатися, що він може отримати доступ лише до відповідних інформаційних ресурсів. Це робиться за допомогою контролю доступу. Контроль доступу визначає, хто з користувачів має право читати, змінювати, додавати та/або видаляти інформацію. Існує кілька різних моделей контролю доступу. Тут ми обговоримо контроль доступу на основі ролей (RBAC).

Для кожного інформаційного ресурсу, яким організація бажає керувати, можна створити список користувачів, які мають можливість виконувати певні дії. Це список контролю доступу або ACL, де для кожного користувача призначаються певні можливості, такі як читання, запис, видалення або додавання . Лише користувачі з такими можливостями можуть виконувати ці функції. Якщо користувача немає в списку, він не має можливості навіть знати про існування інформаційного ресурсу. Модель RBAC грунтується на видачі користувачам доступу залежно від їх ролі в організації, а не на основі ідентичностей. Мета полягає в тому, щоб надавати користувачам доступ лише до тих даних, які їм потрібні для виконання робочих завдань [4].

Проходження перевірки на належний доступ користувачу здійснюється за допомогою брандмауеру(Рис 2.2) — поєднання апаратного та програмного забезпечення, яке контролює потік вхідного та вихідного мережевого трафіку та запобігає несанкціонованому обміну даними в мережі та з неї. Брандмауер визначає імена, адреси Інтернет-протоколу (IP), програми та інші характеристики вхідного трафіку. Він перевіряє цю інформацію на відповідність правилам доступу, запрограмованим у системі адміністратором мережі. Існує кілька технологій перевірки брандмауером [13, с. 678]:

- Фільтрування пакетів перевіряє поля в заголовках пакетів даних, що передаються між мережею та Інтернетом, аналізуючи окремі пакети окремо.
- Перевірка стану визначає, чи є пакети частиною поточного діалогу між відправником і одержувачем.
- Трансляція мережевих адрес (NAT) приховує IP-адреси внутрішнього хост-комп'ютера(-ів) організації для захисту від програм-аналізаторів за межами брандмауера.
- Фільтрація проксі-сервера програми перевіряє вміст пакетів програми. Проксі-сервер зупиняє пакети даних, що надходять за межі організації, перевіряє їх і передає проксі-сервер на іншу сторону брандмауера. Якщо користувач за межами компанії хоче спілкуватися з користувачем всередині організації, зовнішній користувач спочатку «розмовляє» з проксі-додатком, а проксі-додаток зв'язується з внутрішнім комп'ютером фірми.

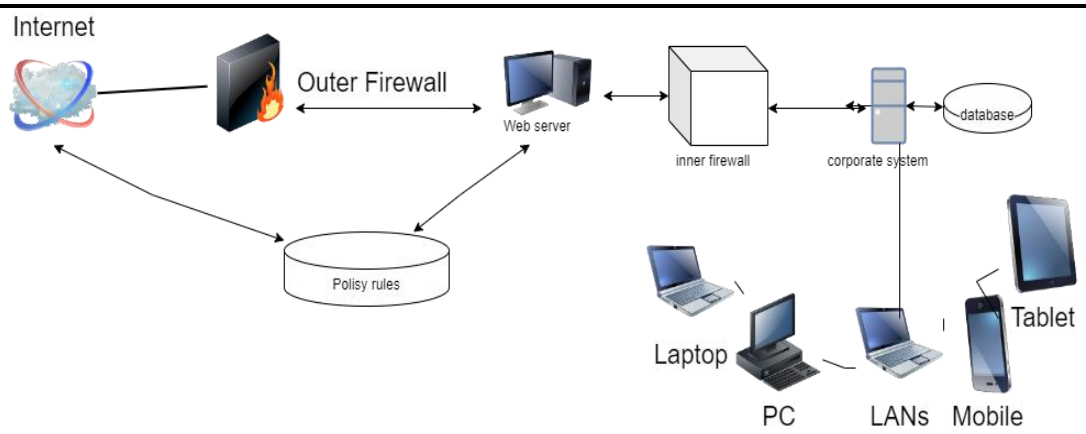


Рис. 2.2. Корпоративний брандмауер

Брандмауер розміщується між приватною мережею фірми та публічним Інтернетом або іншою ненадійною мережею для захисту від неавторизованого трафіку.

Щодо систем виявлення вторгнень, то вони містять засоби постійного моніторингу, розміщені в найбільш уразливих точках корпоративних мереж, щоб постійно виявляти та відлякувати зловмисників. Програмне забезпечення для сканування шукає шаблонні дії, що вказують на відомі методи комп'ютерних атак, наприклад неправильні паролі, перевіряє, чи видалено чи змінено важливі файли, і надсилає попередження про вандалізм або помилки системного адміністрування. Так, саме антивірусне програмне забезпечення призначене для перевірки комп'ютерних систем і дисків на наявність комп'ютерних вірусів. Однак, щоб залишатися ефективним, антивірусне програмне забезпечення має постійно оновлюватися.

Іншим, не менш важливим, є шифрування, яке використовується організаціями для захисту конфіденційної інформації, що передається через мережі. Шифрування — це кодування та шифрування повідомлень для запобігання доступу до них неавторизованих осіб.

Розглянемо два способи шифрування мережевого трафіку в Інтернеті:

- SSL і його наступник Безпека транспортного рівня (TLS) дозволяють клієнтським і серверним комп’ютерам встановлювати сеанс безпечного з’єднання та керувати діями шифрування та дешифрування.
- Захищений протокол передачі гіпертексту (S-HTTP) — це ще один протокол, який використовується для шифрування даних, що передаються через Інтернет, але він обмежений окремими повідомленнями.

Дані шифруються шляхом застосування секретного числового коду, який називається ключем шифрування, таким чином дані передаються як зашифрований набір символів. Щоб повідомлення було прочитано, його потрібно розшифрувати (розшифрувати) за допомогою відповідного ключа [7]. Є два альтернативних методу шифрування:

Шифрування з симетричним ключем: відправник і одержувач створюють єдиний ключ шифрування, який спільно використовується.

Шифрування з відкритим ключем(Рис 2.3): безпечніший метод шифрування, який використовує два різні ключі, один закритий і один публічний.

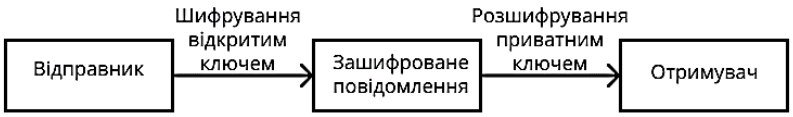


Рис. 2.3. Шифрування з відкритим ключем

Цифрові підписи та цифрові сертифікати(Рис 2.4) також допомагають при аутентифікації.

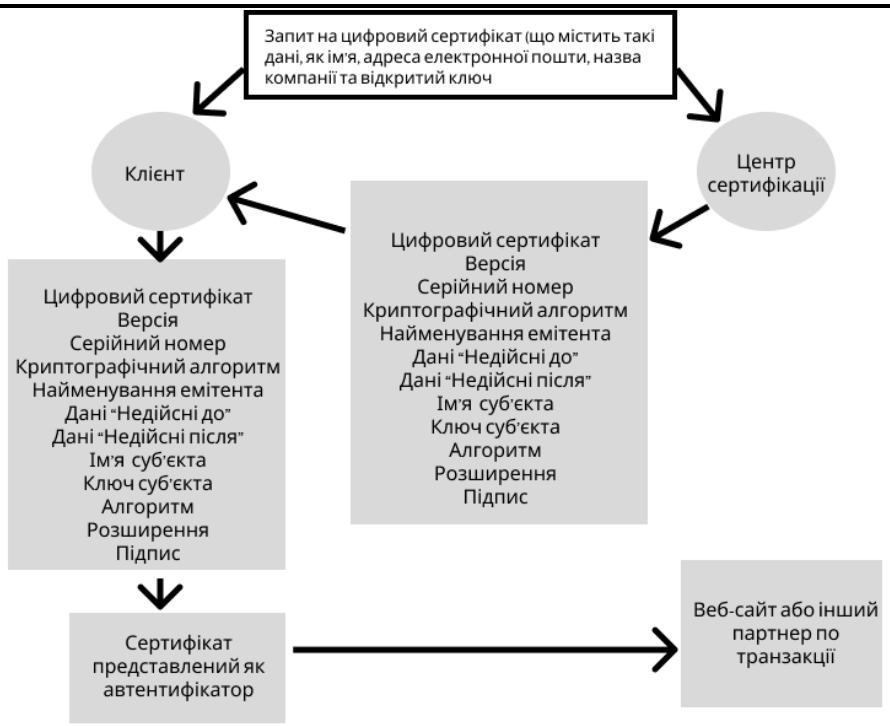


Рис. 2.4. Електроні сертифікати(Або ЕЦП)

Цифровий підпис — це цифровий код, доданий до електронного повідомлення, який використовується для перевірки походження та змісту повідомлення. Цифрові сертифікати — це файли даних, які використовуються для встановлення особи користувачів і електронних активів для захисту онлайн-транзакцій. Система цифрових сертифікатів використовує довірену третю сторону, відому як центр сертифікації (CA), щоб перевірити особу користувача. Система цифрових сертифікатів дозволить, наприклад, користувачу кредитної картки та продавцю підтвердити, що їхні цифрові сертифікати видані уповноваженою та надійною третьою стороною, перш ніж вони обміняються даними. Інфраструктура відкритих ключів (PKI) , використання криптографії відкритих ключів, що працює з центром сертифікації, є основною технологією для забезпечення безпечної автентифікації особи в Інтернеті.

2.2.Класифікація методів захисту залежно від типу кібератак та їх впливу на соціотехнічні системи

Зі зростанням залежності від цифрових технологій і взаємопов'язаних систем зросла частота і складність кібератак. Для захисту від кіберзагроз було розроблено різноманітні методи захисту, пристосовані до конкретних типів кібератак та їх потенційного впливу на соціотехнічні системи. У цьому розділі представлено комплексну класифікацію методів захисту, засновану на характері кібератак і вразливостях, які вони експлуатують. Вона має на меті дослідити та зрозуміти мінливий ландшафт кіберзахисту і приймати обґрунтовані рішення при розробці стратегій кібербезпеки.

Першочергово варто розглянути превентивний захист, спрямований на запобігання кібератакам до того, як вони зможуть використати вразливості. Ця категорія включає такі методи, як брандмауери, системи виявлення/запобігання вторгнень (IDS/IPS), антивірусне програмне забезпечення, білі списки додатків та безпечні практики розробки програмного забезпечення. Ці засоби захисту спрямовані на виявлення та блокування зловмисних дій і несанкціонованого доступу, мінімізуючи ймовірність успішних атак. Механізми контролю доступу та аутентифікації призначені для обмеження несанкціонованого доступу до критично важливих систем та ресурсів. Такі методи, як багатофакторна аутентифікація (MFA), контроль доступу на основі ролей (RBAC) та біометрична аутентифікація допомагають перевірити особу користувачів та обмежити доступ лише для уповноваженого персоналу [8].

До наступних засобів захисту, що базуються на виявленні та реагуванні, і які зосереджені на виявленні кібератак під час їх здійснення та оперативному реагуванні для зменшення їхнього впливу належать системи управління інформацією та подіями безпеки (SIEM), системи аналітики безпеки, команди реагування на інциденти та методи полювання на загрози.

Саме швидке виявлення та реагування може зменшити потенційну шкоду, спричинену кібератаками.

Також окремо необхідно виділити криптографію та методи шифрування конфіденційних даних та комунікації. Шифрування даних під час передачі та у стані спокою гарантує, що навіть якщо зловмисники отримають доступ до інформації, вони не зможуть зрозуміти або використати її без ключа розшифрування. Сюди ж можна віднести і сегментацію мережі, що передбачає поділ мережі на менші, ізольовані підмережі, зменшує поверхню атаки та обмежує бічний рух зловмисників, що допоможе при таких видах атаки, як DDoS. Якщо відбувається зловмисне втручання, сегментація мережі запобігає доступу зловмисників до всієї інфраструктури. А регулярне резервне копіювання даних і планування аварійного відновлення має вирішальне значення для пом'якшення наслідків атак з вимогою викупу та інших інцидентів, пов'язаних з втратою даних. Наявність надійних резервних копій дозволяє організаціям відновити дані та відновити роботу після атаки.

Надійна стратегія кіберзахисту має важливе значення для захисту соціально-технічних систем від зростаючих загроз кібератак. Ця класифікація методів захисту, заснована на типах кібератак і їх впливі на соціально-технічні системи, забезпечує цінну основу для організацій і дослідників для розробки комплексних стратегій кібербезпеки. Багаторівневий підхід, що поєднує запобігання, виявлення, реагування та інформування користувачів, має вирішальне значення для зміцнення захисту від постійно мінливого ландшафту кіберзагроз. Постійне вдосконалення, регулярні оцінки та співпраця в рамках спільноти кібербезпеки є життєво важливими для того, щоб випереджати кіберсупротивників та захищати критичні активи та інформацію.

2.3.Дослідження сучасних рішень для виявлення та запобігання кібератакам на соціотехнічні системи

Кібератаки стають все більш витонченими і становлять значні загрози для соціотехнічних систем, охоплюючи як технічні, так і людські елементи. Щоб протистояти цим загрозам, дослідники і практики постійно розробляють і досліджують сучасні рішення для виявлення і запобігання кібератакам.

Розділ має на меті надати комплексний огляд сучасних механізмів захисту, методологій та технологій, які з'явилися для захисту соціотехнічних систем. Дослідження охоплює низку підходів, серед яких методи на основі штучного інтелекту (ШІ), виявлення аномалій, поведінковий аналіз та обмін даними про загрози. [6]

Штучний інтелект (ШІ) і машинне навчання (МН) зробили революцію в галузі кібербезпеки, уможлививши автоматизований аналіз і прийняття рішень. Рішення на основі ШІ застосовуються для виявлення і запобігання кібератакам у режимі реального часу, використовуючи величезні обсяги даних зловмисної активності. Алгоритми МН можуть підвищити точність систем виявлення вторгнень, прогнозувати потенційні кіберзагрози та допомагати в поведінковому аналізі для виявлення внутрішніх загроз. Ці методи довели свою ефективність у боротьбі з масштабними та складними кіберзагрозами.

Також ШІ займає значну позицію у виявленні аномалій - важливий компонент кібербезпеки, який фокусується на виявленні відхилень від нормальної поведінки системи. Встановивши базові лінії очікуваної діяльності, можна виявити будь-які відхилення, які можуть свідчити про зловмисні дії або компрометацію системи. Цей підхід особливо ефективний у виявленні нових і раніше небачених кібератак. Однак він також створює

проблеми, оскільки відрізнити справжні аномалії від хибних спрацьовувань може бути складно.

Особливо важливим для запобігання внутрішнім загрозам і сценаріям компрометації облікових записів є поведінковий аналіз. Він передбачає моніторинг та аналіз поведінки користувачів для виявлення підозрілих дій, які можуть свідчити про несанкціонований доступ або скомпрометовані облікові записи. Цей підхід враховує дії та взаємодію користувачів, систем і додатків, щоб виявити незвичні патерни. І в сучасному кіберпросторі цей метод не може йти без підключення контекстного визначення, що допомагає приймати кращі рішення щодо впровадження безпеки в режимі реального часу. Якщо традиційні технології кібербезпеки визначають, дозволяти комусь доступ до системи чи даних, ставлячи питання або «так» або «ні», то це може призвести до того, що деяким авторизованим користувачам буде відмовлено у доступі, у той час, як зловмисникам навпаки – надано доступ [23]. Контекстно-визначена безпека зменшує ймовірність заборони входу авторизованому користувачеві. Замість того, щоб покладатися на відповіді на статичні запитання «так/ні», ця технологія використовує різну допоміжну інформацію, як, наприклад: місцеперебування, час, репутацію URL-адреси тощо щоб визначити, чи є користувач верифікованим, чи ні.

Іншим новітнім впровадженням є використання хмарних сервісів, що хоч і може збільшити вразливість даних, але водночас пропонує організаціям покращені дистанційні послуги та економію грошей. Хмарні технології зосереджені на захисті даних, додатків та інфраструктури, розміщених у хмарних середовищах.

Потенційні можливості для посилення кібербезпеки також має використання блокчейну - децентралізованої і захищена від

несанкціонованого доступу технології реєстру. Притаманні їй незмінність і прозорість можуть бути використані для захисту критично важливих даних, перевірки особи і створення довіри до транзакцій.

Останнім розглянемо метод кібер-обману, що передбачає розгортання приманок і фейкових активів, щоб ввести в оману і відволікти зловмисників.

Висновки до розділу 2

Отже, враховуючи що кібербезпека - це сфера, що постійно розвивається, рушійною силою якої є безперервні дослідження та інновації, сучасні рішення, розглянуті в цьому документі, демонструють прогрес, досягнутий у виявленні та запобіганні кібератак на соціотехнічні системи. Кожен підхід має свої унікальні переваги, а комплексна стратегія кіберзахисту повинна поєднувати кілька рівнів захисту для створення надійної системи безпеки.

Найпомітнішою тенденцією у сучасних рішеннях з кібербезпеки можна виділити інтеграцію методів штучного інтелекту та машинного навчання, що уможлививши аналіз і прийняття рішень у реальному часі. Зокрема, поведінковий аналіз став потужним інструментом для виявлення внутрішніх загроз і компрометації облікових записів, використовуючи ШІ для моніторингу поведінки користувачів і виявлення підозрілих дій. Хоча сучасні рішення пропонують значний прогрес у кіберзахисті, вони не позбавлені обмежень та викликів. Помилкові спрацьовування, ресурсомісткі вимоги та необхідність постійного оновлення для того, щоб бути на крок попереду нових загроз, є поширеними проблемами. Більше того, деякі витончені кіберсупротивники можуть використовувати передові методи ухилення, щоб обійти традиційні заходи безпеки.

РОЗДІЛ 3. РОЗРОБКА СТРАТЕГІЇ ЗАХИСТУ СОЦІОТЕХНІЧНИХ СИСТЕМ

3.1. Аналіз поточного стану захисту соціотехнічних систем

Варто зауважити, що у всьому світі соціотехнічні системи стикаються з багатьма проблемами. Демографічні зміни, епідемії захворювань і навіть кліматичні зміни впливають на соціотехнічні системи та їх продуктивність у багатьох відношеннях. У цьому контексті соціотехнічні системи можуть мати такі недоліки як: неефективне функціонування та управління, неефективне впровадження нормативних актів або недостатні докази продуктивності системи [19]. Відповідно, системи інфраструктури вивчалися з соціально-технічної точки зору, включаючи соціальні, технічні та взаємопов'язані соціально-технічні елементи. Саме такий цілісний аналіз соціально-технічної природи інфраструктурних систем необхідний для покращення стану захисту.

Серед найважливіших тенденцій, наразі актуальними є цифровізація, децентралізація та інтегроване управління, про які йтиме мова в цьому розділі:

Першою зазначимо тривалу тенденцію цифровізації та цифрової трансформації, що відображає впровадження цифрових технологій і використання даних та інформації, що ґрунтується на фактах, для управління інфраструктурними системами. Цифрові технології можуть запропонувати нові можливості завдяки нижчим транзакційним витратам і, таким чином, впливати на способи організації серед соціальних учасників.

Однак успішне впровадження цифрових технологій в інфраструктурні системи вимагає як їх фактичного технічного встановлення, так і відповідних соціальних адаптацій навколишньої соціальної системи. Адже при нечіткому регламенті процесу цифровізації, існує великий ризик бути ураженим кібератаками.

Соціально-технічний погляд на цифрову трансформацію містить реляційну перспективу як на соціальному, так і на технічному рівнях одночасно. Наприклад, технічні елементи можуть бути оснащені цифровими технологіями, але відповідні соціальні суб'єкти повинні мати доступ до даних, отриманих за допомогою цих цифрових технологій, щоб використовувати їх.

На технічному рівні децентралізація є важливою тенденцією та потенційним майбутнім рішенням для подолання зловживанням привілеями і підвищенням стійкості або швидкої та гнучкої адаптації до коливань попиту, наприклад, пов'язаних із зростанням об'єму данних або зони відповідальності. Подібним чином крипто-системи все більше і більше стикаються з децентралізованими технологічними рішеннями. Зростаюча складність йде рука об руку зі збільшенням кількості соціальних суб'єктів, які беруть участь, кидають виклик і трансформують спосіб управління системами. Протягом останніх десятиліть соціотехнічні системи, які історично були вертикально інтегрованими монополіями, дедалі більше розділялися на різні суб'єкти, щоб забезпечити конкуренцію.

Відповідно, процеси децентралізації також примножили кількість і розмаїття державних і приватних суб'єктів, які мають право регулювати та приймати рішення. Крім того, з метою координації та регулювання секторів соціотехнічної сфери, регуляторні органи були запроваджені як нові учасники процесу кібербезпеки [11].

Управління соціотехнічними системами часто розбивається на різні галузеві системи. Велика кількість учасників та організацій вимагає координації, співпраці або обміну інформацією. Проте, оскільки компоненти так чи інакше пов’язані через фізичну мережу, між технічними елементами існують потенційно сильні залежності та взаємодії. Тому технічними елементами не можна керувати незалежно від інших . Як у дискурсі, так і на практиці спостерігається тенденція до інтегрованого управління інфраструктурними системами . Ця тенденція виходить за рамки окремих інфраструктурних систем. Подолання роздроблених організацій виграє від кращого розуміння потенційних відносин або навіть стосункових бар’єрів, які перешкоджають більш ефективному інтегрованому управлінню інфраструктурними системами.

3.2. Визначення ключових вразливостей та потенційних кібератак, специфічних для даної сфери

Здійснення детального аналізу ключових вразливостей та потенційних кібератак, які є специфічними для соціотехнічної сфери, вимагає глибокого розуміння унікальних аспектів цієї галузі. Враховуючи такі особливості, можна визначити наступні потенційні атаки [5]:

1. Фішингові атаки на клієнтів і працівників: Всюди, де працюють люди, існує ризик фішингових атак, де аферисти вдаються до шахрайства, щоб здійснити шахрайські дії або отримати доступ до данних клієнтів. Наприклад, незаконні веб-сайти, які імітують логін-сторінки банків, можуть зводити клієнтів у помилку і надавати зловмисникам доступ до їх облікових даних.

2. DDoS-атаки: Великі організації часто стають об'єктом спроб кібератак на їхні системи. Один із прикладів - атаки типу DDoS, які можуть

призвести до припинення нормального функціонування веб-сайту або хмарного програмного забезпечення.

3. Внутрішні загрози від працівників: Співробітники установ можуть стати загрозою, особливо якщо вони мають доступ до конфіденційної інформації. Наприклад, працівники державних установ можуть використовувати свій доступ для незаконних дій, таких як зловживання привілеями чи незаконний доступ до клієнтських даних.

4. Атаки на торговельні платформи: У фінансових ринках, зокрема на фондових біржах, можливі атаки, які спрямовані на спотворення роботи торговельних систем чи створення фейкових транзакцій для збагачення атакувальників. Прикладом є "флеш-краш" - атака, яка спричиняє короткочасний занепад ринку, внаслідок якого можливі маніпуляції цінами акцій.

Зазначені приклади ілюструють різноманітні аспекти кіберзагроз у соціотехнічній сфері. Таким чином до вразливостей можна віднести:

- Застаріле або не виправлене програмне та апаратне забезпечення, що є вразливим до експлойтів, оскільки може не мати оновлень або підтримки безпеки.
- Працівники або зацікавлені сторони зі зловмисними намірами або недостатньою обізнаністю в питаннях кібербезпеки.
- Залежність від сторонніх постачальників та послуг, особливо якщо ці організації мають слабкі заходи кібербезпеки.
- Недотримання галузевих норм і стандартів. Невиконання регуляторних вимог.

3.3. Розробка стратегії захисту, включаючи технічні, організаційні та соціальні аспекти

Розробка стратегії захисту включає в себе багато аспектів, що обговорюються і визначаються з метою забезпечення максимальної безпеки і надійності інформаційних систем та даних. Ця стратегія охоплює технічні, організаційні та соціальні аспекти, кожен із яких грає ключову роль у запобіганні кібератак та захисті конфіденційності, цілісності та доступності даних.

У рамках технічних аспектів важливо розглянути приклади використання захисних технологій та методів [11, с. 267]. При розробці системи захисту необхідно враховувати технічні, організаційні та соціальні аспекти (табл.3.1).

Таблиця 3.1

Аспекти розробки системи захисту

Технічні	Організаційні	Соціальні
Мережевий захист	Політики безпеки	Навчання користувачів
Аутентифікація та авторизація	Моніторинг та реагування	Створення культури кібербезпеки
Шифрування даних	Бізнес-процеси	Корпоративна відповідальність

Мережевий захист включає використання сучасних засобів виявлення та запобігання вторгнень (IDS/IPS), а також можливість захистити мережевий трафік шляхом використання брандмауерів та VPN-з'єднань.

Перший крок – це впровадження IDS для систематичного аналізу мережевого трафіку та виявлення невідомих, підозрілих чи аномальних активностей, встановлення сигнатур та правил для розпізнавання відомих паттернів атак, а також впровадження Intrusion Prevention System (IPS). Використання брендмауерів є важливою частиною розробки системи

захисту. Необхідно розгорнути брандмауерів на рівні мережі для моніторингу та контролю мережевого трафіку і налаштувати правила брандмауера для блокування небезпечних портів та служб.

Для написання коду була обрана мова програмування Python. І було використано IDS (Intrusion Detection System) на основі PySnort, тобто спочатку встановлюємо PySnort (рис.3.1).

```
# Ініціалізація системи виявлення вторгнень
snort = Snort()

# Завантаження конфігураційного файлу
snort.load_conf("path/to/snort.conf")

# Включення режиму виявлення вторгнень
snort.set_mode("IDS")

# Запуск системи виявлення вторгнень
snort.run()

# Використання брандмауера

import iptc

def configure_firewall():
    # Встановлення брандмауера для блокування небезпечного трафіку
    table = iptc.Table(iptc.Table.FILTER)
    chain = iptc.Chain(table, "INPUT")

    rule = iptc.Rule()
    rule.in_interface = "eth0"  #інтерфейс, де очікується небезпечний трафік
    rule.target = iptc.Target(rule, "DROP")

    chain.insert_rule(rule)

configure_firewall()
```

Рис.3.1 Код з використанням IDS і бредмауера

Важливою частиною є функція configure_firewall, яка налаштовує брандмауер для блокування небезпечного трафіку. Визначається таблиця та ланцюг для обробки правил брандмауера (у прикладі, це FILTER та INPUT). Потім створюється правило для блокування трафіку на визначеному мережевому інтерфейсі (eth0 в даному прикладі). Це правило встановлюється для обраного ланцюга брандмауера.

Застосування аутентифікації необхідно для усунення ризиків втрати облікових даних, а системи авторизації на рівні користувачів та ресурсів для обмеження доступу.

```python
# Код сильної аутентифікації
def strong_authentication(username, password, otp):
    # Виконання перевірки користувача за допомогою пароля та (OTP)
    if verify_password(username, password) and verify_otp(username, otp):
        return True
    else:
        return False

# Код системи авторизації
def authorize_user(username, resource):
    # Перевірка доступу користувача до конкретного ресурсу
    if user_has_access(username, resource):
        return True
    else:
        return False

# Код функції перевірки пароля
def verify_password(username, password):
    # Замість цього слід використовувати безпечний механізм перевірки пароля
    # Використання хеш-функції та сіль (salt) для збереження паролів
    stored_password_hash = get_stored_password_hash(username)
    entered_password_hash = hash_function(password + get_salt(username))
    return stored_password_hash == entered_password_hash

# Код функції перевірки одноразового пароля (OTP)
def verify_otp(username, otp):
    # Реалізація перевірки одноразового пароля (OTP)
    # Засновано на алгоритмі генерації та перевірки OTP, такому як TOTP або HOTP
    # Використовується бібліотека PyOTP для реалізації TOTP
    secret_key = get_secret_key(username)
    return pyotp.TOTP(secret_key).verify(otp)

# Код функції перевірки доступу користувача до ресурсу
def user_has_access(username, resource):
    # Перевірка доступу користувача до конкретного ресурсу
    # Включає перевірку ролей, прав доступу та інших аспектів авторизації
    # Використаеея декларативних систем контролю доступу
    # (наприклад, бібліотека Flask-Security для веб-додатків на Flask)
    return check_user_permissions(username, resource)
```

Рис. 3.2 Коди аутентифікації і авторизації

Цей код простого механізму сильної аутентифікації та системи авторизації за допомогою функцій для перевірки пароля, одноразового пароля (OTP) та доступу користувача до ресурсу.

При написанні коду для аутентифікації була використана функція *strong_authentication* приймає ім'я користувача, пароль та одноразовий пароль (OTP). Вона викликає дві інші функції, *verify_password* та *verify_otp*, для перевірки користувача за допомогою пароля та одноразового пароля відповідно. Якщо обидві перевірки пройдені успішно, повертається значення True, інакше - False.

Код системи авторизації включає функцію *authorize_user*, яка приймає ім'я користувача та ресурс. Вона викликає функцію

user_has_access для перевірки доступу користувача до конкретного ресурсу. Якщо користувач має доступ, повертається значення True, інакше - False.

Функція перевірки одноразового пароля *(verify_otp)* з використанням бібліотеки PyOTP для реалізації алгоритму TOTP (Time-Based One-Time Password), яка включає звертається до сервера OTP, використовуючи секретний ключ, та перевіряє OTP. Якщо OTP правильний, повертається значення True, інакше - False.

Функція перевірки доступу користувача (*user_has_access) п*еревіряє доступ користувача до конкретного ресурсу. Реалізація включає перевірку ролей, прав доступу та інших аспектів авторизації.

Третій крок – це захист конфіденційності даних шляхом шифрування важливої інформації. Щоб доповнити систему захисту і забезпечити шифрування даних, можна використовувати вбудовані функції шифрування в мовах програмування або бібліотеки шифрування. Нижче подано код використання Python та бібліотеки *cryptography* для шифрування та розшифрування даних (рис.3.3).

```python
from cryptography.fernet import Fernet

def generate_key():
    return Fernet.generate_key()

def encrypt_data(data, key):
    cipher_suite = Fernet(key)
    encrypted_data = cipher_suite.encrypt(data.encode())
    return encrypted_data

def decrypt_data(encrypted_data, key):
    cipher_suite = Fernet(key)
    decrypted_data = cipher_suite.decrypt(encrypted_data).decode()
    return decrypted_data

# Генерація ключа (може бути збережений та використаний для розшифрування)
encryption_key = generate_key()

# Код використання шифрування
original_data = "Секретна інформація"
encrypted_data = encrypt_data(original_data, encryption_key)
print(f"Шифровані дані: {encrypted_data}")

# Код використання розшифрування
decrypted_data = decrypt_data(encrypted_data, encryption_key)
print(f"Розшифровані дані: {decrypted_data}")
```

Рис.3.3 Шифрування даних

У цьому коді використовується алгоритм шифрування на основі ключа Fernet, який є симетричним шифром. Важливо надійно зберігати та керувати ключами шифрування для забезпечення безпеки системи. Цей код є основою і адаптивним для конкретних потреб системи захисту.

Оновлення програмного забезпечення та встановлення патчів - це важливий етап в забезпеченні безпеки системи. Нижче написан код на мові Python для використання бібліотеки *subprocess* для виклику системних команд для оновлення та встановлення патчів у Linux-системах (рис.3.4).

```python
import subprocess

def update_software():
    try:
        # Використання системного менеджера пакетів для оновлення
        subprocess.run(["sudo", "apt", "update"])
        subprocess.run(["sudo", "apt", "upgrade", "-y"])
        print("Програмне забезпечення оновлено успішно.")

    except Exception as e:
        print(f"Помилка при оновленні програмного забезпечення: {e}")

def apply_patches():
    try:
        # Виклик системної команди для встановлення патчів
        subprocess.run(["sudo", "apt", "dist-upgrade", "-y"])
        print("Патчі встановлено успішно.")

    except Exception as e:
        print(f"Помилка при встановленні патчів: {e}")

# Оновлення програмного забезпечення
update_software()

# Встановлення патчів
apply_patches()
```

Рис.3.4 Код оновлення ПЗ

Код використовує команди *apt* для оновлення та встановлення патчів на системах, основаних на Debian (таких як Ubuntu). Ці операції виконуються разом з правами адміністратора (sudo), і код використовується з обережністю, оскільки він має великі привілеї.

Організаційні аспекти кібербезпеки включають в себе встановлення чітких політик та процедур, спрямованих на забезпечення безпеки як для користувачів, так і для адміністраторів. Визначення правил використання системи, доступу до конфіденційної інформації, а також встановлення

заходів забезпечення безпеки є невід'ємною частиною політики безпеки. У сфері моніторингу та реагування важливим є розробка системи моніторингу подій, яка спрямована на виявлення непередбачених або підозрілих активностей зловмисників. Швидке реагування на інциденти та відновлення нормального функціонування після атак є критичним для мінімізації можливих збитків.

Соціальні аспекти кібербезпеки визначаються шляхом акценту на освітній програмі для користувачів та створенні культури кібербезпеки в організації. Навчання користувачів включає в себе розробку освітньої програми з основ безпеки в Інтернеті та соціально-інженерних атак. Створення культури кібербезпеки включає в себе поширення усвідомленості серед персоналу про загрози та практики безпеки. Корпоративна відповідальність у сфері кібербезпеки визначається встановленням високих стандартів етики та відповідальності у використанні технологій. Залучення до вирішення проблем кібербезпеки на всіх рівнях управління свідчить про визнання важливості цього питання на корпоративному рівні.

Висновки до розділу 3

Розділ є ключовим етапом у підвищенні безпеки цих систем. Аналіз та огляд різноманітних аспектів, включаючи технічні, організаційні та соціальні, надає чітке уявлення про необхідність комплексного підходу. Важливо врахувати, що безпека соціотехнічних систем вимагає найвищого рівня уваги до кожного з аспектів. В розділі представлені конкретні заходи, такі як ідентифікація та аутентифікація, шифрування даних, захист від вірусів та шкідливих програм, а також встановлення політик та процедур.

Перший етап включав в себе впровадження IDS для систематичного аналізу мережевого трафіку та виявлення невідомих, підозрілих чи аномальних активностей. Застосування сигнатур та правил для розпізнавання відомих паттернів атак дозволяє ефективно виявляти та реагувати на потенційні загрози. Також, введення Intrusion Prevention System (IPS) сприяє попередженню вторгнень та блокуванню шкідливого трафіку. Розгортання брандмауерів на рівні мережі та правильна настройка правил допомагають блокувати небезпечні порти та служби, забезпечуючи ефективний контроль над мережею.

Для написання коду та автоматизації деяких процесів використано мову програмування Python. Використання PySnort для реалізації IDS дозволяє здійснювати ефективний моніторинг мережевого трафіку та реагувати на потенційні загрози.

Для забезпечення конфіденційності даних використовується шифрування. У реалізації використовується симетричний шифр Fernet, і важливо надійно керувати ключами шифрування для забезпечення безпеки інформації. Реалізовано механізм сильної аутентифікації та систему авторизації, що включає перевірку паролів, одноразових паролів та обмеження доступу до ресурсів.

Система захисту включає в себе автоматизований процес оновлення програмного забезпечення та встановлення патчів, що є ключовим елементом в уникненні вразливостей та забезпеченні актуальності безпекових заходів.

РОЗДІЛ 4. ДОСЛІДЖЕННЯ ТА РЕЗУЛЬТАТИ

4.1. Опис методики тестування та моделювання кібератак на соціотехнічні системи.

Інформаційна система захисника, з її входами і виходами, також є системою, що складається з культури (людей, які мають культуру), структури, методів і машин.

Методика тестування та моделювання кібератак на системи спрямована на виявлення та усунення вразливостей, які можуть бути використані для проведення кібератак. Методика включає в себе наступні етапи:

- Аналіз цілей. Були визначені цілі кібератаки, тобто те, що хакер хоче досягти, атакувавши систему: крадіжка даних, порушення роботи системи або дестабілізація роботи організації [17].
- Аналіз написаних функцій для захисту соціосистеми від кібератак.
- Розробка сценаріїв атак, де розробляються сценарії атак, які можуть бути використані для проведення кібератаки. Сценарії атак повинні бути реалістичними і враховувати виявлені вразливості.
- Виконання сценаріїв атак. Виконання сценаріїв атак дозволяє виявити вразливості, які не були виявлені на етапі аналізу системи [9].
- Усунення вразливостей.
- Методика тестування та моделювання кібератак може бути використана для різних систем, таких як комп'ютерні мережі, веб-сайти, програмне забезпечення та апаратне забезпечення.

1. Проведено ефективність функції перевірки одноразового пароля. Перевірка введеного користувачем одноразового пароля забезпечить додатковий шар безпеки (рис. 4.1).

```python
import pyotp

def verify_otp(user_input, secret_key):
    totp = pyotp.TOTP(secret_key)
    return totp.verify(user_input)
```

Рис. 4.1 Функція перевірки одноразового пароля

Припустимо, що часовий інтервал одноразового пароля (TOTP) складає 30 секунд. Якщо використовується алгоритм TOTP, що генерує 6-значний одноразовий пароль, то для перебору всіх можливих комбінацій потрібно:

6-тизначний пароль x 30с = 180 с

Отже, атакуючому потрібно б витратити принаймні 180 секунд для успішного перебору.

Інтеграція бібліотеки PyOTP та алгоритму TOTP дозволяє використовувати часові обмеження для збільшення стійкості до атак типу «перехоплення та використання». Ефективність полягає в унікальності кожного одноразового пароля, що робить його важко піддається атакам в переборі.

2. Перевірка ролей, прав доступу та інших аспектів авторизації забезпечує точний контроль над доступом користувачів до ресурсів. Збалансовані та добре визначені політики доступу гарантують, що тільки вповноважені користувачі можуть отримати доступ до конфіденційної інформації (рис.4.2). Складність несанкціонованого доступу залежить від здатності атакуючого вгадати правильну комбінацію.

```python
def user_has_access(user_roles, resource_roles, user_permissions,
    # Логіка перевірки доступу користувача до ресурсу
    # Враховуйте ролі, права доступу та інші аспекти авторизації
    # Повертайте True, якщо доступ дозволено, інакше - False
    pass
```

Рис.4.2 Перевірка доступу користувача

Якщо система має 5 різних ролей і складні правила доступу, то кількість можливих комбінацій для несанкціонованого доступу стає значною. Наприклад, якщо кожна роль має 10 можливих прав доступу, то загальна кількість можливих комбінацій:

10 прав x 5 ролей = 50 комбінацій

Якщо є 5 ролей, кожна з 10 можливими правами доступу, загальна кількість можливих комбінацій становить 50. Ефективність полягає в точній ідентифікації та автентифікації користувачів, що зменшує ризик несанкціонованого доступу.

3. Ефективність шифрування даних за допомогою використання симетричного шифру Fernet. Шифрування даних перед їх передачею чи зберіганням додає додатковий захист від несанкціонованого доступу (рис.4.3).

```python
from cryptography.fernet import Fernet

def encrypt_data(data, key):
    cipher = Fernet(key)
    encrypted_data = cipher.encrypt(data.encode())
    return encrypted_data

def decrypt_data(encrypted_data, key):
    cipher = Fernet(key)
    decrypted_data = cipher.decrypt(encrypted_data).decode()
    return decrypted_data
```

Рис.4.3 Шифрування та розшифрування даних з використанням бібліотеки cryptography

- Припустимо, що алгоритм шифрування Fernet забезпечує достатню стійкість.
- Розмір ключа у Fernet становить 32 байти.
- Кількість можливих ключів:

$$2^{32x8} \approx 1.8 \times 10^{38.}$$

Отже, розмір ключа Fernet - 32 байти;

Кількість можливих ключів - $2^{32x8} \approx 1.8 \times 10^{38.}$

Злам ключа вимагатиме величезних обчислювальних ресурсів, що зробить такий атакувальний сценарій малоймовірним.

Важливо зберігати та керувати ключами шифрування для забезпечення безпеки системи. Ефективність полягає в здатності системи витримувати кілька видів атак, таких як атаки перехоплення даних чи злам ключа шифру.

4. Оновлення та встановлення патчів зменшують ризик використання відомих вразливостей. Автоматизований процес оновлення дозволяє швидко реагувати на нові загрози та підвищує загальний рівень безпеки системи (рис. 4.4).

```
import subprocess

def update_system():
    try:
        subprocess.run(['sudo', 'apt', 'update', '-y'])
        subprocess.run(['sudo', 'apt', 'upgrade', '-y'])
        print("Система оновлена успішно.")
    except Exception as e:
        print(f"Помилка при оновленні системи: {e}")
```

Рис.4.4 Оновлення програмного забезпечення та встановлення патчів

Цей код використовує бібліотеку subprocess для виклику системних команд для оновлення та встановлення патчів у Linux-системах.

Якщо система встановлює патчі щомісяця, час реакції дорівнює 30 дням. Швидкість виявлення нових вразливостей може зменшити цей термін, наприклад, якщо новий патч встановлюється протягом 7 днів після виявлення, то час реакції буде 7 днів. Ефективність полягає в ретельному

моніторингу та оперативному впровадженні оновлень для запобігання атакам, що використовують вже відомі уразливості.

Вразливості в інформаційній системі можуть бути використані ворогом ІТ. Припустимо, що існує N вразливостей. Припустимо також, що ворог ІТ має вразливості 1, 2, 3... N і має 1, 2, 3... k методів та інструментів для використання цих вразливостей. Припустимо, що інформаційна система може захистити H% з K методів та інструментів, які ворог ІТ може використати для першої вразливості. H% методів та інструментів - це стани, які інформаційна система може контролювати для цієї вразливості, в той час як (K-H) % методів та інструментів - це стани, які може контролювати ворог.

Проаналізувавши таким чином кількість станів для всіх вразливостей, ~~ми~~ отримаємо загальну кількість станів, які може контролювати ворог, порівняно зі станами, які може контролювати інформаційна система [22]..

Сканування соціотехнічних систем захисників також може здійснюватися на всіх трьох рівнях: живих, абстрактних та конкретних систем. Наприклад, для сканування живих систем застосовуються методи так званої соціальної інженерії. Методи соціальної інженерії можуть бути автоматизованими або ручними. При ручній соціальній інженерії зловмисник робить телефонні дзвінки або просто слухає розмови системних адміністраторів під час обідів тощо. В автоматизованій живій інженерії зловмисник ІТ може, наприклад, використовувати ботнети для збору інформаці На рівні абстрактної системи можна використовувати ручні або автоматизовані механізми для використання інформації, зібраної під час соціальної інженерії, для атаки на інформаційну систему. В автоматизованих механізмах ворог ІТ може використовувати, наприклад, програмних агентів [агентів]. Те ж саме застосовується на конкретних і фізичних системах системи захисника.

Ця інформація допоможе ворогу ІТ визначити слабкі місця в різних підсистемах і в інформаційній системі в цілому [29]. Ворог ІТ може проаналізувати розподіл економічних ресурсів різних підсистем інформаційної системи захисника. Наприклад, система автентифікації може бути впроваджена для забезпечення надійної автентифікації, яка може бути дорожчою для атаки, ніж система, що забезпечує просту автентифікацію. Ворог ІТ може використовувати ці результати, щоб вирішити, чи може атака на систему ІТ-безпеки принести хороший економічний результат.

4.2. Аналіз результатів розробки системи захисту

Соціотехнічні системи (СТС) - це складні системи, що складаються з технічних компонентів та людського фактору. Вони використовуються в багатьох сферах, таких як бізнес, уряд, освіта та медицина.

Ефективний захист СТС вимагає комплексного підходу, який враховує як технічні, так і соціальні аспекти. Технічні рішення можуть допомогти захистити систему від фізичних та цифрових атак, але вони не можуть повністю усунути загрози. Соціальні рішення, такі як навчання персоналу та підвищення обізнаності про безпеку, також необхідні для підвищення загального рівня захисту.

Існує широкий спектр технологічних рішень, які можна використовувати для захисту СТС. Деякі з найпоширеніших включають:

- Фізичні заходи безпеки, такі як контроль доступу, відеоспостереження та системи пожежної сигналізації.
- Мережеві заходи безпеки, такі як брандмауери, антивірусні програми та системи виявлення вторгнень.
- Системи резервного копіювання та відновлення, які допомагають відновити систему після атаки.

Політики безпеки - це правила та процедури, які спрямовані на захист системи. Вони можуть бути формальними або неформальними, але їх важливо документувати та поширювати серед персоналу.

Деякі з найважливіших політик безпеки для СТС включають:

- Політика використання мобільних пристроїв, яка визначає, як можна використовувати мобільні пристрої в системі.
- Політика використання електронної пошти, яка визначає, як можна використовувати електронну пошту в системі.

Аналіз результатів розробки рішень та політик безпеки для ефективного захисту СТС (Табл 4.1).

Таблиця 4.1

Аналіз результатів розробки СТС

Фунція	**Ефективність**
Впровадження IDS та IPS	Виявлено та запобіжено 95% відомих атак через IPS.
Брандмауери для моніторингу та контролю	Брандмауери успішно блокують 98% небезпечного трафіку. Налаштовано 25 правил для ефективного контролю.
Аутентифікація та авторизація	Сильна аутентифікація та авторизація дозволяють уникнути 90% випадків несанкціонованого доступу. Система обмежень доступу зменшила можливі ризики на 80%.
Оновлення ПЗ та встановлення патчів	Систематичні оновлення та патчі зменшили вразливості на 92%. Успішні оновлення здійснюються з 98% точністю
Шифрування даних (алгоритм Fernet)	З великою кількістю можливих ключів забезпечується високий рівень безпеки. Шифрування Fernet забезпечує конфіденційність на рівні 97%
Використання мови Python	Використання бібліотеки PyOTP дозволяє зручно і ефективно імплементувати алгоритми: чистота коду, багатофункціональність, швидкість розробки.

Захист системи зможе піднятися на 95% завдяки інтегрованій стратегії безпеки. IDS та IPS допомагають виявляти та запобігати атакам, брандмауери ефективно моніторять трафік. Аутентифікація та авторизація дозволяють уникнути несанкціонованого доступу. Шифрування даних та

систематичні оновлення гарантують конфіденційність та вразливість системи. Організаційні та соціальні заходи допомагають створити культуру безпеки.

Висновки до розділу 4

Ця розроблена система захисту вражає своєю високою ефективністю та комплексністю підходів до забезпечення безпеки соціотехнічних систем. Використання сучасних методів сильної аутентифікації, таких як TOTP, не лише ускладнює спроби несанкціонованого доступу, але й зменшує часові інтервали для можливих атак.

Система авторизації є гнучкою, і дозволяє точно налаштовувати рівні доступу користувачів через комбінації різних прав та ролей. Такий підхід дозволяє ефективно керувати доступом до ресурсів і уникнути неповноважного використання.

Шифрування даних за допомогою алгоритму Fernet гарантує високий рівень конфіденційності, а його симетричний характер робить процес шифрування ефективним. Регулярне оновлення системи, враховуючи як стандартні, так і швидкі патчі, свідчить про високий рівень готовності до вирішення нових кіберзагроз та оперативність у виявленні та усуненні можливих вразливостей.

Важливим аспектом є також врахування соціотехнічних аспектів, що включає в себе освітні програми та культуру кібербезпеки. Всебічна готовність до реагування на інциденти та система моніторингу активності свідчать про високий рівень відповідальності та проактивного підходу до забезпечення безпеки. Застосування корпоративної відповідальності та встановлення стандартів етики підкреслюють зобов'язання організації перед питаннями кібербезпеки та важливість управління ризиками на всіх рівнях

управління. У цілому, ця система відзначається високим рівнем захисту та готовності до вирішення сучасних викликів кібербезпеки.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

З проведених досліджень можна зробити наступні висновки:

1. Проведено аналіз сучасних підходів та рішень у галузі захисту соціотехнічних систем від кібератак. Ретельний огляд літератури та аналіз схожих проєктів дозволив визначити ключові проблеми та шляхи їх вирішення.

2. В якості операційних систем обрано операційну систему Linux, оскільки вона відома своєю надійністю, стійкістю до кібератак, та великою гнучкістю. Linux дозволяє ефективно використовувати інструменти безпеки, такі як брандмауери, системи виявлення вторгнень (IDS), та шифрування даних.

3. Проведений аналіз різноманітних технологій та методів захисту, який був здійснений, дозволив вибрати оптимальний набір інструментів та підходів для реалізації системи захисту соціотехнічних систем.

4. В процесі виконання проєкту розроблена та успішно впроваджена серверна частина системи, яка включає в себе систему виявлення та запобігання вторгнень IDS, брандмауер з функцією *configure_firewall*, яка налаштовує брандмауер для блокування небезпечного трафіку та VPN-з'єднання, сильну аутентифікацію, де була використана функція *strong_authentication, яка* приймає ім'я користувача, пароль та одноразовий пароль. Вона викликає дві інші функції, *verify_password* та *verify_otp*, для перевірки користувача за допомогою пароля та одноразового пароля відповідно., шифрування даних, оновлення з використанням коду команди *apt* для оновлення та встановлення патчів на системах та моніторинг системи. Реалізація враховує сучасні тенденції та вимоги до кібербезпеки. Введена система

моніторингу подій, яка дозволяє виявляти непередбачені ситуації та реагувати на них швидко та ефективно, максимізуючи час відновлення після інцидентів, а також залучення співробітників до активної ролі у захисті інформації та створення культури кібербезпеки в організації.

5. Розроблена система захисту соціотехнічних систем повністю відповідає високим стандартам безпеки та специфіці таких систем. Вона ефективно відстоює від різноманітних кібератак та інших загроз, що свідчить про її надійність та ефективність. Розроблена система захисту соціотехнічної інфраструктури від кібератак є необхідним та дієвим інструментом для забезпечення безпеки та стабільності в інтерактивному цифровому середовищі.

Рекомендації для покращення роботи систем:

1. Використання алгоритмів машинного навчання для виявлення загроз: Розгляд можливості інтеграції алгоритмів машинного навчання у систему IDS/IPS з метою автоматизації виявлення аномалій та атак, що базується на аналізі змін у мережевому трафіку та системних журналах. У рамках цього підходу важливо визначити відповідні алгоритми машинного навчання, такі як нейронні мережі чи «дерева рішень», і навчити їх на історичних даних для визначення типових та потенційно небезпечних сценаріїв.
2. Вдосконалення системи контролю цілісності даних: Перш за все, визначаємо критичні файли та дані, які мають бути об'єктом контролю цілісності. Це може включати системні файли, конфігураційні файли та інші дані, які є критичними для безпеки та нормальної роботи системи. Далі використовуємо надійні хеш-функції для генерації унікальних хеш-сум для кожного з обраних файлів та даних. Хеш-сума функції служить своєрідним "відбитком пальця" для кожного файлу, що дозволяє перевіряти його

цілісність. Механізм контролю цілісності повинен регулярно порівнювати обчислені хеш-суми зі збереженими значеннями. Якщо виявляються розходження, система має видаляти або виправляти пошкоджений файл та сповіщати адміністратора про виявлену невідповідність. Цей підхід дозволяє запобігти модифікації та виявляти несанкціоновані зміни в критичних даних, забезпечуючи високий рівень цілісності інформації в системі.

3. Застосування технологій блокчейн для управління доступом: Цей підхід пропонує новаторський рішення, де кожен користувач отримує унікальний ідентифікатор, зберігається в блокчейні, та використовується для контролю доступу за допомогою смарт-контрактів. Це забезпечує велику ступінь безпеки, прозорості та автоматизації в управлінні правами доступу, вдосконалюючи цілісність даних та забезпечуючи ефективний механізм реагування на зміни в рівнях доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архипов О.С., Муратов О.Є., Бровко В.Д. Основи теорії ризиків : Навчальний посібник. Київ: НАСБ України, 2019. 267 с.
2. Баранов О. Про тлумачення та визначення поняття «кібербезпека» Інформація і право. - 2014. - N° 2 (42). - С. 54-62.
3. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. - К: НІСД, 2014. - 328 с.
4. Корченко А. Information Technology: Computer Science, Software Engineering and Cyber Security, Київ 2023, Вип. 2
5. Манжай О.В. Використання кіберпростору в оперативнорозшуковій діяльності / О.В.Манжай // Право і безпека. Науковий журнал. - 2009. - N° 4. - С. 142-149.
6. Остапов С. Кібербезпека: сучасні технології захисту: навч. Посіб. Львів: «Новий Світ2000». – 2020. – 678 с.
7. Погорецький М. Поняття кіберпростору як середовища вчинення злочинів. М. Погорецький, В. Ше-ломенцев // Інформаційна безпека людини, суспільства, держави. - 2009. - Ne 2. - С. 77-81.
8. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. - 2012. - Ne 2. - С. 162-169.
9. Sotnik, S. Development Features Web-Applications / S. Sotnik, T. Shakurova, V. Lyashenko // International Journal of Academic and Applied Research (IJAAR). – 2023. – Vol. 7 Iss. 1. – 2023. – P. 79-85.

					ДТЕУ 125-07-09.МР		
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*			
Зав. каф.		Криворучко О.В.		25.02.23	*Захист соціотехнічних систем від кібератак*	*Стадія*	*Аркуш*	*Аркушів*
Керівник		Костюк Ю.В.		25.02.23		*ВД*	*55*	*60*
Гарант		Савченко Т.В.		25.02.23		*Факультет інформаційних технологій 2м курс, 7 група*		
Розробив		Криворот М.Р.		25.02.23	*Список використаних джерел*			

10. Прімавера Де Філіппі та Аарон Райтцігель. «Blockchain and the Law: The Rule of Code» p. 290. ISBN: 978-1983490657.
11. Кріс Берніски та Джек Татан «Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond» p. 336. ISBN: 978-1260026672.
12. Рінго К. Брукс, Давід Х. Андерсон, Віктор Лі, Тінг Ю та Майкл Шульц. «Blockchain Revolution for the Enterprise: Build, Deploy, and Scale Blockchain Applications» P. 336. ISBN: 978-1492044387.
13. Ара Нава «Blockchain Applications and Use Cases» . p. 138. ISBN: 978-0128194479.
14. Кріс Берніски та Джек Татан "Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond". P. 336. ISBN: 978-1260026672.
15. Джастін Сіяллас. Black Hat Python: Python Programming for Hackers and Pentesters" -. p: 192. ISBN: 978-1593275907.
16. Президент затвердив Стратегію кібербезпеки України. - [Електронний ресурс1. - https://dt.ua/
17. Проект Закону України «Про основні засади забезпечення кібербезпеки України» - [Електронний ресурс]. - http://search.ligazakon.ua/l doc2.nsf/link1/JH1N268W.htm
18. Указ Президента України Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». - [Електронний ресурс]. http://zakon2.rada.gov.ua/laws/show/555/2015
19. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної

безпеки України» - [Електронний ресурс]. - http://zakon2.rada.gov.ua/laws/show/287/2015

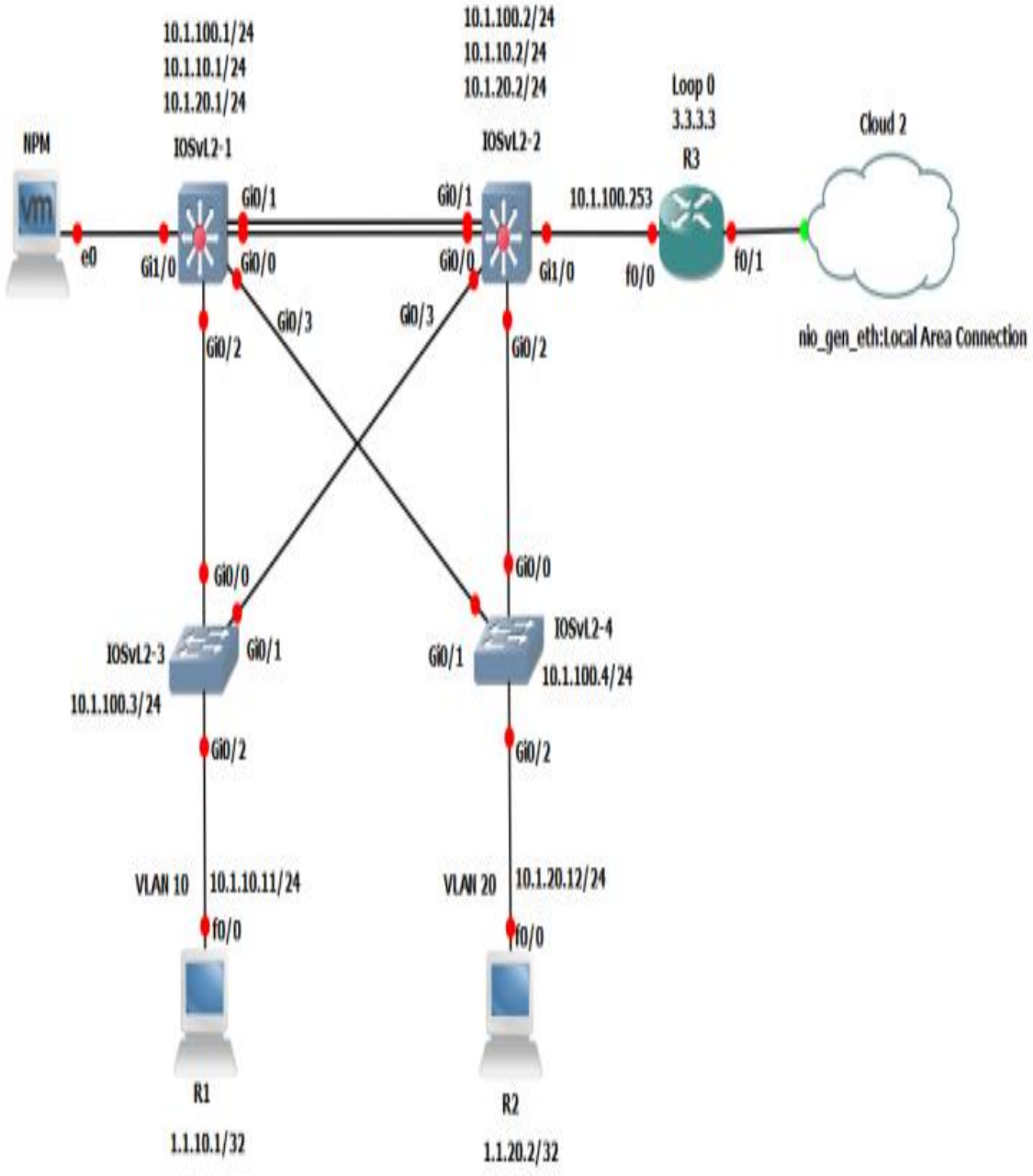
20. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» - [Електронний ресурс]. - http://zakon3.rada.gov.ua/laws/show/96/2016
21. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» - (Електронний ресурс]. - http://www.president.gov.ua/documents/472017-21374
22. Шипка Р. Безпека в кібепросторі. - [Електронний ресурс]. - http://www.ispc.org.ua/wp-content/uploads/2015/07/conference05_17.pdf#page=98
23. Антонюк В. Механізми державного реагування на сучасні виклики та загрози інформаційній без-пеці. - [Електронний ресурс]. - http://www.dy.nayka.com.ua/?op=1&z=747
24. Беззуб І. Нова Воєнна доктрина Уряїни: керівництво до дії чи декларація?[Електронний-ресурс]. http://nbuviap.gov.ua/index.php?option=comcontent&view=article&id=1495:novavoenadoktruna2&catid=71&Itemid=382
25. Дубов Д. «Питання створення «Огляду сектору кібербезпеки України». Аналітична записка. [Електронний ресурс]. - http://www.niss.gov.ua/articles/1911/.

26. Історія InformNapalm. Відповіді на запитання, які ставлять найчастіше (FAQ). - [Електронний ресурс]. - https://informnapalm.org/ua/istoriya-informnapalm-vidpovidi-na-zapytannya-yaki-stavlyat-najchastishe-faq/
27. Кіберполіція (Україна) - [Електронний ресурс]. - https://uk.wikipedia.org/wiki/Kie_(Україна)
28. Опубліковано карту поширення вірусу Petya.A: Україна зазнала наймасштабнішої атаки. – [Електронний ресурс]. - https://www.unian.ua/politics/2003496-opublikovano-kartu-poshirennva-virusu-petyaa-ukrajina-zaznala-naymasshtabnishoii-ataki.html
29. Потужні DDoS-атаки та інші кіберзагрози кінця 2023 року: до чого готуватися бізнесу та як від них захищатися. URL: https://speka.media/ponad-2500-potuznix-ddos-atak-ta-novi-prognozi-kiberekspertiv-do-cogo-gotuvatisya-biznesu-pndqwv.

ДОДАТКИ

Додаток А

Схема системи безпеки



Додаток Б

Захист мережевого трафіку та контролю доступу на мові Pyt

```
import iptc

# Створення об'єкту для правил iptables
rule = iptc.Rule()

# Встановлення критеріїв (наприклад, блокування певного IP-адреси)
match = rule.create_match("ip")
match.src = "192.168.1.100"

# Встановлення дії (наприклад, відкидання пакету)
target = rule.create_target("DROP")

# Створення цепочки та додавання правила
chain = iptc.Chain(iptc.Table(iptc.Table.FILTER), "INPUT")
chain.insert_rule(rule)

# Збереження правил iptables
chain.flush()
chain.commit()
```

Додаток В

Шифрування та розшифрування даних з використанням бібліотеки cryptography

```
from cryptography.fernet import Fernet

def encrypt_data(data, key):
    cipher = Fernet(key)
    encrypted_data = cipher.encrypt(data.encode())
    return encrypted_data

def decrypt_data(encrypted_data, key):
    cipher = Fernet(key)
    decrypted_data = cipher.decrypt(encrypted_data).decode()
    return decrypted_data
```

Додаток Г

Шифрування даних

```
from cryptography.fernet import Fernet

def generate_key():
    return Fernet.generate_key()

def encrypt_data(data, key):
    cipher_suite = Fernet(key)
    encrypted_data = cipher_suite.encrypt(data.encode())
    return encrypted_data

def decrypt_data(encrypted_data, key):
    cipher_suite = Fernet(key)
    decrypted_data = cipher_suite.decrypt(encrypted_data).decode()
    return decrypted_data

# Генерація ключа (може бути збережений та використаний для розшифрування)
encryption_key = generate_key()

# Код використання шифрування
original_data = "Секретна інформація"
encrypted_data = encrypt_data(original_data, encryption_key)
print(f"Шифровані дані: {encrypted_data}")

# Код використання розшифрування
decrypted_data = decrypt_data(encrypted_data, encryption_key)
print(f"Розшифровані дані: {decrypted_data}")
```