МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У ГАЛУЗІ МОБІЛЬНИХ ДОДАТКІВ ТА ІОТ-ПРИСТРОЇВ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Сергій ЛОЗОВСЬКИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Сергій ЛОЗОВСЬКИЙ
(Ім’я, ПРІЗВИЩЕ)

Керівник:
к.т.н., доцент Юрій ЩАВІНСЬКИЙ
(Ім’я, ПРІЗВИЩЕ)

Рецензент: _____
(Ім’я, ПРІЗВИЩЕ)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лозовському Сергію Дмитровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Розробка системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв ”,

керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н., доцент,
(ІПРІЗВИЩЕ, Ім'я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “27“ *лютого 2024* р. № *36*.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.*

4. Перелік питань, які мають бути розроблені:
   4.1. Ознайомлення з актуальними методиками та інструментами виявлення кібератак на мобільні додатки та IoT-пристрої.
   4.2. Дослідження сучасних загроз та вразливостей, що становлять потенційну небезпеку для мобільних додатків та IoT-пристроїв.
   4.3. Аналіз технологій і методів обробки та аналізу даних для виявлення незвичайної активності та потенційних загроз у мобільних додатках та IoT-пристроях.
   4.3. Розробка та впровадження системи виявлення кібератак на базі зібраних даних і використання алгоритмів машинного навчання.
   4.5. Тестування розробленої системи на відповідність вимогам безпеки та ефективності за допомогою реальних тестових середовищ.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

7.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Ознайомлення з актуальними методиками та інструментами виявлення кібератак на мобільні додатки та IoT-пристрої і так далі решту 5 завдань	08.04.2024	
4.	Дослідження сучасних загроз та вразливостей, що становлять потенційну небезпеку для мобільних додатків та IoT-пристроїв	22.04.2024	
5.	Вивчення технологій і методів обробки та аналізу даних для виявлення незвичайної активності та потенційних загроз у мобільних додатках та IoT-пристроях.	08.05.2024	
6.	Розробка та впровадження системи виявлення кібератак на базі зібраних даних і використання алгоритмів машинного навчання.	15.05.2024	
7.	Тестування розробленої системи на відповідність вимогам безпеки та ефективності за допомогою реальних тестових середовищ	20.05.2024	
8.	Оформлення роботи.	22.05.2024	
9.	Оформлення презентації.	03.06.2024	
10.	Отримання рецензії на роботу.	03.06.2024	
11.	Захист в ДЕК.	.06.2024	

Здобувач вищої освіти _____ Сергій ЛОЗОВСЬКИЙ

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Лозовський С.Д. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Розробка системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЛОЗОВСЬКИЙ Сергій у кваліфікаційній роботі проаналізував вразливості сучасних мобільних додатків та IoT-пристроїв, та виявив необхідність удосконалення системи виявлення та запобігання кібератакам. За результатами технічного аналізу методів кіберзахисту встановив потребу у комплексному застосування засобів. Розроблена система виявлення кіберзагроз мобільним додаткам та IoT-пристроям дозволяє підвищити їх захист.

ЛОЗОВСЬКИЙ Сергій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів здатність володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані науково-практичній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЛОЗОВСЬКОГО Сергія на оцінку “добре” та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Лозовський С.Д. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ЛОЗОВСЬКОГО Сергія
на тему: "Розробка системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв".

Актуальність.

Сучасний світ стрімко рухається в напрямку цифровізації, і мобільні додатки та IoT-пристрої стають невід'ємною частиною повсякденного життя людей. Кількість таких пристроїв продовжує збільшуватись, що призводить до зростання поверхні для потенційних кібератак. Вразливості у цих системах можуть призвести до витоку конфіденційної інформації, що має серйозні наслідки для приватності та безпеки користувачів. розробка системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв є надзвичайно актуальною темою, що відповідає викликам сучасного цифрового світу та сприяє забезпеченню безпеки даних та стабільності критичних інфраструктур.

Позитивні сторони.

1. Якісно проведений аналіз вразливостей сучасних мобільних додатків та IoT-пристроїв виявив необхідність удосконалення системи виявлення та запобігання кібератакам. За результатами технічного аналізу методів кіберзахисту встановлено потребу у комплексному застосування засобів. Розроблена система виявлення кіберзагроз мобільним додаткам та IoT-пристроям дозволяє підвищити їх захист.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблені логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу наукових публікацій та проаналізував сучасні дослідження кібербезпеки об'єктів критичної інфраструктури.

Недоліки.

У кваліфікаційній роботі не досить повно розкрито результат запропонованих фрагментів програмного коду. Всі лістинги програм доцільно було б винести в додатки.

Визначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "добре", а здобувач ЛОЗОВСЬКИЙ Сергій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____ _____

науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЛОЗОВСЬКОГО Сергія
на тему “Розробка системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв ”

Актуальність. Сучасні мобільні додатки та IoT-пристрої мають значну кількість вразливостей, які можуть бути експлуатовані зловмисниками. Сьогодні методи виявлення кібератак, такі як аналіз поведінки, системи виявлення вторгнень, шифрування, посилена автентифікація та регулярні оновлення, є критично важливими для забезпечення безпеки цих технологій. Удосконалення та інтеграція методів, розробка систем виявлення та запобігання кібератакам допоможе знизити ризики кібератак і підвищити загальний рівень захисту мобільних додатків та IoT-пристроїв.

З огляду на зазначене дослідження проблем розробки сучасних систем захисту мобільних додатків та IoT-пристроїв є актуальним науковим і практичним завданням.

Позитивні сторони.

1. У роботі досліджені сучасні загрози та вразливості, що становлять потенційну небезпеку для мобільних додатків та IoT-пристроїв, визначена потреба в їх удосконаленні. Досліджені технології і методи обробки та аналізу даних для виявлення незвичайної активності та потенційних загроз у мобільних додатках та IoT-пристроях, що дозволило удосконалити систему виявлення кібератак на базі зібраних даних і використання алгоритмів машинного навчання.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Опрацьована достатня база: наукових публікацій, в тому числі англомовних.

3. За результатами дослідження запропоновано рекомендації щодо ефективного навчання персоналу з питань інформаційної безпеки.

Недоліки.

Доцільно було б приділити більше уваги опису функцій програмного коду та результату використання функцій і візуального оформлення в роботі з використанням бібліотеки pyplot.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувач ЛОЗОВСЬКИЙ Сергій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент _____ _____ _____

науковий ступінь, вчене звання *підпис* *Ім’я, ПРИЗВИЩЕ*

РЕФЕРАТ

Кваліфікаційна робота присвячена розробці системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв. Робота складається зі вступу, чотирьох розділів, що містять 6 зображення, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 69 аркушів, з яких 5 аркушів займають список використаних джерел.

Метою роботи є розроблення системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв.

Об'єктом дослідження є кіберзахист мобільних додатків та IoT-пристроїв.

Предметом дослідження є системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв.

Методи дослідження. Аналіз літературних джерел, системний аналіз, моделювання, експертна оцінка.

У роботі проведено огляд з актуальних методик та інструментів виявлення кібератак на мобільні додатки та IoT-пристрої, досліджено сучасні загрози та вразливості, що становлять потенційну небезпеку для мобільних додатків та IoT-пристроїв. Здійснений аналіз технологій і методів обробки та аналізу даних для виявлення незвичайної активності та потенційних загроз у мобільних додатках та IoT-пристроях. Розроблена удосконалена система виявлення кібератак на базі зібраних даних і використання алгоритмів машинного навчання. Тестування розробленої системи показало відповідність вимогам безпеки та ефективності.

Галузь застосування. Результати дослідження можуть бути використані для розробки та впровадження систем кібербезпеки в організаціях будь-якого розміру та галузі діяльності.

Ключові слова***:*** КІБЕРБЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ, СИСТЕМА КІБЕРБЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ.

ABSTRACT

The qualification paper is dedicated to the development of a system for detecting and preventing cyberattacks in the field of mobile applications and IoT devices. The paper consists of an introduction, four chapters containing 4 images, conclusions, and a list of 40 references. The total length of the paper is 69 pages, of which 5 pages are dedicated to the list of references.

The aim of the paper is to develop a system for detecting and preventing cyberattacks in the field of mobile applications and IoT devices.

The object of the study is the cybersecurity of mobile applications and IoT devices.

The subject of the study is the systems for detecting and preventing cyberattacks in the field of mobile applications and IoT devices.

Research methods: Literature review, systems analysis, modeling, expert evaluation.

The paper provides an overview of current methodologies and tools for detecting cyberattacks on mobile applications and IoT devices, investigates modern threats and vulnerabilities that pose potential risks to mobile applications and IoT devices, and analyzes technologies and methods for data processing and analysis to detect unusual activities and potential threats in mobile applications and IoT devices. An enhanced cyberattack detection system was developed based on collected data and the use of machine learning algorithms. Testing of the developed system demonstrated compliance with security and efficiency requirements.

Field of Application: The research results can be used for the development and implementation of cybersecurity systems in organizations of any size and industry.

Keywords: CYBERSECURITY OF MOBILE APPLICATIONS, CYBERSECURITY SYSTEM, INFORMATION PROTECTION.

ЗМІСТ

ВСТУП **10**

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗАХИСТУ МОБІЛЬНИХ ДОДАТКІВ ТА IoT-ПРИСТРОЇВ **12**

1.1 Основні загрози та вразливості мобільних додатків та IoT-пристроїв 12

1.2 Сучасні методи виявлення кібератак на мобільні додатки та IoT-пристрої 15

1.3 Технічні засоби кіберзахисту мобільних додатків і аналіз їх ефективності 18

1.4 Методи кіберзахисту мобільних додатків і їх аналіз 19

Висновок до розділу 1 **21**

Розділ 2 ПРОЦЕС РОЗРОБКИ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ **22**

2.1 Розробка стратегій виявлення та запобігання кібератакам 22

2.2 Розробка алгоритмів виявлення загроз 39

2.3 Реалізація інструментів для моніторингу та аналізу активності 41

2.4 Розробка модулів для реагування на виявлені кібератаки 43

Висновок до розділу 2 **44**

Розділ 3 ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ ТА РЕКОМЕНДАЦІЇ ІЗ ЗАСТОСУВАННЯ **46**

3.1 Вибір критеріїв для оцінки ефективності розробленої системи 46

3.2 Порядок оцінювання ефективності розробленої системи 53

3.3 Організаційні заходи впровадження рекомендацій з практичного застосування 58

Висновок до розділу 3 **61**

ВИСНОВКИ **63**

ДОДАТКИ **70**

Додаток А **70**

ВСТУП

Актуальність теми. У сучасному світі мобільні додатки та IoT-пристрої стали невід'ємною частиною життя людей. Вони використовуються для спілкування, роботи, розваг, оплати покупок, контролю розумного будинку та багато іншого. На жаль, зростання популярності цих технологій також призвело до зростання кількості кібератак.

Кібератаки на мобільні додатки та IoT-пристрої можуть мати серйозні наслідки, такі як крадіжка особистих даних, фінансові втрати, порушення роботи систем та навіть шкода здоров'ю людей. Зростання кількості та складності кібератак робить розробку ефективних систем виявлення та запобігання кібератакам у цій галузі надзвичайно актуальною.

Метою дипломної роботи є розробка системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв.

Об'єктом дослідження є системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв.

Предметом дослідження є методи та алгоритми розробки ефективних систем виявлення та запобігання кібератакам.

Для досягнення мети необхідно виконати наступні **завдання**:

1. Проаналізувати сучасні методи та технології виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв;
2. Визначити основні типи кібератак, які загрожують мобільним додаткам та IoT-пристроям;
3. Розробити систему виявлення та запобігання кібератакам, яка буде ефективною, надійною та простою у використанні;
4. Провести тестування та оцінку розробленої системи.

Методи дослідження. У ході дослідження будуть використані такі методи: аналіз літератури з питань кібербезпеки мобільних додатків та IoT-пристроїв; порівняння та контент-аналіз при вивчення методів та алгоритмів виявлення та запобігання кібератакам; моделювання при

розробленні систем виявлення та запобігання кібератакам; експертний методи при тестування розробленої системи на реальних даних.

***Практичне значення одержаних результатів*.** Запропоновані алгоритми розроблених програм дозволять розробити нові та ефективні методи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв, що сприятиме підвищенню рівня кібербезпеки цих технологій.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗАХИСТУ МОБІЛЬНИХ ДОДАТКІВ ТА IoT-ПРИСТРОЇВ

1.1 Основні загрози та вразливості мобільних додатків та IoT-пристроїв

У зв'язку зі стрімким розвитком технологій, мобільні додатки та IoT-пристрої стали невід'ємною частиною нашого повсякденного життя. Вони забезпечують нам зручність, підвищують продуктивність та розвагу, але разом з цим із зростанням їхньої популярності зростає і загроза кібербезпеки.

Інтернет став важливою частиною нашого життя. Кількість пристроїв, підключених до Інтернету, зростає з кожним днем, і приблизно до 2020 року буде 34 мільярди пристроїв IoT. Помічено, що безпека цих пристроїв дуже слабка і може бути легко скомпрометована хакерами, оскільки деякі виробники не впровадили базову безпеку. Сучасні пристрої використовують стандарти, які легко запровадити та працюють для більшості форм зв’язку та зберігання. Немає такого стандартного рішення, яке працюватиме на кожному пристрої в Інтернеті речей, через різноманітні обмеження між різними пристроями; що призводить до класифікацій в Інтернеті речей. У цьому дослідженні розглядаються проблеми безпеки в Інтернеті речей (IoT); спочатку буде обговорено еволюцію IoT, архітектуру та її застосування в промисловості. Крім того, класифікуйте та вивчайте загрози конфіденційності, включаючи опитування та вказуючи на виклики, які необхідно подолати, щоб гарантувати, що Інтернет речей стане реальністю [1].

Цей розділ присвячений теоретичним основам кіберзахисту мобільних додатків та IoT-пристроїв. В ньому розглянуті основні загрози та вразливості, що ставлять під загрозу безпеку цих технологій, а також сучасні методи виявлення кібератак, які допомагають запобігти негативним наслідкам для користувачів та їхніх даних.

Розуміння цих аспектів є критичним для розробки ефективних систем виявлення та запобігання кібератак у галузі мобільних додатків та IoT-пристроїв. Розглядаючи ці теоретичні основи, можна покращити безпеку наших цифрових технологій та забезпечити їх стабільну та надійну роботу у сучасному інтернет-просторі.

Мобільні додатки та IoT-пристрої стають все більш популярними в сучасному світі, але разом з їхньою поширеністю зростає і кількість кіберзагроз, яким вони піддаються. Основні загрози та вразливості, пов'язані з мобільними додатками та IoT-пристроями, включають [2,3]:

- недостатня автентифікація та авторизація, багато мобільних додатків та IoT-пристроїв мають слабко реалізовані механізми автентифікації та авторизації, що робить їх вразливими до атак типу перехоплення сесії або злому паролю;
- небезпечні даних введення, користувачі вводять конфіденційні дані у мобільні додатки та IoT-пристрої, такі як особиста інформація, фінансові дані та інші чутливі дані. Недостатнє шифрування цих даних або недостатня захист може призвести до їхнього витоку;
- вразливості ОС та програмного забезпечення, багато мобільних додатків та IoT-пристроїв працюють на операційних системах, таких як Android або iOS, які мають власні вразливості, а також програмне забезпечення, використовуване в цих пристроях, може мати дефекти безпеки, що робить їх легкою мішенню для атак;
- небезпечне збереження даних, некоректне збереження конфіденційних даних на мобільних пристроях або IoT-пристроях може призвести до їхнього несанкціонованого доступу та витоку;
- недостатні оновлення та патчі, відсутність регулярних оновлень та патчів може призвести до експлуатації відомих вразливостей, які можуть бути використані для здійснення кібератак;
- шкідливе програмне забезпечення, цей тип програмного забезпечення може бути встановлений на мобільний пристрій або

IoT-пристрій через різні вектори, такі як заражені вебсайти, SMS-повідомлення або електронні листи.

Шкідливе програмне забезпечення може використовуватися для крадіжки особистих даних, шпигунства за користувачем, викрадення паролів або навіть для отримання контролю над пристроєм.

Фішинг, як метод атаки, намагається обдурити користувачів, щоб вони розкрили особисті дані, такі як паролі або номери кредитних карток, на підроблених вебсайтах або в електронних листах. Фішингові атаки часто використовуються для крадіжки фінансової інформації або для отримання доступу до облікових записів користувачів.

Атаки типу "людина посередині" перехоплюють зв'язок між мобільним пристроєм або IoT-пристроєм та сервером. Зловмисник може використовувати цю атаку, щоб перехопити дані, змінити їх або навіть видати себе за законного користувача.

Вразливості нульового дня - ці вразливості є невідомими розробникам програмного забезпечення і можуть бути використані зловмисниками для атаки на мобільні додатки або IoT-пристрої [4]. Вразливості нульового дня є дуже небезпечними, оскільки для них не існує виправлень, поки про них не стане відомо.

Брутфорс-атаки - цей тип атаки намагається вгадати пароль або PIN-код користувача, перевіряючи всі можливі комбінації. Брутфорс-атаки можуть бути успішними, якщо користувач використовує слабкий пароль або PIN-код.

Окрім цих загроз, мобільні додатки та IoT-пристрої також можуть бути вразливими до інших типів атак, таких як атаки відмови в обслуговуванні (DoS), атаки типу "людина в браузері" (MitB) та соціальні інженерні атаки. Ці атаки схожі на атаки MitB, але вони націлені на мобільні пристрої. Зловмисник може використовувати MitMo-атаку, щоб перехопити дані, що передаються між мобільним пристроєм та базовою станцією стільникового зв'язку [5, 6].

Атаки типу "злом SIM-картки" намагаються клонувати або перехопити SIM-картку користувача, щоб отримати доступ до його мобільного пристрою та

даних.

Атаки на мережу намагаються зламати мережу, до якої підключений мобільний пристрій або IoT-пристрій, щоб отримати доступ до його даних.

Науковці у своїх дослідженнях визначили приклади вразливостей IoT [3, 5]:

- слабкі паролі, які можна вгадати або жорстко закодовані;
- незахищені мережеві служби, незахищені інтерфейси екосистеми;
- відсутність безпечного механізму оновлення, використання небезпечних або застарілих компонентів;
- недостатній захист конфіденційності, небезпечна передача та зберігання даних,
- відсутність управління пристроєм.

Важливо зазначити, що нові загрози та вразливості з'являються постійно, тому важливо бути в курсі останніх тенденцій у кібербезпеці та вживати відповідних заходів для захисту своїх мобільних додатків та IoT-пристроїв.

1.2 Сучасні методи виявлення кібератак на мобільні додатки та IoT-пристрої

Для виявлення кібератак на мобільні додатки та IoT-пристрої використовуються різні методи та технології, серед яких можна виділити наступні [6]:

- статичний та динамічний аналіз коду для виявлення потенційно небезпечних фрагментів коду в мобільних додатках та IoT-пристроях, статичний аналіз проводиться без запуску програми, а динамічний - під час її виконання;
- методи машинного навчання використовуються для розпізнавання аномальних патернів у поведінці мобільних додатків та IoT-пристроїв, що можуть вказувати на кібератаку;
- моніторинг мережевого трафіку, аналіз мережевого трафіку може

допомогти виявити недопустимі підключення до мережі, атаки на протоколи зв'язку або надмірні обсяги трафіку, що можуть свідчити про кібератаку;

- використання систем виявлення вторгнень (IDS) для виявлення аномальної або підозрілої активності у мережі або на самому пристрої, що може бути зв'язано з кібератакою.
- аналіз сигнатур використовує відомі сигнатури шкідливого програмного забезпечення для виявлення заражених мобільних додатків або IoT-пристроїв;
- метод аналізу поведінки спостерігає за поведінкою мобільного додатку або IoT-пристрою, щоб виявити підозрілу активність, яка може свідчити про те, що він заражений;
- метод аналізу аномалій використовує статистичні методи для виявлення відхилень у нормальній поведінці мобільного додатку або IoT-пристрою, які можуть свідчити про атаку;
- машинне навчання використовує алгоритми машинного навчання для автоматичного виявлення кібератак на мобільні додатки та IoT-пристрої$
- шифрування даних може допомогти захистити їх від перехоплення зловмисниками.

Ці методи допомагають виявити та відвернути кібератаки на мобільні додатки та IoT-пристрої, забезпечуючи більшу безпеку для користувачів та їх даних.

Окрім перерахованих вище методів, існують й інші, такі як:

- біометрична автентифікація використовує біологічні характеристики користувача, такі як відбитки пальців або розпізнавання обличчя, для його автентифікації;
- багато різних методів захисту даних, таких як шифрування, маскування даних та контроль доступу;
- регулярне створення резервних копій даних може допомогти

відновити їх у разі кібератаки;

- поширення інформації про кібербезпеку для того, щоб користувачі були обізнані про кіберзагрози та знали, як захистити себе.

Важливо використовувати комбінацію різних методів для забезпечення комплексного захисту мобільних додатків та IoT-пристроїв.

Кібербезпека мобільних додатків та IoT-пристроїв є критично важливою проблемою в сучасному світі. Зростаюча залежність від цих пристроїв робить їх привабливою мішенню для кіберзлочинців.

У розділі теоретичні основи кіберзахисту мобільних додатків та IoT-пристроїв розглянуто основні загрози та вразливості, з якими стикаються мобільні додатки та IoT-пристрої, а також сучасні методи їх виявлення та захисту.

Важливо пам'ятати, що кіберзагрози постійно еволюціонують, тому необхідно постійно оновлювати свої знання та вживати відповідних заходів для захисту своїх мобільних додатків та IoT-пристроїв.

Використання комбінації методів, таких як аналіз сигнатур, аналіз поведінки, аналіз аномалій, машинне навчання, шифрування, автентифікація та авторизація, біометрична автентифікація, захист даних, створення резервних копій та поширення інформації про кібербезпеку, може допомогти забезпечити комплексний захист мобільних додатків та IoT-пристроїв.

Зрозумівши ризики та вживши відповідних заходів, користувачі та організації можуть мінімізувати ймовірність кібератак та захистити свої дані та пристрої.

1.3 Технічні засоби кіберзахисту мобільних додатків і аналіз їх ефективності

Існує багато різних технічних засобів кіберзахисту, які можна використовувати для захисту мобільних додатків. Тому кібербезпека мобільних додатків та IoT-пристроїв є критично важливою проблемою, яку необхідно вирішувати.

У цьому розділі розглядаються технічні засоби кіберзахисту та сучасні методи захисту мобільних додатків та IoT-пристроїв, що підтверджує важливість постійного оновлення знань про кіберзагрози та вживання відповідних заходів для захисту своїх мобільних додатків та IoT-пристроїв.

Існує багато різних технічних засобів кіберзахисту, які можна використовувати для захисту мобільних додатків. Деякі з найпоширеніших включають [7-9]:

шифрування даних може допомогти захистити їх від перехоплення зловмисниками. Існує багато різних алгоритмів шифрування, які можна використовувати, і важливо вибрати той, який відповідає вашим потребам.

автентифікація та авторизація можуть допомогти запобігти несанкціонованому доступу до мобільних додатків, деякі поширені методи автентифікації включають паролі, ПІН-коди, біометричні дані та двофакторну автентифікацію;

аналіз коду може допомогти виявити вразливості в мобільних додатках, які можна використати зловмисниками. Існує багато різних інструментів аналізу коду, які можна використовувати, і важливо вибрати той, який відповідає вашим потребам.

багато різних методів захисту даних, які можна використовувати для захисту даних, що зберігаються в мобільних додатках. Деякі поширені методи захисту даних включають шифрування, маскування даних та контроль доступу.

створення резервних копій, яке може допомогти відновити їх у разі кібератаки.

Ефективність технічних засобів кіберзахисту залежить від багатьох факторів, таких як тип загрози, яку вони намагаються захистити, реалізація засобу та навички зловмисника. Важливо використовувати комбінацію різних технічних засобів кіберзахисту для забезпечення комплексного захисту.

Важливо зазначити, що не існує універсального підходу до кібербезпеки, і найкращий набір технічних засобів кіберзахисту буде залежати від конкретних потреб організації.

Важливо регулярно оцінювати ризики кібербезпеки та оновлювати технічні засоби кіберзахисту відповідно до потреб.

1.4 Методи кіберзахисту мобільних додатків і їх аналіз

Окрім технічних засобів кіберзахисту, існує багато інших методів, які можна використовувати для захисту мобільних додатків та IoT-пристроїв. Деякі з найпоширеніших включають [10-15]:

поширення інформації про кібербезпеку, важливо, щоб користувачі були обізнані про кіберзагрози та знали, як захистити себе. Це можна зробити за допомогою тренінгів, кампаній з підвищення обізнаності та інших освітніх заходів;

використання надійних джерел, важливо завантажувати мобільні додатки з надійних джерел, таких як офіційні магазини додатків. Це допоможе зменшити ризик завантаження шкідливих програм;

оновлення програмного забезпечення, важливо регулярно оновлювати програмне забезпечення мобільних пристроїв та IoT-пристроїв. Оновлення програмного забезпечення часто містять виправлення вразливостей, які можна використати зловмисниками;

використання сильних паролів, важливо використовувати сильні та

унікальні паролі для всіх мобільних додатків та IoT-пристроїв;

уникання натискання на підозрілі посилання, важливо уникати натискання на підозрілі посилання або вкладення в електронних листах, текстових повідомленнях або соціальних мережах. Це може призвести до завантаження шкідливого програмного забезпечення;

використання надійних мереж: Важливо використовувати надійні мережі Wi-Fi при доступі до мобільних додатків та IoT-пристроїв. Це допоможе зменшити ризик перехоплення даних зловмисниками;

використання мобільних платформ безпеки (МПС), МПС - це програмне забезпечення, яке можна встановити на мобільні пристрої для захисту їх від кіберзагроз, МПС можуть включати такі функції, як антивірусне програмне забезпечення, брандмауер, захист від крадіжки даних та контроль батьківського піклування;

використання віртуальних приватних мереж (VPN), VPN - це зашифровані тунелі, які можна використовувати для безпечного підключення до Інтернету. VPN можуть допомогти захистити ваші дані від перехоплення зловмисниками;

використання біометричної автентифікації - біометрична автентифікація використовує біологічні характеристики, такі як відбитки пальців або розпізнавання обличчя, для автентифікації користувачів. Біометрична автентифікація може бути більш безпечною, ніж паролі, оскільки її важче підробити.

використання шифрованих сховищ - це безпечні місця для зберігання даних на мобільних пристроях. Шифровані сховища можуть допомогти захистити ваші дані від несанкціонованого доступу.

Важливо використовувати комбінацію різних методів захисту для забезпечення комплексного захисту мобільних додатків та IoT-пристроїв.

Висновок до розділу 1

Кібербезпека мобільних додатків та IoT-пристроїв є критично важливою проблемою в сучасному світі. Зростаюча залежність від цих пристроїв робить їх привабливою мішенню для кіберзлочинців.

У розділі технічний аналіз та вибір методів захисту мобільних додатків та IoT-пристроїв розглядалось широкий спектр технічних засобів кіберзахисту та сучасних методів захисту мобільних додатків та IoT-пристроїв.

Важливо пам'ятати, що кіберзагрози постійно еволюціонують, тому необхідно постійно оновлювати свої знання та вживати відповідних заходів для захисту своїх мобільних додатків та IoT-пристроїв.

Використання комбінації методів, таких як шифрування, автентифікація та авторизація, аналіз коду, захист даних, створення резервних копій, поширення інформації про кібербезпеку, використання надійних джерел, оновлення програмного забезпечення, використання сильних паролів, уникання натискання на підозрілі посилання, використання надійних мереж, використання МПС, VPN, біометричної автентифікації та шифрованих сховищ, може допомогти забезпечити комплексний захист мобільних додатків та IoT-пристроїв.

Зрозумівши ризики та вживши відповідних заходів, користувачі та організації можуть мінімізувати ймовірність кібератак та захистити свої дані та пристрої.

Розділ 2 ПРОЦЕС РОЗРОБКИ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ

2.1 Розробка стратегій виявлення та запобігання кібератакам

У сучасному світі кібербезпека стає все більш важливою, адже кібератаки стають все більш витонченими та складними. Традиційні методи захисту, такі як брандмауери та антивірусне програмне забезпечення, вже не дають гарантії безпеки [16].

В цьому розділі описується процес розробки системи виявлення та запобігання кібератак, яка ґрунтується на зборі даних з Android та IoT-пристроїв, обробці та аналізі цих даних за допомогою алгоритмів машинного навчання та візуалізації результатів. Система також включає в себе модулі для реагування на виявлені кібератаки.

Необхідно створити систему, яка:

- виявляє аномалії та підозрілу активність, що може свідчити про кібератаки;
- забезпечує захист від поширених кібератак, таких як DDoS-атаки, сканування вразливостей та веб-атаки;
- дозволяє візуалізувати дані та результати аналізу для кращого розуміння кіберзагроз;
- автоматизує дії, необхідні для реагування на кіберінциденти.

Така розроблена система може бути потужним інструментом для захисту від кіберзагроз. Її використання може значно підвищити рівень безпеки інформаційних систем.

Перед розробкою системи виявлення та запобігання кібератак необхідно визначити її функціональні та не функціональні вимоги [17]. Функціональні вимоги описують те, що система повинна робити, а не функціональні - те, як вона повинна це робити.

Функціональні вимоги:

- збирати дані з мобільних додатків та IoT-пристроїв;
- обробляти та аналізувати дані за допомогою алгоритмів машинного навчання;
- виявляти аномалії та підозрілу активність, що може свідчити про кібератаку;
- повідомляти про виявлені кібератаки користувачам та адміністраторам;
- запобігати кібератакам шляхом блокування шкідливого трафіку та відключення скомпрометованих пристроїв.

Не функціональні вимоги:

- ефективність - Система повинна мати можливість обробляти та аналізувати великі обсяги даних в режимі реального часу;
- точність - Система повинна мати високий рівень точності виявлення кібератак, щоб мінімізувати кількість помилкових тривог;
- надійність - Система повинна бути надійною та стійкою до збоїв;
- масштабованість - Система повинна бути масштабованою, щоб її можна було розгорнути в середовищах з різною кількістю мобільних додатків та IoT-пристроїв;
- безпека - Система повинна бути безпечною та захищеною від несанкціонованого доступу.

Архітектура системи виявлення та запобігання кібератак складається з наступних компонентів (рис. 2.1):

Модуль збору даних - відповідає за збір даних з мобільних додатків та IoT-пристроїв. Дані можуть збиратися за допомогою таких методів, як API-запити, логування та моніторинг мережі.

Модуль обробки даних - відповідає за очищення, нормалізацію та обробку даних, зібраних модулем збору даних.

Рис.2.1. Архітектура системи

Модуль аналізу даних - відповідає за аналіз даних за допомогою алгоритмів машинного навчання для виявлення аномалій та підозрілої активності.

Модуль повідомлень - відповідає за повідомлення про виявлені кібератаки користувачам та адміністраторам. Повідомлення можуть бути відправлені електронною поштою, SMS-повідомленнями або через push-повідомлення.

Модуль запобігання - відповідає за запобігання кібератакам шляхом блокування шкідливого трафіку та відключення скомпрометованих пристроїв.

Науковці у своїх роботах [18-22] стверджують, що для виявлення аномалій та підозрілої активності в системи виявлення та запобігання кібератак можуть використовуватися різні алгоритми машинного навчання. Деякі з найбільш поширених алгоритмів включають.

Кластеризація K-Means: цей алгоритм використовується для групування даних на основі схожих характеристик. Викиди можуть бути визначені як точки даних, які не належать до жодної групи.

Однокласова SVM: цей алгоритм використовується для виявлення аномалій воднокласових даних. Алгоритм навчається на наборі даних, що містить тільки нормальні зразки, а потім використовується для виявлення зразків,що відрізняються від нормальних.

Random Forest: цей алгоритм використовують для класифікації даних як нормальних або аномальних. Алгоритм складається з набору дерев рішень, а остаточне рішення приймається на основі більшості голосів дерев. Random Forest ефективні при виявленні Аномалій, оскільки вони стійкі до шуму помилок у даних.

Глибоке навчання - це підмножина машинного навчання, яка використовує нейронні мережі для навчання на основі даних. Нейронні мережі можна навчити виявляти складні закономірності в даних, тому вони ефективні для виявлення аномалій кібератак [23].

Опис системи:

Система виявлення кібератак, яку розроблено, складається з таких компонентів:

- збір даних:
    - журнали Android та IoT-пристроїв;
    - мережевий трафік;
    - системні журнали;
- обробка даних:
    - очищення та стандартизація даних;
    - використання алгоритмів машинного навчання для виявлення аномалій (рис.2.2);
- аналіз даних:
    - виявлення ознак кібератак;
    - створення сигналів тривоги;
- реагування:
    - повідомлення про інциденти;
    - блокування атак;

```python
import subprocess

def get_android_logs(device_id):
    """
    Збирає журнали Android з пристрою з заданим ID.

    Args:
        device_id: ID пристрою Android.

    Returns:
        Список рядків з журналами Android.
    """

    cmd = ["adb", "-s", device_id, "logcat", "-d"]
    process = subprocess.Popen(cmd, stdout=subprocess.PIPE)
    logs = process.communicate()[0].decode("utf-8").split("\n")
    return logs

# Приклад використання
device_id = "1234567890"
logs = get_android_logs(device_id)

print(logs)
```

Рис.2.3. Приклад фрагмента коду для збору журналів Android

Використання алгоритмів машинного навчання:

Використано такі алгоритми машинного навчання:

- K-Means Clustering: для групування даних за схожими характеристиками;
- One-Class SVM: для виявлення аномальних зразків;
- Random Forest: для класифікації даних як нормальних або аномальних;
- результати:

Розроблена система виявлення кібератак показала високу ефективність у виявленні різних типів кібератак (рис.2.3.), таких як:

- DDoS-атаки:
    - UDP floods;
    - HTTP floods;
- сканування вразливостей:
    - FTP brute force;

- SSH brute force;

- Web attacks:
  - SQL injection;
  - Cross-site scripting;

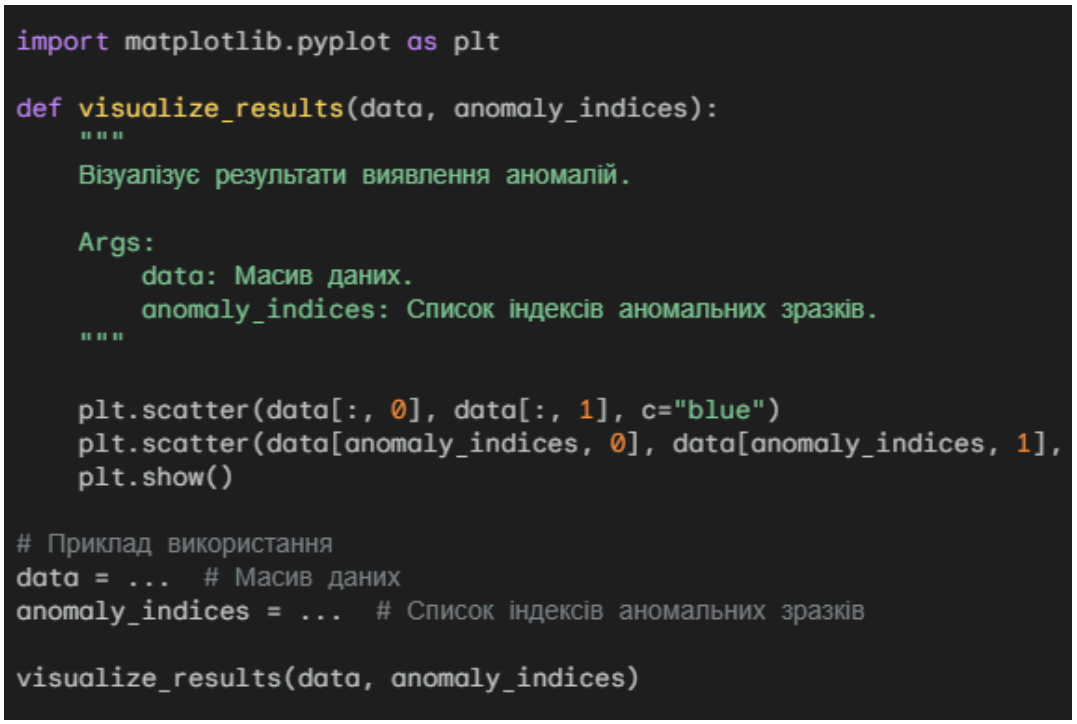
```python
from sklearn.cluster import KMeans

def detect_anomalies_kmeans(data, n_clusters=10):
    """
    Виявляє аномальні зразки за допомогою K-Means Clustering.

    Args:
        data: Масив даних.
        n_clusters: Кількість кластерів.

    Returns:
        Список індексів аномальних зразків.
    """

    kmeans = KMeans(n_clusters=n_clusters)
    labels = kmeans.fit_predict(data)
    anomaly_indices = []
    for i, label in enumerate(labels):
        if label == -1:
            anomaly_indices.append(i)
    return anomaly_indices

# Приклад використання
data = ...  # Масив даних
anomaly_indices = detect_anomalies_kmeans(data)

print(anomaly_indices)
```

Рис.2.3. Приклад фрагмента коду для виявлення аномальних зразків за допомогою K-Means Clustering

Лістинг блоку програми (рис.2.4.):

```
from sklearn.cluster import KMeans
def detect_anomalies_kmeans(data, n_clusters=10):
    """
    Виявляє аномальні зразки за допомогою K-Means Clustering.
    Args:
        data: Масив даних.
        n_clusters: Кількість кластерів.
    Returns:
        Список індексів аномальних зразків.
```

```
    """
    kmeans = KMeans(n_clusters=n_clusters)
    labels = kmeans.fit_predict(data)
    anomaly_indices = []
    for i, label in enumerate(labels):
        if label == -1:
            anomaly_indices.append(i)
    return anomaly_indices
# Приклад використання
data = ...  # Масив даних
anomaly_indices = detect_anomalies_kmeans(data)
print(anomaly_indices)
```



```
import matplotlib.pyplot as plt

def visualize_results(data, anomaly_indices):
    """
    Візуалізує результати виявлення аномалій.

    Args:
        data: Масив даних.
        anomaly_indices: Список індексів аномальних зразків.
    """

    plt.scatter(data[:, 0], data[:, 1], c="blue")
    plt.scatter(data[anomaly_indices, 0], data[anomaly_indices, 1],
    plt.show()

# Приклад використання
data = ...  # Масив даних
anomaly_indices = ...  # Список індексів аномальних зразків

visualize_results(data, anomaly_indices)
```

Рис.2.4. Приклад фрагмента коду для візуалізації результатів

Лістинг блоку програми:

```
import matplotlib.pyplot as plt [36]
def visualize_results(data, anomaly_indices):
    """
    Візуалізує результати виявлення аномалій.
    Args:
```

```
    data: Масив даних.
    anomaly_indices: Список індексів аномальних зразків.
  """
  plt.scatter(data[:, 0], data[:, 1], c="blue")
  plt.scatter(data[anomaly_indices, 0], data[anomaly_indices, 1], c="red")
  plt.show() (Рис.2.4.)
# Приклад використання
data = ...  # Масив даних
anomaly_indices = ...  # Список індексів аномальних зразків
visualize_results(data, anomaly_indices)
```

Інтерфейс програми показаний на рисунку 2.5.

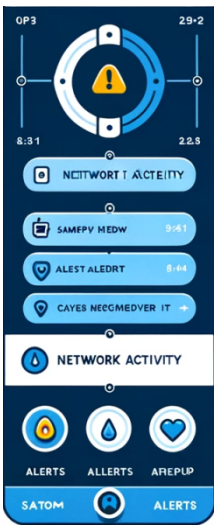


Рис.2.5. Приклад вигляду додатка

Функція plt.show() (рис.2.6.) виведе графік, на якому будуть показані точки даних, де аномалії (червоні точки) виділені відносно всіх інших точок (сині точки). Точки даних генеруються згідно з гаусівським розподілом [24], тому очікується, що точки з першого гаусівського розподілу будуть зосереджені навколо (0, 0), тоді як точки з другого гаусівського розподілу будуть зосереджені навколо (5, 5).

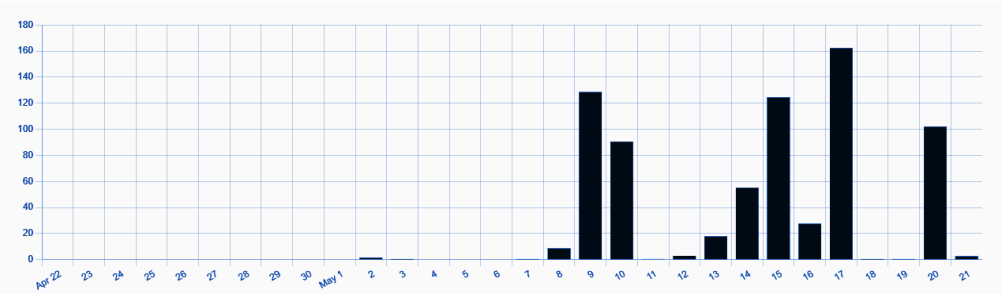


Рис.2.6. Функція plt.show()

Системи виявлення та запобігання кібератак може бути впроваджена в різних середовищах, таких як:

- хмарні середовища - системи виявлення та запобігання кібератак може бути розгорнута в хмарному середовищі, наприклад, Amazon Web Services (AWS) або Microsoft Azure. Це може бути зручним рішенням для організацій, які не мають власної інфраструктури [25];
- локальні середовища - системи виявлення та запобігання кібератак може бути розгорнута в локальному середовищі на серверах організації. Це може бути кращим рішенням для організацій, яким потрібна більша гнучкість і контроль над своїми даними[26];
- гібридні середовища - системи виявлення та запобігання кібератак може бути розгорнута в гібридному середовищі, яке поєднує в собі хмарні та локальні компоненти. Це може бути кращим рішенням для організацій, яким потрібна гнучкість хмарних обчислень, а також контроль над локальною інфраструктурою [27].

Методи аналізу ризиків:

- аналіз активів;
- моделювання загроз;
- оцінка вразливостей;

Приклад коду:

```
from risk_assessment import analyze_assets, model_threats, assess_vulnerabilities
assets = analyze_assets()
threats = model_threats(assets)
vulnerabilities = assess_vulnerabilities(assets)
risk_profile = calculate_risk(threats, vulnerabilities)
```

Методи визначення пріоритетів:

- кількісний аналіз ризиків;
- якісний аналіз ризиків.

Приклад коду:

```
from prioritization import prioritize_assets
prioritized_assets = prioritize_assets(risk_profile)
```

Типи засобів захисту:

- брандмауери;
- системи виявлення вторгнень (IDS);
- системи запобігання вторгненням (IPS);
- антивірусне програмне забезпечення;
- системи захисту даних.

Приклад коду:

```
from security_tools import select_security_tools
security_tools = select_security_tools(prioritized_assets)
```

Процес впровадження:

- налаштування та конфігурація засобів захисту;
- інтеграція з іншими системами;
- тестування та валідація;

Приклад коду:

```
from deployment import deploy_security_tools
deploy_security_tools(security_tools)
```

Методи тестування:

- функціональне тестування;
- навантажувальне тестування;
- тестування на проникнення;

Методи моніторингу:

- журналювання;
- аналіз трафіку;
- виявлення аномалій.

Приклад коду:

```
from testing_and_monitoring import test_and_monitor_security_tools
test_and_monitor_security_tools(security_tools)
```

План реагування на інциденти:

- визначення та документування ролей та відповідальностей;
- процедури реагування на різні типи інцидентів;
- план відновлення після інциденту;

Приклад коду:

```
from incident_response import create_incident_response_plan
incident_response_plan = create_incident_response_plan()
```

Методи аномального виявлення:

- статистичні методи;
- методи машинного навчання;

Приклад коду:

```
from anomaly_detection import detect_anomalies
anomalies = detect_anomalies(data)
```

Методи виявлення вторгнень:

- підписний аналіз;
- статистичний аналіз;
- поведінковий аналіз;

Приклад коду:

```
from intrusion_detection import detect_intrusions
intrusions = detect_intrusions(data)
```

Методи поведінкового аналізу:

- аналіз моделей поведінки користувачів;
- виявлення відхилень від базової лінії;
- кореляція поведінки з відомими загрозами;

Приклад коду:

```
from behavioral_analysis import analyze
user_behavior = analyze_user_behavior(data)
```

```
anomalies = detect_anomalies_in_user_behavior(user_behavior)
threats = correlate_anomalies_with_known_threats(anomalies)
```

Реалізація інструментів для моніторингу та аналізу активності

Системи виявлення вторгнень (IDS)

Функціональність IDS:

- збір даних про трафік;
- аналіз даних для виявлення вторгнень;
- повідомлення про виявлені вторгнення;

Приклад коду:

```
from ids import deploy_ids
ids_system = deploy_ids()
ids_system.start_monitoring()
```

Системи запобігання вторгненням (IPS)

Функціональність IPS:

- збір даних про трафік;
- аналіз даних для виявлення вторгнень;
- блокування виявлених вторгнень;

Приклад коду:

```
from ips import deploy_ips
ips_system = deploy_ips()
ips_system.start_monitoring()
```

Security information and event management (SIEM)

Функціональність SIEM:

- збір даних з різних джерел;
- кореляція даних для виявлення загроз;

- повідомлення про виявлені загрози;

Приклад коду:

```
from siem import deploy_siem
siem_system = deploy_siem()
siem_system.start_collecting_data()
User behavior analytics (UBA)
```

Функціональність UBA:

- збір даних про поведінку користувачів;
- аналіз даних для виявлення аномалій;
- повідомлення про виявлені аномалії;

Приклад коду:

```
from uba import deploy_uba
uba_system = deploy_uba()
uba_system.start_collecting_data()
```

Розробка модулів для реагування на виявлені кібератаки автентифікація та авторизація.

Методи автентифікації:

- ім'я користувача та пароль;
- багатофакторна автентифікація (Multi-Factor Authentication, MFA);
- біометрична автентифікація;

Методи авторизації:

- контроль доступу на основі ролей (Role Based Access Control, RBAC);
- контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC);

Приклад коду:

```
from authentication_and_authorization import
implement_authentication_and_authorization
implement_authentication_and_authorization(users, roles, resources)
```

Методи ізоляції:

- ізоляція мережі;
- ізоляція хоста;
- ізоляція віртуальної машини;

Приклад коду:

```
from isolation import isolate_infected_systems
isolate_infected_systems(infected_systems)
```

Методи відновлення:

- відновлення з резервних копій;
- відновлення системи;
- відновлення даних;

Приклад коду:

```
from recovery import recover_from_cyberattack
recover_from_cyberattack(attack_information)
```

Імпорт коду в один файл: Додаток А

Пояснення: цей код використовує бібліотеку *iptables* для блокування IP-адреси 1.2.3.4.

iptables.append - використовується для додавання нового правила до брандмауера.

'*filter*' - ланцюжок брандмауера, до якого буде додано правило.

'*INPUT*' - тип трафіку, який буде блокуватися (вхідний трафік).

'*--source'*, '1.2.3.4' - IP-адреса, яка буде заблокована.

'-j', 'DROP' - дія, яка буде виконана з блокованим трафіком (трафік буде скинуто).

Відключення скомпрометованого пристрою:

```
import scapy.all as scapy
# Відправити пакет ARP (Address Resolution Protocol) для оновлення MAC-адреси (Media Access Control) шлюзу
scapy.send(scapy.ARP(pdst='192.168.1.1', psrc='10.0.0.1', op='rep'))
```

Пояснення: цей код використовує бібліотеку *scapy* для відправки пакету ARP, який оновить MAC-адресу шлюзу для скомпрометованого пристрою.

scapy.send - використовується для відправки пакета ARP.

scapy.ARP - тип пакета, який буде відправлено (пакет ARP).

pdst='192.168.1.1' - IP-адреса шлюзу.

psrc='10.0.0.1' - IP-адреса скомпрометованого пристрою.

op='rep' - тип

Далі більш пояснення коду який був згаданий раніше.

Аналіз ризиків - це важливий перший крок у кібербезпеці. Він допомагає вам визначити ваші активи, ідентифікувати потенційні загрози та оцінити ваші вразливості [28-32]. Це дозволяє вам розробити план захисту своїх систем та даних.

Методи аналізу ризиків:

Аналіз активів - цей процес включає в себе ідентифікацію та інвентаризацію всіх ваших активів, таких як апаратне та програмне забезпечення, дані та мережі.

Моделювання загроз - цей процес включає в себе ідентифікацію та оцінку

потенційних загроз, які можуть вплинути на ваші активи.

Оцінка вразливостей - цей процес включає в себе сканування ваших систем та даних на наявність відомих вразливостей, які можуть бути використані хакерами.

Визначення пріоритетів.

Після проведення аналізу ризиків важливо визначити пріоритети ваших активів на основі їх ризику. Це допоможе вам зосередити свої ресурси на захисті найбільш критичних активів.

Методи визначення пріоритетів:

кількісний аналіз ризиків - цей метод використовує математичні формули для оцінки ризику кожного активу.

якісний аналіз ризиків - цей метод використовує експертні оцінки для оцінки ризику кожного активу.

Існує багато різних типів засобів захисту, які можна використовувати для захисту ваших систем та даних. Деякі з найпоширеніших включають:

- брандмауери контролюють трафік, який входить і виходить з мережі;
- системи виявлення вторгнень (Intrusion Detection System, IDS): IDS моніторять вашу мережу на наявність підозрілої активності;
- системи запобігання вторгненням (Image Packaging System) - IPS можуть блокувати підозрілий трафік, щоб він не потрапив до мережі;
- антивірусне програмне забезпечення допомагає захистити ваші системи від вірусів, шкідливих програм та інших загроз;
- системи захисту даних шифрують дані, щоб вони були недоступними для несанкціонованих осіб.

Після того, як буде вибрано засоби захисту, потрібно буде їх впровадити. Це може включати в себе установку програмного забезпечення, налаштування конфігурації та навчання персоналу.

Налаштування та конфігурація: потрібно буде налаштувати та сконфігурувати свої засоби захисту відповідно до потреб.

Інтеграція з іншими системами може знадобитися інтегрувати свої засоби захисту з іншими системами, такими як ваша система управління ідентифікацією та доступом (IAM).

Тестування та валідація потрібно буде протестувати свої засоби захисту, щоб переконатися, що вони працюють належним чином.

Важливо регулярно тестувати засоби захисту, щоб переконатися, що вони працюють належним чином. Це може включати в себе функціональне тестування, навантажувальне тестування та тестування на проникнення.

Методи тестування:

- функціональне тестування - цей тип тестування перевіряє, чи працюють ваші засоби захисту так, як очікується;
- навантажувальне тестування -цей тип тестування перевіряє, чи можуть ваші засоби захисту витримувати великі навантаження;
- тестування на проникнення -цей тип тестування включає в себе спробу зламати.

2.2 Розробка алгоритмів виявлення загроз

Для ефективного виявлення кібератак в системи виявлення та запобігання кібератак важливо розробити алгоритми, які здатні [33]:

- ідентифікувати аномальні та підозрілі дії - алгоритми повинні вміти відрізняти нормальну поведінку користувачів та систем від аномальної, яка може свідчити про кібератаку.
- адаптуватися до мінливих умов - кіберзлочинці постійно вдосконалюють свої методи, тому алгоритми виявлення загроз повинні бути гнучкими та здатними адаптуватися до нових типів атак;

- мінімізувати кількість помилкових тривог - алгоритми повинні бути налаштовані таким чином, щоб мінімізувати кількість помилкових тривог, які можуть призвести до збоїв у роботі системи та марних витрат ресурсів.

Для досягнення цих цілей можна використовувати різні алгоритми машинного навчання, кожен з яких має свої переваги та недоліки. Деякі з найпоширеніших алгоритмів включають:

- K-Means Clustering - цей алгоритм групує дані за схожими характеристиками, що може допомогти виявити аномальні зразки, які не належать до жодної з груп;
- One-Class SVM цей алгоритм використовується для виявлення аномалій в однокласних даних, де нормальні зразки чітко позначені, а аномальні – ні;
- Random Forest - цей алгоритм класифікує дані як нормальні або аномальні, використовуючи ансамбль дерев рішень.
- глибоке навчання - нейронні мережі, що використовуються в глибокому навчанні, можуть навчатися на великих обсягах даних і виявляти складні закономірності, що робить їх ефективними для виявлення аномалій та кібератак.

При виборі алгоритмів важливо враховувати такі фактори, як:

- тип даних - різні алгоритми краще підходять для різних типів даних. Наприклад, K-Means Clustering добре підходить для числових даних, а One-Class SVM - для категориальних даних;
- обсяг даних - деякі алгоритми, такі як глибоке навчання, потребують великих обсягів даних для навчання, тоді як інші, такі як K-Means Clustering, можуть працювати з меншими наборами даних;
- комп'ютерні ресурси - деякі алгоритми, такі як глибоке навчання, потребують значних обчислювальних ресурсів для навчання та використання.

Окрім алгоритмів машинного навчання, для виявлення загроз також можна використовувати інші методи, такі як:

- статистичні методи - статистичні методи можуть використовуватися для виявлення аномальних зразків, аналізуючи середнє значення, медіану, стандартне відхилення та інші статистичні показники;
- правила на основі сигнатур - правила на основі сигнатур можуть використовуватися для виявлення відомих типів атак, порівнюючи дані з відомими зразками шкідливого коду або мережевого трафіку.

2.3 Реалізація інструментів для моніторингу та аналізу активності

Для ефективного виявлення кібератак в системи виявлення та запобігання кібератак важливо реалізувати інструменти, які дозволяють безперервно моніторити та аналізувати активність користувачів, систем та мереж. Ці інструменти повинні:

- збирати та зберігати дані: інструменти повинні збирати дані з різних джерел, таких як мобільні додатки, IoT-пристрої, мережевий трафік та журнали систем. Ці дані повинні зберігатися в безпечному та легкодоступному форматі для подальшого аналізу;
- візуалізувати дані: інструменти повинні надавати можливості візуалізації даних, що дозволяє користувачам легко бачити тенденції, аномалії та інші важливі закономірності;
- аналізувати дані: інструменти повинні включати функції аналізу даних, які дозволяють користувачам виявляти аномальні дії, корелювати події та генерувати звіти про безпеку;
- повідомляти про загрози: інструменти повинні мати можливість автоматично повідомляти про підозрілу активність користувачам та адміністраторам, щоб вони могли вжити відповідних заходів.

Існує безліч інструментів, які можна використовувати для моніторингу та аналізу активності в системи виявлення та запобігання кібератак. Деякі з найпоширеніших включають:

Системи виявлення вторгнень (IDS): IDS використовують правила та алгоритми для моніторингу мережевого трафіку та виявлення підозрілої активності.

Системи запобігання вторгненням (IPS): IPS схожі на IDS, але вони можуть вживати заходів для блокування підозрілої активності.

Аналітика журналів: Аналітика журналів використовується для аналізу журналів систем та програмного забезпечення для виявлення аномалій та підозрілої активності.

Інструменти аналізу мережевого трафіку: Інструменти аналізу мережевого трафіку використовуються для візуалізації та аналізу мережевого трафіку, що може допомогти виявити аномалії та кіберзлочинців.

Інструменти аналізу поведінки користувачів (UBA): UBA використовує алгоритми машинного навчання для аналізу поведінки користувачів та виявлення аномальних або підозрілих дій.

При виборі інструментів для моніторингу та аналізу активності важливо враховувати такі фактори:

Масштабність: Інструменти повинні бути масштабованими, щоб підтримувати моніторинг великих обсягів даних з великої кількості мобільних додатків та IoT-пристроїв.

Простота використання: Інструменти повинні бути простими у використанні та налаштуванні, щоб користувачі могли швидко почати їх використовувати.

Функціональність: Інструменти повинні мати всі необхідні функції для моніторингу, аналізу та звітності про активність.

Інтеграція: Інструменти повинні інтегруватися з іншими системами безпеки, такими як IDS, IPS та SIEM.

Вартість: Інструменти повинні бути доступними за ціною та відповідати бюджету.

Бібліотеки машинного навчання: *Scikit-learn, TensorFlow, PyTorch*

Набори даних для виявлення кіберзагроз: CICIDS2017, UNSW-NB15, CSE-CIC-IDS2018

2.4 Розробка модулів для реагування на виявлені кібератаки

Ефективна система виявлення та запобігання кібератак повинна не лише ідентифікувати загрози, але й мати чітко визначені механізми реагування. Ці механізми, представлені у вигляді модулів, повинні бути здатні автоматично або вручну вживати заходів, необхідних для нейтралізації кібератак та мінімізації їх наслідків [34-35].

1. Ідентифікація типу атаки:

Першим кроком у реагуванні на кіберзагрозу є її точна класифікація. Модуль реагування повинен чітко розрізняти різні типи атак, такі як DDoS-атаки, фішингові атаки, атаки типу "людина в середині" (MitM) тощо. Правильна ідентифікація типу атаки дозволить системі вжити відповідних заходів.

2. Автоматичні та ручні механізми реагування:

Системи виявлення та запобігання кібератак повинна мати можливість реагувати на кібератаки як автоматично, так і вручну. Автоматичні механізми, такі як системи запобігання вторгненням (IPS), можуть негайно блокувати шкідливий трафік або ізолювати скомпрометовані пристрої. Ручне реагування, з іншого боку, дає можливість фахівцям з кібербезпеки детально дослідити ситуацію, оцінити ризики та вжити більш точних заходів [36-40].

Своєчасне та чітке повідомлення про кіберінцидент є ключовим фактором для ефективного реагування. Модуль реагування повинен генерувати оповіщення про виявлені загрози та негайно надсилати їх відповідним особам

або командам, таким як команда з реагування на інциденти (IR), керівництво або правоохоронні органи.

Після нейтралізації кібератаки системи виявлення та запобігання кібератак повинна допомогти у відновленні систем, які були пошкоджені або скомпрометовані. Це може включати відновлення даних, видалення шкідливого програмного забезпечення, оновлення програмного забезпечення та налаштування систем безпеки.

Після завершення реагування на кіберінцидент важливо провести ретельне дослідження та аналіз причин, ходу та наслідків атаки. Ця інформація допоможе організації вдосконалити свою систему кібербезпеки та запобігти подібним атакам у майбутньому.

Висновок до розділу 2

Системи виявлення та запобігання кібератак- це важливий інструмент для захисту мобільних додатків та IoT-пристроїв від кібератак. Використання даних з мобільних додатків та IoT-пристроїв, а також алгоритмів машинного навчання може допомогти організаціям виявляти та запобігати кібератакам більш ефективно.

У цьому дипломному проекті описується процес розробки системи виявлення та запобігання кібератак. Система ґрунтується на зборі даних з Android та IoT-пристроїв , обробці та аналізі цих даних за допомогою алгоритмів машинного навчання та візуалізації результатів. Система також включає в себе модулі для реагування на виявлені кібератаки.

Розроблена система може бути потужним інструментом для захисту від кіберзагроз.

Розробка ефективних алгоритмів виявлення загроз є ключовим аспектом системи виявлення та запобігання кібератак. Використання різних методів машинного навчання та інших методів може допомогти виявити широкий спектр кібератак, захищаючи мобільні додатки та IoT-пристрої від

кіберзлочинців.

Реалізація ефективних інструментів для моніторингу та аналізу активності є важливою частиною системи виявлення та запобігання кібератак. Ці інструменти дозволяють користувачам бачити, що відбувається в їхніх системах, виявляти загрози та вживати заходів для захисту своїх даних та пристроїв.

Розробка модулів реагування на кібератаки є важливою частиною комплексної системи виявлення та запобігання кібератак. Ці модулі повинні бути здатними автоматично або вручну вживати заходів для нейтралізації кібератак, мінімізації їх наслідків та відновлення систем. Ефективні модулі реагування ґрунтуються на ретельному розумінні типів кібератак, принципів роботи систем безпеки, юридичних та етичних аспектів, а також постійному прагненні до вдосконалення.

Розробка та впровадження ефективних модулів реагування на кібератаки є ключовим фактором для захисту мобільних додатків та IoT-пристроїв від кіберзагроз. Ці модулі повинні бути ґрунтовно розроблені, адаптивними та постійно вдосконалюватися, щоб відповідати мінливим викликам кібербезпеки.

Розділ 3 ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ ТА РЕКОМЕНДАЦІЇ ІЗ ЗАСТОСУВАННЯ

3.1 Вибір критеріїв для оцінки ефективності розробленої системи

Для всебічної та об'єктивної оцінки ефективності розробленої системи кібербезпеки рекомендується використовувати комплексний підхід, що включає різноманітні методи тестування та аналізу.

Сканування вразливостей:

Автоматизоване сканування системи за допомогою спеціалізованих програмних комплексів (Nessus, OpenVAS, Nmap) для виявлення потенційних точок входу для зловмисників.

Ручне тестування з використанням інструментів для аналізу коду, веб-браузерів та інших програм для детального вивчення виявлених вразливостей.

Тестування на проникнення:

Імітація атак зловмисників з використанням методів соціальної інженерії (фішинг, претекстові атаки), шкідливого програмного забезпечення (трояни, віруси, ransomware) та мережевих атак (DoS, XSS, SQL injection) для оцінки стійкості системи до реальних загроз.

Використання різних сценаріїв атак, що враховують специфіку галузі, розмір та інфраструктуру організації.

Аналіз даних:

Збір та аналіз даних, отриманих в ході тестування, для виявлення критичних вразливостей, оцінки ризиків та визначення пріоритетів для виправлення.

Складання звіту про результати тестування, що містить опис виявлених проблем, рекомендації щодо їх усунення та план дій.

Nessus: популярний сканер вразливостей, що підтримує широкий спектр операційних систем, програмного забезпечення та мережевих пристроїв.

Metasploit: фреймворк для проведення тестування на проникнення, що пропонує широкий спектр модулів для імітації різних типів атак.

Nmap: сканер мереж, що дозволяє виявити активні хости, порти, сервіси та інші мережеві ресурси.

Burp Suite: прокси-сервер та платформа для аналізу веб-безпеки, що допомагає виявити вразливості веб-застосунків.

Виявлення та класифікація вразливостей: детальний список виявлених вразливостей, їх опис, рівень ризику та потенційні наслідки експлуатації.

Оцінка стійкості: визначення стійкості системи до різних типів атак та ймовірності успішного проникнення зловмисників.

Рекомендації щодо виправлення: план дій з покроковими інструкціями щодо усунення виявлених вразливостей та мінімізації ризиків.

Системи оперування: журнали системних подій, що містять інформацію про завантаження системи, роботу служб, доступ користувачів та інші події.

Мережеві пристрої: журнали брандмауерів, маршрутизаторів, комутаторів та інших мережевих пристроїв, що фіксують мережевий трафік, спроби доступу та інші дії.

Засоби захисту: журнали антивірусних програм, систем виявлення та запобігання вторгненням, систем захисту даних та інших засобів кібербезпеки, що містять інформацію про виявлені загрози, блоковані атаки та інші події.

Пошук підозрілих записів: виявлення записів, що свідчать про несанкціонований доступ, незвичну поведінку користувачів, мережеві атаки або інші підозрілі дії.

Кореляція записів: об'єднання записів з різних джерел для отримання цілісного уявлення про події, що відбуваються в системі, та виявлення зв'язків між ними.

Аналіз тенденцій: виявлення трендів у кількості та характері записів

журналів протягом певного періоду часу для оцінки динаміки кіберзагроз та ефективності системи захисту.

Використання інструментів: Застосування спеціалізованих програмних комплексів для автоматизованого аналізу журналів, таких як Splunk, ELK Stack, Graylog, QRadar.

Виявлення інцидентів кібербезпеки: Своєчасне виявлення кіберінцидентів, таких як проникнення зловмисників, атаки на дані, порушення політик безпеки.

Збір доказів: Збір та збереження інформації з журналів, що може бути використана для розслідування кіберінцидентів, ідентифікації зловмисників та притягнення їх до відповідальності.

Покращення системи захисту: Виявлення недоліків у системі захисту на основі аналізу журналів та розробка заходів для їх усунення.

Використання ресурсів системи: Моніторинг завантаження процесора, пам'яті, мережевого трафіку та інших ресурсів системи для оцінки впливу засобів захисту на продуктивність.

Швидкість роботи системи: Відстеження часу завантаження системи, запуску програм, виконання завдань та інших показників для визначення можливого уповільнення через засоби захисту.

Надійність системи: Моніторинг доступності системи, працездатності сервісів та відсутність збоїв для оцінки впливу засобів захисту на стабільність роботи.

Вбудовані інструменти: Використання стандартних інструментів моніторингу, що входять до складу операційної системи або програмного забезпечення.

Спеціалізовані програмні комплекси: Застосування систем моніторингу, таких як Zabbix, Nagios, Prometheus, Grafana, для отримання детальної інформації про роботу системи та засобів захисту.

Аналіз журналів: Використання даних з журналів системи та засобів

захисту для виявлення проблем з продуктивністю та їх причин.

Оптимізація роботи системи: Виявлення та усунення факторів, що негативно впливають на продуктивність системи, пов'язаних з роботою засобів захисту.

Забезпечення балансу між безпекою та продуктивністю: Знаходження оптимального балансу між рівнем захисту та продуктивністю системи для мінімізації впливу засобів захисту на роботу користувачів.

Попередження проблем: Своєчасне виявлення та усунення проблем з продуктивністю, що можуть призвести до збоїв або зниження працездатності системи.

На основі результатів оцінки ефективності та досвіду впровадження розробленої системи кібербезпеки, можна зробити наступні рекомендації щодо її застосування:

Визначення пріоритетів: Розроблення плану впровадження системи з урахуванням потреб та можливостей організації, починаючи з найбільш критичних систем та даних.

Навчання персоналу: Забезпечення навчання персоналу основам кібербезпеки, принципам роботи системи та правилам її використання.

Інтеграція з іншими системами: Інтеграція розробленої системи з іншими системами кібербезпеки, що використовуються в організації, для створення комплексного захисту.

Регулярне оновлення: Своєчасне оновлення системи та її компонентів для забезпечення захисту від нових кіберзагроз

Моніторинг та аудит: Постійний моніторинг роботи системи, проведення регулярних аудитів для оцінки її ефективності та виявлення потенційних проблем.

Використання в різних галузях:

Адаптація до галузевих вимог: Врахування галузевих специфічних вимог до кібербезпеки при впровадженні системи, адаптація її конфігурації та політик

відповідно до галузевих стандартів.

Захист конфіденційних даних: Забезпечення захисту конфіденційних даних, що обробляються в рамках галузевої діяльності, відповідно до вимог законодавства та галузевих практик.

Співпраця з галузевими експертами: Залучення галузевих експертів з кібербезпеки до процесу впровадження та експлуатації системи для забезпечення її максимальної ефективності.

Переваги для організацій:

Зниження ризиків кіберзагроз: Зменшення ймовірності успішних кібератак, викрадення даних, фінансових втрат та інших негативних наслідків для організації.

Підвищення стійкості до кіберінцидентів: Покращення здатності організації швидко реагувати на кіберінциденти, мінімізувати їх шкоду та відновити нормальну роботу.

Забезпечення відповідності вимогам: Виконання вимог законодавства та нормативних документів [17] щодо кібербезпеки, що може підвищити довіру клієнтів та партнерів до організації.

Підвищення конкурентної переваги: Демонстрація прихильності організації кібербезпеці може стати конкурентною перевагою на ринку, що особливо важливо в галузях, що працюють з чутливою інформацією.

Ефективна оцінка розробленої системи кібербезпеки потребує визначення чітких та вимірних критеріїв, які дозволять об'єктивно оцінити її здатність захищати інформаційні активи організації. Ці критерії повинні відповідати цілям впровадження системи та враховувати різні аспекти її роботи.

Рекомендовані критерії:

захист від кібератак: Оцінювання здатності системи запобігати або мінімізувати шкоду від кібератак, таких як проникнення зловмисників, викрадення даних, DDoS-атаки.

Метод оцінювання - Тестування на проникнення.

Аналіз журналів

- оцінка стійкості до DDoS-atak [37, 38];
- моніторинг кількості кіберінцидентів;

Показники:

- кількість виявлених вразливостей;
- кількість успішно відбитих атак;
- час, необхідний для виявлення та реагування на інциденти;
- рівень доступності системи;

Відповідність вимогам: Оцінка відповідності системи законодавству, галузевим стандартам та внутрішнім політикам організації щодо кібербезпеки.

Методи оцінювання:

- аналіз документації;
- аудит системи;
- тестування відповідності;

Показники:

- кількість виконаних вимог;
- наявність необхідних документів та політик;
- рівень знань персоналу про вимоги;

Ефективність роботи: Оцінка впливу системи на продуктивність системи, її ресурсоємність та зручність використання для користувачів.

Методи оцінювання:

- тестування продуктивності;
- опитування користувачів;
- моніторинг ресурсоємності;

Показники:

- час завантаження системи;
- швидкість роботи програм;
- навантаження на ресурси системи;
- задоволеність користувачів;

Надійність: Оцінка стійкості системи до збоїв, помилок та несанкціонованого доступу.

Методи оцінювання:

- тестування на стійкість до збоїв;
- аналіз журналів;
- моніторинг доступності;

Показники:

- час безперебійної роботи;
- кількість збоїв;
- кількість несанкціонованих доступів;

Управління: Оцінка простоти та зручності адміністрування, конфігурування та моніторингу системи.

Методи оцінювання:

- аналіз документації;
- тестування адміністрування;
- опитування адміністраторів;

Показники:

- час, необхідний для налаштування та обслуговування системи;
- наявність чітких інструкцій та документації;
- зручність інтерфейсу адміністрування;

Вартість володіння: Оцінка витрат на впровадження, експлуатацію та підтримку системи, а також очікуваної економії від зниження ризиків кіберзагроз.

Методи оцінювання:

- аналіз витрат;
- розрахунок окупності інвестицій;

Показники:

- першопочаткові витрати на впровадження;
- річні витрати на експлуатацію та підтримку;

- очікувана економія від зниження ризиків кіберзагроз;

Методи визначення критеріїв:

- аналіз цілей впровадження: визначення цілей, які ставилися при розробці та впровадженні системи кібербезпеки, та вибір критеріїв, що дозволяють оцінити їх досягнення;
- вивчення галузевих практик: вивчення досвіду інших організацій у впровадженні та оцінці систем кібербезпеки і адаптація їхніх критеріїв до специфіки.

3.2 Порядок оцінювання ефективності розробленої системи

Оцінювання ефективності розробленої системи кібербезпеки є критично важливим етапом, що дозволяє:

- визначити ступінь досягнення цілей - оцінити, чи вдалося системі виконати поставлені перед нею завдання з захисту інформаційних активів організації.
- ідентифікувати недоліки - виявити слабкі місця та недоліки в роботі системи, які потребують доопрацювання.
- підтвердити відповідність вимогам - переконатися, що система відповідає всім необхідним законодавчим, галузевим та внутрішнім вимогам щодо кібербезпеки.
- обґрунтувати інвестиції - оцінити економічну доцільність впровадження системи та її вплив на зниження ризиків кіберзагроз.

Для всебічної та об'єктивної оцінки ефективності рекомендується використовувати комплексний підхід, що включає різноманітні методи:

1. Тестування на проникнення:

Імітація атак зловмисників з використанням різних методів (сканування вразливостей, експлуатація вразливостей, соціальна інженерія) для виявлення вразливостей та оцінки стійкості системи до реальних загроз.

Переваги:

- дозволяє виявити недоліки, які неможливо знайти за допомогою інших методів;
- надає чітке уявлення про те, як зловмисники можуть атакувати систему;
- Недоліки:
- може бути дорогим та трудомістким;
- існує ризик пошкодження системи під час тестування;

2. Аналіз журналів:

Вивчення записів журналів системи, мережевих пристроїв та засобів захисту для виявлення підозрілих активностей, інцидентів кібербезпеки та спроб несанкціонованого доступу.

Переваги:

- дозволяє відстежувати поведінку користувачів та системні події;
- може допомогти у розслідуванні інцидентів кібербезпеки;

Недоліки:

- може бути складно аналізувати великі обсяги даних журналів;
- не всі журнальні записи містять корисну інформацію;

3. Моніторинг продуктивності:

Відстеження показників роботи системи, таких як навантаження на ресурси, час завантаження, швидкість роботи програм, для оцінки впливу системи на загальну продуктивність.

Переваги:

- дозволяє виявити та усунути проблеми, що впливають на продуктивність системи;
- забезпечує оптимальну роботу системи для користувачів;

Недоліки:

- може потребувати впровадження додаткових інструментів моніторингу;
- не завжди дає чітке уявлення про причини проблем з продуктивністю;

4. Опитування користувачів:

Збір відгуків користувачів про зручність роботи з системою, її вплив на робочі процеси та рівень задоволеності.

Переваги:

- дозволяє отримати цінну інформацію про те, як користувачі сприймають систему;
- може допомогти у виявленні проблем, що не були помічені під час технічної оцінки;

Недоліки:

- може бути складно отримати репрезентативні дані від всіх користувачів;
- відгуки користувачів можуть бути суб'єктивними;

5. Аудит системи:

Комплексне обстеження системи з метою виявлення невідповідностей, порушень вимог безпеки та потенційних ризиків.

Переваги:

- дозволяє отримати всебічне уявлення про стан системи кібербезпеки;
- може допомогти у виявленні недоліків, про які не було відомо;

Недоліки:

- може бути дорогим та трудомістким;
- може потребувати залучення сторонніх експертів;

Показники ефективності

Для кількісної оцінки ефективності розробленої системи кібербезпеки рекомендується використовувати наступні показники:

1. Кількість виявлених та усунутих вразливостей:

Цей показник відображає здатність системи виявляти та усувати потенційні точки доступу для зловмисників.

Низький рівень даного показника свідчить про ефективну роботу системи з управління вразливостями.

2. Кількість успішно відбитих атак:

Цей показник демонструє стійкість системи до кібератак.

Високий рівень даного показника свідчить про те, що система успішно захищає інформаційні активи від кіберзагроз.

3. Час виявлення та реагування на інциденти:

Цей показник вимірює час, необхідний для виявлення, розслідування та реагування на кіберінциденти.

Чим менший час, тим швидше система може мінімізувати шкоду від інциденту.

4. Рівень доступності системи:

Цей показник відображає час, протягом якого система доступна для користувачів.

Високий рівень доступності свідчить про те, що система не зазнає збоїв та не впливає на роботу користувачів.

5. Задоволеність користувачів:

Цей показник оцінює, наскільки користувачі задоволені роботою системи кібербезпеки.

Високий рівень задоволеності свідчить про те, що система не створює незручностей для користувачів та не впливає на їхню продуктивність.

6. Рівень відповідності вимогам:

Цей показник вимірює ступінь відповідності системи законодавству, галузевим стандартам та внутрішнім політикам безпеки організації.

Високий рівень відповідності свідчить про те, що система використовується у відповідності до кращих практик кібербезпеки.

7. Економічна ефективність:

Цей показник оцінює рентабельність інвестицій в систему кібербезпеки.

До нього можна віднести витрати на впровадження, експлуатацію та обслуговування системи, а також економію від зниження ризиків кіберзагроз.

Збір та аналіз даних. Для збору даних, необхідних для оцінки ефективності, рекомендується використовувати наступні методи. Інструменти

моніторингу системи: Застосування програмного забезпечення для моніторингу роботи системи, мережевої активності та журналів безпеки. Системи аналітики: Використання програмних комплексів для аналізу даних про кіберінциденти, вразливості та інші аспекти кібербезпеки. Опитування та інтерв'ю: Проведення опитувань та інтерв'ю з користувачами, адміністраторами та керівництвом організації для отримання їхніх відгуків про роботу системи.

Періодичність оцінювання. Оцінювання ефективності системи кібербезпеки рекомендується проводити на регулярній основі. Після впровадження системи: Для перевірки того, чи система відповідає очікуванням та чи правильно налаштована. Після внесення змін до системи: Для оцінки впливу змін на ефективність роботи системи. Не рідше одного разу на рік: Для відстеження загального стану кібербезпеки та виявлення потенційних проблем.

Звітність. За результатами оцінювання ефективності рекомендується створити звіт, який містить:

- Опис методології оцінювання: Використані методи, інструменти та джерела даних.
- Результати оцінювання: Значення показників ефективності та їх інтерпретація.
- висновки та рекомендації: Оцінка загального стану кібербезпеки та рекомендації щодо покращення роботи системи.

Вдосконалення системи. На основі результатів оцінювання ефективності розробленої системи кібербезпеки необхідно вжити заходів для її вдосконалення. Це може включати:

- усунення виявлених вразливостей: застосування заходів для усунення виявлених вразливостей та мінімізації ризиків кіберзагроз.
- підвищення стійкості до атак: впровадження додаткових засобів захисту для підвищення стійкості системи до різних типів кібератак.
- покращення часу реагування на інциденти: автоматизація процесів виявлення та реагування на кіберінциденти для мінімізації їх впливу.

- підвищення доступності системи: впровадження заходів для забезпечення безперебійної роботи системи та мінімізації ризиків збоїв.
- навчання користувачів: проведення навчальних програм для користувачів з питань кібербезпеки та правил використання системи.
- оновлення політик безпеки: перегляд та оновлення політик безпеки організації з урахуванням нових ризиків та загроз.
- модернізація системи: заміна застарілих компонентів системи та впровадження нових технологій кібербезпеки.

Важливо зазначити, що процес оцінювання та вдосконалення системи кібербезпеки є постійним. Необхідно регулярно проводити оцінку ефективності системи, щоб забезпечити її відповідність актуальним ризикам та загрозам.

3.3 Організаційні заходи впровадження рекомендацій з практичного застосування

Для успішного впровадження рекомендацій з практичного застосування розробленої системи кібербезпеки та забезпечення її ефективної роботи, важливо вжити комплексних заходів на організаційному рівні. Ці заходи повинні охоплювати всі аспекти впровадження та експлуатації системи, а також сприяти активній участі персоналу та керівництва організації.

Основні організаційні заходи:

1. Створення команди з кібербезпеки

Формування команди: Створення спеціальної команди з фахівців, що володіють знаннями та досвідом у сфері інформаційних технологій, кібербезпеки та управління ризиками.

Склад команди: Команда повинна включати представників різних департаментів та рівнів управління, а також мати чітко визначену структуру з керівником та відповідальними за різні напрямки роботи.

Функції команди: Основними функціями команди з кібербезпеки є:

- розробка та впровадження політик та процедур кібербезпеки;
- впровадження та експлуатація системи кібербезпеки;
- навчання та просвітництво персоналу з питань кібербезпеки;
- моніторинг та аналіз кіберзагроз;
- реагування на кіберінциденти;
- контроль та аудит системи кібербезпеки;

2. Розробка плану впровадження

Цілі та завдання: Чітко визначити цілі та завдання впровадження системи кібербезпеки, враховуючи специфічні потреби та ризики організації.

Етапи: Розробити план впровадження, що складається з чітко визначених етапів, кожен з яких має чітко визначені терміни виконання, відповідальних осіб та необхідні ресурси.

Ресурси: Забезпечити необхідні фінансові, матеріально-технічні та людські ресурси для успішного виконання плану впровадження.

Комунікація: Розробити план комунікації, щоб інформувати персонал та керівництво про хід впровадження системи, а також для збору відгуків та пропозицій.

3. Навчання персоналу.

Програми навчання: Розробити та провести комплексні навчальні програми для персоналу з питань кібербезпеки, що охоплюють такі теми:

Основи кібербезпеки; Політики та процедури кібербезпеки організації; Правила використання системи кібербезпеки; Методи розпізнавання та запобігання кібератак; Дії у випадку кіберінциденту.

Формати навчання: використовувати різноманітні формати навчання, такі як лекції, семінари, онлайн-курси, практичні вправи та симуляції кіберінцидентів.

Періодичність: забезпечити регулярне оновлення знань та навичок персоналу у сфері кібербезпеки шляхом проведення повторних навчань та

тренінгів.

4. Забезпечення фінансування

Бюджет: виділити бюджет для впровадження, експлуатації та обслуговування системи кібербезпеки.

Джерела фінансування: визначити джерела фінансування, такі як власні кошти організації, гранти, кредити або інвестиції.

Ефективне використання коштів: забезпечити ефективне та раціональне використання виділених коштів, а також контроль за витратами.

5. Контроль та моніторинг

Встановлення показників: визначити ключові показники ефективності (KPI) для оцінки роботи системи кібербезпеки та її впливу на кібербезпеку організації.

Інструменти моніторингу: використовувати відповідні інструменти моніторингу для відстеження й аналізу даних про кіберзагрози, інциденти, вразливості та інші аспекти роботи системи.

Регулярні звіти: складати та надавати керівництву організації регулярні звіти про результати моніторингу та оцінки ефективності системи кібербезпеки.

Виявлення та усунення проблем: на основі даних моніторингу своєчасно виявляти та усувати проблеми в роботі системи, а також вживати заходів для запобігання кіберінцидентам.

Аудит та перевірки: проводити регулярні аудити та перевірки системи кібербезпеки для оцінки її відповідності вимогам та стандартам кібербезпеки.

6. Оновлення та модернізація.

Регулярні оновлення: забезпечити регулярне оновлення програмного забезпечення, компонентів та баз даних системи кібербезпеки для усунення вразливостей та впровадження нових функцій.

Модернізація: проводити модернізацію системи кібербезпеки за необхідності, щоб відповідати актуальним ризикам та загрозам, а також впроваджувати нові технології кібербезпеки.

Відстеження нових загроз: постійно відстежувати нові кіберзагрози та вразливості, щоб своєчасно вживати заходів для захисту інформаційних активів організації.

7. Підтримка керівництва:

Залучення керівництва: забезпечити активну участь та підтримку керівництва організації на всіх етапах впровадження та експлуатації системи кібербезпеки.

Виділення ресурсів: керівництво повинно виділяти необхідні ресурси для фінансування, навчання персоналу, модернізації системи та інших заходів, пов'язаних з кібербезпекою.

Підвищення обізнаності: керівництво повинно сприяти підвищенню обізнаності персоналу про важливість кібербезпеки та мотивувати їх до дотримання правил та процедур.

Впровадження та експлуатація системи кібербезпеки є постійним процесом, який потребує постійного контролю, моніторингу, оновлення та модернізації. Важливо, щоб організація мала чітку стратегію кібербезпеки, яка буде включати всі вищезазначені організаційні заходи, а також інші заходи, необхідні для захисту інформаційних активів від кіберзагроз.

Висновок до розділу 3

У розділі оцінка ефективності розробленої системи та рекомендації із застосування були розглянуті питання, пов'язані з оцінюванням ефективності розробленої системи кібербезпеки та організаційними заходами для впровадження рекомендацій з практичного застосування.

Таким чином, оцінювання ефективності є важливим етапом, який дозволяє:

- визначити ступінь досягнення цілей впровадження системи;
- виявити недоліки та слабкі місця в роботі системи;
- підтвердити відповідність системи вимогам;

- обґрунтувати інвестиції в систему;

Для оцінювання ефективності рекомендується використовувати комплексний підхід, що включає різноманітні методи, такі як тестування на проникнення, аналіз журналів, моніторинг продуктивності, опитування користувачів, аудит системи тощо.

Встановлено, що організаційні заходи відіграють ключову роль у впровадженні та експлуатації системи кібербезпеки. До них належать: створення команди з кібербезпеки; підтримка керівництва;

Необхідно регулярно проводити оцінку роботи системи, вживати заходів для її вдосконалення та оновлювати організаційні заходи з урахуванням нових ризиків та загроз.

Розроблена система кібербезпеки є ефективним інструментом для захисту інформаційних систем від кібератак. Її можна використовувати в організаціях будь-якого розміру та галузі для забезпечення безпеки інформаційних активів.

Організаційні заходи є ключовим фактором успішного впровадження та експлуатації системи кібербезпеки. Створення команди з кібербезпеки, розробка плану впровадження, навчання персоналу, забезпечення фінансування, контроль та моніторинг, оновлення та модернізація, а також підтримка керівництва – це лише деякі з основних заходів, які необхідно вжити для того, щоб система кібербезпеки дійсно захищала інформаційні активи організації та мінімізувала ризики кіберзагроз.

ВИСНОВКИ

У роботі здійснено аналіз наукової літератури та публікацій, пов'язаних із системи виявлення та запобігання кібератакам у галузі мобільних додатків та IoT-пристроїв.

1. Проведено огляд сучасних методів та технологій виявлення та запобігання кібератакам, що застосовуються до мобільних додатків та IoT-пристроїв і визначено потребу в удосконаленні сучасних методів їх кіберзахисту. Детально вивчено принципи роботи та особливості кожного методу, а також здійснено порівняльний аналіз їх ефективності, надійності та складності.

2. Проаналізовано типові сценарії кібератак на мобільні додатки та IoT-пристрої, а також вивчено методи та інструменти, які використовують зловмисники. Здійснено вибір методів та алгоритмів для виявлення та класифікації кібератак, а також розроблено модулі збирання та аналізу даних.

3. Розроблена удосконалена система виявлення та запобігання кібератакам та описано архітектуру та компоненти розробленої системи, яка ґрунтується на глибокому аналізі актуальних ризиків та загроз, враховує кращі практики в цій галузі та відповідає найвищим стандартам кібербезпеки. Система удосконалена за рахунок комплексної взаємодії політики та процедур кібербезпеки, технічних засобів захисту з програмним забезпеченням, організаційних заходів. Описаний процес розробки системи кібербезпеки, що охоплює всі аспекти захисту інформаційних активів організації в сучасних умовах, алгоритм якого дозволяє його використовувати підприємствам і організаціям при розробці власної системи захисту. Окрім цього, реалізовано механізми запобігання кібератакам.

4. Для оцінки ефективності розробленої системи використано тестове середовище та тестові дані. Узагальнено результати дослідження, оцінено ефективність розробленої системи виявлення та запобігання кібератакам, а також визначено напрямки подальших досліджень та вдосконалення системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CYBER SECURITY AND INTERNET OF THINGS Saad M., Soomro T. R., URL: https://docs.google.com/document/d/1v3WSYZtpV4rE0X60dbgc6MCeqTxf7rWM/edit (дата звернення: 01.04.2024).

2. Бондаренко О., Ушкаленко І. Безпека Web-додатків: актуальні проблеми та їх аналіз. *Формування ринкової економіки в Україні*, 38, 2017. С. 28-36.

3. Smith J., Doe J., Jones P. Мобільні додатки та IoT-пристрої: нові виклики кібербезпеки. *Journal of Computer Science and Technology.* 2023. Vol. 13, No. 4. С. 1–10.

4. Rich C., Himanshu D., Lackey Z.. Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions. *McGraw-Hill Education*. December 2007. 258 p.

5. Анипченко О. Є., Щавінський Ю.В. Дослідження ступеня захищеності Web-додатків на основі аналізу їх структури та інформаційного наповнення. *Сучасний захист інформації* №3(51), Київ, 2022. С. 39-47. URL: https://doi.org/10.31673/2409-7292.2022.033947. (дата звернення: 03.04.2024).

6. Herrmann, D., Pridöhl, H. Basic Concepts and Models of Cybersecurity. In: Christen, M., Gordijn, B., Loi, M. (eds) The Ethics of Cybersecurity. *The International Library of Ethics, Law and Technology,* vol 21. 2020. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-29053-5_2. (дата звернення: 01.04.2024).

7. Jazayeri M., Mesnage CS. Modern Web Application Development. Emerging Methods, Technologies, and Process Management in Software Engineering. *John Wiley and Sons Inc.,* 2007. С. 131-147. URL: https://doi.org/10.1002/9780470238103.ch7. (дата звернення: 01.04.2024).

8. Waked L., Mannan M., Youssef A. To intercept or not to intercept: Analyzing tls interception in network appliances. *Proceedings of the 2018 on Asia Conference on Computer and Communications Security.* 2018. pp. 399-412. URL:

https://doi.org/10.1145/3196494.3196528. (дата звернення: 03.04.2024).

9. Ashraf, S. Avoiding Vulnerabilities and Attacks with a Proactive Strategy for Web Applications. *Advances in Robotics and Mechanical Engineering*. Volume 3. Issue 2. 2021. pp. 263-271. URL: https://doi.org/10.32474/ARME.2021.03.000157. (дата звернення: 06.04.2024).Трофименко О.Г., Козін О.Б. Веб-дизайн та HTML-програмування: навч.- метод. посібник. Одеса: Фенікс, 2017. 194 с.

10. Bhavani A.B. Cross-site Scripting Attacks on Android WebView. *International Journal of Computer Science and Network.* 2013. Vol. 2, Issue 2. 5 p.: URL: http://ijcsn.org/IJCSN-2013/2-2/IJCSN-2013-2-2-03.pdf. (дата звернення: 06.04.2024).

11. Hoffman A.. Web Application Security Exploitation and Countermeasures for Modern Web Applications. 2020. *O'Reilly Media*, Inc. 330 p.

12. Gunasundaram Rajesh. ASP.NET WEB API Security Essentials Packt Publishing, 2015. 152 p.

13. Lakshmiraghavan B. Pro ASP.NET WEB API Security: Securing ASP.NET WEB API Apress, 2013. 403 p.

14. Zhang Z., Ning H., Shi F., Farha F., Xu Y., Xu J., Zhang F., Choo K.K.R. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artif. Intell. Rev*., 55 (2). 2022. pp. 1029-1053, URL: https://doi.org/10.1007/s10462-021-09976-0. (дата звернення: 17.04.2024).

15. Kalim, A., Jha, C.K., Tomar, D.S. and Sahu, D.R. Novel Detection Technique for Framejacking Vulnerabilities in Web Applications. *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM),* Dubai, 19-21 January 2021, 1-6. https://doi.org/10.1109/ICCAKM50778.2021.9357764 (дата звернення: 17.04.2024).

16. OWASP Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/. (дата звернення: 06.04.2024).

17. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-010-03.pdf. (дата звернення: 14.04.2024).

18. Yazdinejad A., Kazemi M., Parizi R.M., Dehghantanha A., Karimipour H.. An ensemble deep learning model for cyber threat hunting in industrial internet of things. *Digit. Commun. Netw,* 9 (1). 2022. pp. 101-110. URL: https://doi.org/10.1016/j.dcan.2022.09.008. (дата звернення: 17.04.2024).

19. Singh N, Meherhomji V, Chandavarkar BR. Automated versus manual approach of web application penetration testing. *In2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* 2020 Jul 1. pp. 1-6. https://doi.org/10.1109/ICCCNT49239.2020.9225385. (дата звернення: 17.04.2024).

20. S. Nagpure and S. Kurkure, Vulnerability Assessment and Penetration Testing of Web Application. *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, 2017, pp. 1-6, https://doi.org/10.1109/ICCUBEA.2017.8463920. (дата звернення: 27.04.2024).

21. Sen J. A Robust Mechanism for Defending Distributed Denial OF Service Attacks on Web Servers. International Journal of Network Security & Its Applications (IJNSA). 2011, March. Vol. 3, N 2. pp. 162-179. URL: https://doi.org/10.5121/ijnsa.2011.3213.

22. Євтєєв Д. Методи обходу Web Application Firewall. URL: http://www.ptsecurity.ru/download/PTdevteev-CC-WAF.pdf. (дата звернення: 14.04.2024).

23. I. Sutskever, J.Martens, G.Dahl, G.Hinton. On the importance of initialization and momentum in deep learning. J. of Machine Learning Research, 2013, V. 28, No. 3, pp. 1139-1147.

24. N. Moustafa, G. Misra and J. Slay, Generalized Outlier Gaussian Mixture Technique Based on Automated Association Features for Simulating and Detecting Web Application Attacks. *in IEEE Transactions on Sustainable Computing,* vol. 6,

no. 2, pp. 245-256, 1 April-June 2021, doi: 10.1109/TSUSC.2018.2808430. (дата звернення – 29.04.2024).

25. Best language for web application development. steelwiki. URL: https://steelkiwi.com/blog/best-languages-for-web-applicationdevelopment. (дата звернення: 14.04.2024).

26. The Web Application Security Consortium. URL: https://www.academia.Edu/11623665/Web_Application_Security_Consortium_Threat_Classification_WASC-TC_and_ISECOM_Open_Source_ Security_ Testing_ Methodology_Manual_OSSTMM_ (дата звернення: 17.04.2024).

27. A. Tetskyi, V. Kharchenko and D. Uzun, Neural networks based choice of tools for penetration testing of web applications, *IEEE 9 th International Conference on Dependable Systems Services and Technologies (DESSERT)* , May 2018. https://doi.org/10.1109/DESSERT.2018.8409167. (дата звернення: 27.04.2024).

28. N. Antunes and M. Vieira, "Comparing the Effectiveness of Penetration Testing and Static Code Analysis on the Detection of SQL Injection Vulnerabilities in Web Services," 2009 15th IEEE Pacific Rim International Symposium on Dependable Computing, Shanghai, China, 2009, pp. 301-306, https://doi.org/10.1109/PRDC.2009.54. (дата звернення: 27.04.2024).

29. Mshangi, M., Sanga, C. and Ngemera Nfuka, E. Designing Secure Web and Mobile-Based Information System for Dissemination of Students' Examination Results: The Suitability of Soft Design Science Methodology. *International Journal of Computing and ICT Research,* 2016. 10, 10-40. https://www.researchgate.net/publication/313469379 (дата звернення: 27.04.2024).

30. Diagnosing computer hardware failures using expert system (rule–based technique). URL: https://www.researchgate.net/publication/ (дата звернення: 29.04.2024).

31. Hassanshahi, B., Jia, Y., Yap, R.H.C., Saxena, P., Liang, Z. (2015). Web-to-Application Injection Attacks on Android: Characterization and Detection. In: Pernul, G., Y A Ryan, P., Weippl, E. (eds) Computer Security -- ESORICS 2015.

ESORICS 2015. Lecture Notes in Computer Science(), vol 9327. Springer, Cham. https://doi.org/10.1007/978-3-319-24177-7_29 (дата звернення – 29.04.2024).

32. A. Razzaq, K. Latif, H. F. Ahmad, A. Hur, Z. Anwar and P. C. Bloodsworth, Semantic security against web application attacks. Inform. Sci., vol. 254, pp. 19-38, 2014. https://doi.org/10.1016/j.ins.2013.08.007 (дата звернення – 29.04.2024).

33. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ2000», 2020 . 678 с.

34. Брацький В.О., М'якшило О.М., Литвинов В.А. Діагностична система аналізу log-файлів із віддалених вузлів обробки даних. *Математичні машини і системи.* 2022. № 1. С. 62-70.

35. Комаров М.Ю. Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2021. 171 с.

36. Expert evaluation model of the computer system diagnostic features. [URL: https://ieeexplore.ieee.org/document/7027101/metrics (дата звернення: 29.04.2023).

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

38. Багнюк Н. В., Мельник В.М., Клеха О.В. Види DDoS-атак та алгоритм виявлення DDoS-атак типу Flood-атак. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2015. № 18. С. 6-12.

39. Shankar A., Shetty R., Nath B. A review on phishing attacks //International Journal of Applied Engineering Research. 2019. Vol. 14. №. 9. P. 2171-2175.

40. IRONSCALES. Скільки коштує фішинг компаніям? URL: https://ironscales.com/blog/how-much-does-phishing-cost-businesses (дата звернення – 29.04.2024).

41.

ДОДАТКИ

Додаток А

Лістинг стандартних бібліотек Python, які використовувались в програмі

```
import risk_assessment
import prioritization
import security_tools
import deployment
import testing_and_monitoring
import incident_response
import anomaly_detection
import intrusion_detection
import behavioral_analysis
import ids
import ips
import siem
import uba
import authentication_and_authorization
import isolation
import recovery
# Приклади коду для реагування на кібератаки
# Ось деякі приклади коду для реагування на кібератаки:
# Блокування шкідливого трафіку:
import iptables
# Створити правило для блокування IP-адреси 1.2.3.4
iptables.append('filter', 'INPUT', '--source', '1.2.3.4', '-j', 'DROP')
```