НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: **Методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів**

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-91

Подус Олексій Сергійович _____
(підпис)

Керівник: д.т.н., професор каф. ІБ, заслужений діяч Даник Ю.Г. _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент: доцент каф. ММЗІ ФТІ, Хмельницький М.О. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2023 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2023 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Подусу Олексію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів».
Керівник роботи: д.т.н., професор каф. ІБ, заслужений діяч Даник Ю.Г.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету №2028 - с від «26» травня 2023 р.

2. Термін подання здобувачем вищої освіти роботи «15» червня 2023 р.

3. Вихідні дані до роботи : Інформаційні джерела та роботи за темою дослідження

4. Зміст роботи: аналіз існуючих механізмів захисту персональних даних в мобільних додатках та гаджетах для запобігання наявності вразливостей і шляхів їх запобігання.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Презентація

6. Перелік публікацій: Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення». (Випуск 77)

7. Дата видачі завдання 05.01.2023

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1.	Отримання завдання на дипломну роботу	05.01.2023	виконано
2.	Дослідження літератури за темою	25.01.2023 – 27.02.2023	виконано
3.	Робота над першим розділом	04.03.2023 – 21.03.2023	виконано
4.	Робота над другим розділом	22.03.2023 – 28.04.2023	виконано
5.	Робота над третім розділом	03.05.2023 - 20.05.2023	виконано
6.	Аналіз результатів	21.05.2023 – 28.05.2023	виконано
7.	Оформлення дипломної роботи та доробка недоліків	29.05.2023 – 14.06.2023	виконано

Здобувач вищої освіти _____ Олексій, ПОДУС
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

Керівник роботи _____ Юрій, ДАНИК
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Дипломна робота складається з 3 розділів, містить 31 ілюстрацію, 1 додаток та 25 літературних джерел, загальний обсяг роботи – 81 сторінка.

Мета роботи - розробка методу, що дозволяє виявляти несанкціонований доступ до мобільних гаджетів з використанням динамічного аналізу та зробити оцінку даного методу за розробленими критеріями

Метод дослідження - аналіз існуючих механізмів захисту персональних даних в мобільних додатках та гаджетах для запобігання наявності вразливостей і шляхів їх запобігання.

Наукова новизна дослідження полягає в тому, що представлено методи виявлення несанкціонованого доступу до мобільних гаджетів, методи удосконалення системи безпеки, розроблено критерії для оцінки ефективності методів, оцінено, реалізований програмно, метод динамічного виявлення несанкціонованого доступу до мобільного гаджету.

Ключові слова: мобільний гаджет, метод виявлення, несанкціонований доступ, оцінка ефективності.

ABSTRACT

The work consists of 3 chapters, 31 illustrations, 1 appendix, and 25 references, the total volume of the work is 81 pages.

The purpose of the work - is to develop a method that allows for the detection of unauthorized access to mobile devices using dynamic analysis and to evaluate this method based on the developed criteria.

Research method – involves analyzing existing mechanisms for protecting personal data in mobile applications and devices to prevent vulnerabilities and their mitigation.

The scientific novelty of the research lies in the presentation of methods for detecting unauthorized access to mobile devices, methods for improving security systems, the development of criteria for evaluating the effectiveness of the methods, and the implementation and evaluation of a dynamic method for detecting unauthorized access to mobile devices.

Keywords: mobile device, detection method, unauthorized access, effectiveness evaluation

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

USI - Unauthorized Access to Information

НРД - Несанкціоноване Розповсюдження Даних

ІС - Інформаційна Система

ІБ - Інформаційна Безпека

АІТУ - Автоматизована Інформаційна Технологія Управління

ПІ - Персональна Інформація

VPN - Virtual Private Network

ПЗ - Програмне забезпечення

VLAN - Virtual Local Area Network

ASLR - Address Space Layout Randomization

OTP - One-Time Password

ADB – Android Debug Bridge

ВСТУП

Актуальність роботи. Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але крім зручності та безлічі технологічних можливостей, вони несуть у собі все більше небезпек. Одним із головних питань сучасного ринку мобільних продуктів є безпека додатків і особистих даних користувачів. Проблема починається зі звичайного використання особистих даних, таких як особисті вподобання, біометричні дані, приватні фотографії, які використовуються програмами, і навіть прихованого відстеження геометричних даних, тобто мобільного місцезнаходження користувача. По всьому світу відбувається викрадення, а в гіршому випадку – продаж великих баз даних електронних адрес для масової реклами – «спаму». Тому тема дипломного проекту «Методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів» є значущою для населення в цілому

Мета і завдання дослідження. розробка методу, що дозволяє виявляти несанкціонований доступ до мобільних гаджетів з використанням динамічного аналізу та зробити оцінку даного методу за розробленими критеріями

Об'єктом дослідження є мобільні застосунки та гаджети

Предметом дослідження є інструменти, правила та вказівки щодо захисту мобільних пристроїв.

Методи дослідження. В роботі включений детальний аналіз існуючих механізмів захисту персональних даних в мобільних додатках та гаджетах для запобігання наявності вразливостей і шляхів їх запобігання.

Наукова новизна отриманих результатів полягає в тому, що представлено методи виявлення несанкціонованого доступу до мобільних гаджетів, методи удосконалення системи безпеки, розроблено рекомендації та критерії для оцінки ефективності методів, оцінено реалізований програмно метод динамічного виявлення несанкціонованого доступу до мобільного гаджету

Апробація результатів роботи

Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення». (Випуск 77)

1 ТЕОРЕТИКО-МЕТОДИЧНІ АСПЕКТИ ФОРМУВАННЯ МОБІЛЬНИХ ЗАСТОСУНКІВ ТА ГАДЖЕТІВ

1.1 Поняття несанкціонованого доступу до інформації

Сучасні мобільні пристрої та гаджети забезпечують нам доступ до безлічі корисної інформації, але водночас стають об'єктом потенційних кібератак. Несанкціонований доступ до інформації є процесом здобування доступу до інформації без дозволу власника цієї інформації. Такий доступ може статися через використання шкідливих програм, злочинну діяльність, використання слабких точок безпеки і т.д.

У сучасному світі мобільні пристрої стали необхідними помічниками в повсякденному житті. Вони використовуються для зберігання великої кількості особистої інформації, такої як контакти, повідомлення, фотографії, відео та інші дані. Проте ця інформація може бути небезпечна в разі несанкціонованого доступу до неї з боку зловмисників.

Це може статися через використання різноманітних методів, таких як віруси, шпигунський софт, фішингові сайти, технічні вразливості і т.д. Якщо зловмисники отримають доступ до інформації, то вони можуть використовувати її для вчинення злочинів, таких як шахрайство, викрадення особистих даних та інших злочинів, пов'язаних з кібербезпекою.

Подібним чином несанкціонований доступ іноді називають отриманням доступу до інформації, коли особа має право на доступ до інформації в більшому обсязі, ніж це необхідно для виконання службових обов’язків[1].

Рисунок 1.1 – Класифікація загроз несанкціонованого доступу

Несанкціонований доступ до інформації (Unauthorized Access to Information (USI)) – доступ до інформації, який порушує правила обмеження доступу за допомогою звичайних засобів, наданих комп'ютерним обладнанням або автоматизованими системами[2].

Причини несанкціонованого доступу до інформації[2]:

- Помилка конфігурації

- Слабка безпека статутних фондів (викрадені паролі, смарт-карти, фізичний доступ до погано захищених пристроїв, доступ до незаблокованих робочих місць співробітників за їх відсутності)

- Помилки програмного забезпечення

- Зловживання службовим становищем (викрадення резервних копій, тиражування інформації на зовнішні носії з доступом до інформації)

- Прослуховування каналів зв'язку під час використання незахищеного з'єднання в локальній мережі

- Видання за допомогою клавіатурних шпигунів, вірусів і троянських програм на комп'ютерах співробітників.

З розвитком технологій обробки інформації методи несанкціонованого доступу до інформації стали поширеними. Найбільш популярними стали такі методи[3]:

- Робота між мережами - підключення до ліній зв'язку та використання прогалин у роботі законних користувачів у комп'ютерних системах.

- «Відмова в обслуговуванні» - несанкціоноване використання комп'ютерної системи у власних цілях (наприклад, для безкоштовного вирішення власних завдань), або для того, щоб система не відмовляла в обслуговуванні іншим користувачам. Для досягнення цього зловживання використовуються так звані «жадібні програми» — програми, здатні монополізувати певні системні ресурси.

- Повторне використання об’єктів — включає відновлення та повторне використання віддалених системних об’єктів. Прикладом такого зловживання є видалення файлів операційною системою. Коли операційна система видає повідомлення про те, що файл видалено, це не означає, що інформація, яка міститься в цьому файлі, була буквально пошкоджена. Інформація в цьому блоці не зникне, доки в це місце не буде записана інша інформація. Одним із видів повторного використання об’єктів є використання комп’ютерного «сміття».

- Маскування – зловмисник входить у систему, використовуючи відому особу законного користувача.

- «Підкладання свині» — зловмисники підключаються до ліній зв’язку та імітують роботу системи для незаконних операцій. Наприклад, він може видати себе за законного користувача, щоб імітувати сеанс зв’язку та отримати дані.

- Аналіз трафіку – зловмисники аналізують, як часто та як користувачі звертаються до системи. У той же час можна з'ясувати правила для вхідних повідомлень і потім спробувати достукатися до підтипів легітимних користувачів.

- «Роздягачі» - комплекс спеціально розроблених програмних засобів, орієнтованих на дослідження механізмів захисту програмних продуктів від НРД та їх подолання.

Розвиток засобів зв'язку та електронної пошти висвітлив зловживання, відоме в літературі як "пінг". Природа цього зловживання полягає в тому, що за допомогою стандартних або спеціально розроблених програмних засобів зловмисник може вимкнути адресу електронної пошти, бомбардуючи її потоком поштових повідомлень. Наслідками використання цієї утиліти можуть стати ускладнення та ймовірність ненавмисного ігнорування вхідних листів.

Слід зазначити, що в міру планування та розвитку зловживань зловмисники можуть створювати нові зловживання, не перераховані в цій класифікації, а також застосовувати будь-яку комбінацію описаних зловживань.

Інформаційна загроза - реалізація передбачуваного небезпечного впливу на інформаційну систему. За характером виникнення його можна розділити на 2 види: Навмисні і ненавмисні[4].

Ненавмисні загрози – це випадкові дії, які проявляються у вигляді недостатньої підтримки або неправильного керування механізмами захисту. Навмисне — це несанкціонований доступ до інформації та несанкціоноване маніпулювання даними, ресурсами та самою системою[5].

Залежно від типу реалізації загрози розрізняють: програмні; непрограмні.

Програмне забезпечення включає ті, які реалізовані як частина програмного забезпечення у вигляді окремих програмних модулів. До непроцесуальних належать зловживання, засновані на підготовці та вчиненні комп’ютерних злочинів з використанням технічних засобів інформаційних систем (ІС) (наприклад, несанкціоноване підключення до мереж зв’язку, використання спеціального обладнання для запису інформації тощо).

Для досягнення різноманітних цілей зловмисники використовують широкий спектр програмних засобів. Виходячи з цього, представляється можливим розділити програмні засоби на дві групи: тактичні та стратегічні.

Тактика включає досягнення найближчої мети (наприклад, отримання паролів, знищення даних тощо). Вони часто використовуються для підготовки та реалізації стратегічних заходів, спрямованих на досягнення далекосяжних цілей і пов'язані з величезними фінансовими втратами для ІБ. До групи стратегій входять інструменти, які реалізовані для забезпечення контролю над операціями технології перетворення інформації, що впливають на функціональність компонентів ІБ.

Програмні засоби, які можуть бути використані при перетворенні інформації [5]:

- довільне спотворення, блокування та/або заміна масивів інформації, що виводяться в зовнішню пам'ять або канали зв'язку внаслідок виконання програми, або масивів даних, які вже є в зовнішній пам'яті.
- приховування ознак особистої присутності в програмному середовищі мобільного пристрою;
- знищувати (довільно спотворювати) програмний код в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в певних областях з прямим доступом до зовнішньої пам'яті (локальної або віддаленої);
- володіти здатністю копіювати себе, асоціювати з іншими програмами та/або переносити свої фрагменти в інші операційні області або зовнішню пам'ять.

Розглянувши основні способи та види несанкціонованого доступу, звернемося до визначення моделі порушника, що виконує описані вище дії.

Розробка моделі порушника залежить від: 1) припущень щодо категорій людей, до яких може належати порушник; 2) припущень щодо мотивації поведінки порушника (цілей, які переслідує порушник); 3) припущень щодо кваліфікації порушника та його технічне оснащення (способи та засоби вчинення порушення); 4) обмеження та припущення щодо характеру можливих дій порушника.

Щодо автоматизованої інформаційної технології управління (АІТУ), правопорушники є інсайдерами (серед системних людей) або аутсайдерами (чужими). Внутрішнім порушником може бути особа таких категорій персоналу[6]:

- користувачі системи (оператори);

- Персонал, що обслуговує технічне обладнання (інженери, техніки);

- Співробітники відділів розробки та підтримки програмного забезпечення (прикладні та системні програмісти);

- Технічні працівники, що обслуговують будівлі (прибиральники, електрики, сантехніки та інші працівники, які мають доступ до будівель і приміщень, де розташовані компоненти АІТУ);

- Співробітники відділу охорони АІТУ;

- Менеджери на різних посадових рівнях.

Рисунок 1.2 – Класифікація способів несанкціонованого доступу до ПІ

Треті особи, які є зовнішніми порушниками: клієнти (представники організацій, громадяни); відвідувачі (запрошені неспроста); представники конкуруючих організацій (іноземних спецслужб) або особи, що діють від їх імені; особа, яка випадково або навмисно порушує пропускний режим (без мети порушення безпеки АІТУ); будь-хто за межами контрольованої території.

Рисунок 1.3 – Потенційні загрози і канали витоку ПІ

Можна виділити три основні причини порушень[8]:

а) безвідповідальність;

б) самоствердження;

в) егоїстичні інтереси.

У разі порушень через безвідповідальність, будь-яка деструктивна дія, здійснена навмисно чи ненавмисно користувачем, але не пов'язана зі зловмисним умислом. У більшості випадків це відбувається через некомпетентність або недбалість.

Деякі користувачі вважають отримання доступу до наборів даних системи величезним успіхом, починаючи гру в самоствердження «користувач проти системи» як у власних очах, так і в очах своїх колег.

Порушення безпеки з боку АІТУ також є наслідком власних інтересів користувачів системи. У цьому випадку він буде цілеспрямовано намагатися обійти систему захисту, щоб отримати доступ до інформації, яка зберігається, передається та обробляється в АІТУ. Навіть якби АІТУ мав засоби, щоб надзвичайно ускладнити цей вид проникнення, повністю захистити його від проникнення було б практично неможливо. Усіх правопорушників можна класифікувати за чотирма параметрами.

Знання про АІТУ відрізняє порушників[9]:

· Люди, які знають функціональні характеристики АІТУ, основні правила формування масиву даних і потоку запитів, а також як використовувати стандартні засоби;

· Високий рівень знань і досвіду використання технічних засобів систем та їх обслуговування;

· Володіти високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем;

· Розуміти будову, функції та механізм дії засобів захисту, а також їх переваги та недоліки.

Залежно від рівня компетенції (використаних методів і засобів) правопорушники можуть:

· Отримувати інформацію, використовуючи суто проксі-підхід;

· Використовувати пасивні методи (методи технічного перехоплення, які не модифікують компоненти системи);

· подолання лише звичайними засобами та недоліками систем захисту (несанкціоновані дії з використанням санкціонованих засобів), а також компактними магнітними носіями інформації, які можна таємно переносити через пости охорони;

· Використання методів і засобів активного впливу (модифікація і підключення додаткових механічних пристроїв, підключення каналів передачі

даних, впровадження програмних «закладок» і використання спеціальних приладів і технічних процедур).

Порушників розрізняють за часом дії:

· Під час роботи АІТУ (при роботі компонента системи);

· У періоди простою компонентів системи (у неробочий час, під час планових припинень роботи, відключень на технічне обслуговування та ремонт тощо);

· Під час роботи АІТУ та в період простою компонентів системи.

При цьому можуть розглядатися такі обмеження та припущення щодо характеру поведінки можливого порушника:

· Вербування та спеціальні заходи ускладнюють формування коаліцій правопорушників, тобто єдиних і цілеспрямованих дій для подолання двох і більше захисних підсистем порушників;

· Злочинець планує спробу несанкціонованого доступу до інформації з метою приховування своєї протиправної діяльності від інших співробітників;

· Несанкціонований доступ до інформації може бути наслідком помилок користувачів, адміністраторів, операторів і обслуговуючого персоналу, а також через відсутність визнаних методів обробки інформації.

Визначення точного значення характеристик ймовірного порушника значною мірою суб'єктивне. Модель порушника, побудовану з урахуванням специфіки конкретної предметної області та технології обробки інформації, можна представити перерахуванням кількох варіантів її появи. Кожен тип злочинця повинен характеризуватися власними значеннями, наведеними вище.

1.2 Конфіденційність даних мобільних пристроїв

Конфіденційність даних мобільних пристроїв стає все більш необхідним сегментом в нашому світі, бо мобільні телефони стали не тільки засобом зв'язку, але й незамінними інструментами для роботи, навчання та розваг. З одного боку, мобільні пристрої дозволяють людям бути підключеними та інформованими у

будь-який час і в будь-якому місці, а з іншого - вони зберігають значну кількість особистих даних, які скомпрометовані, якщо зловмисники отримають до них доступ.

Один з основних аспектів конфіденційності даних мобільних пристроїв - це захист від несанкціонованого доступу до даних користувача. На сьогоднішній день, мобільні пристрої мають велику кількість різноманітних захистів, таких як підтвердження особистості, використання паролів та відбитків пальців. Однак, незважаючи на це, зловмисники знаходять способи обходу захистів та використовують вразливості програмного забезпечення для отримання доступу до даних користувачів[10].

Ще одним важливим аспектом конфіденційності даних мобільних пристроїв є захист від небажаного збору даних користувачів. Зараз, більшість програм та додатків на мобільних пристроях збирають деякі дані про користувачів, що може бути використано для персоналізації реклами або продажу даних третім сторонам. Однак, є певні норми та правила, які забороняють збір деяких особистих даних користувачів без їх згоди.

Існує також проблема зберігання даних в хмарних сервісах. Більшість мобільних пристроїв мають можливість зберігати дані в хмарній пам'яті, що забезпечує зручний доступ до даних з будь-якого місця та з будь-якого пристрою. Однак, це також створює ризик викрадення та компрометування даних користувачів.

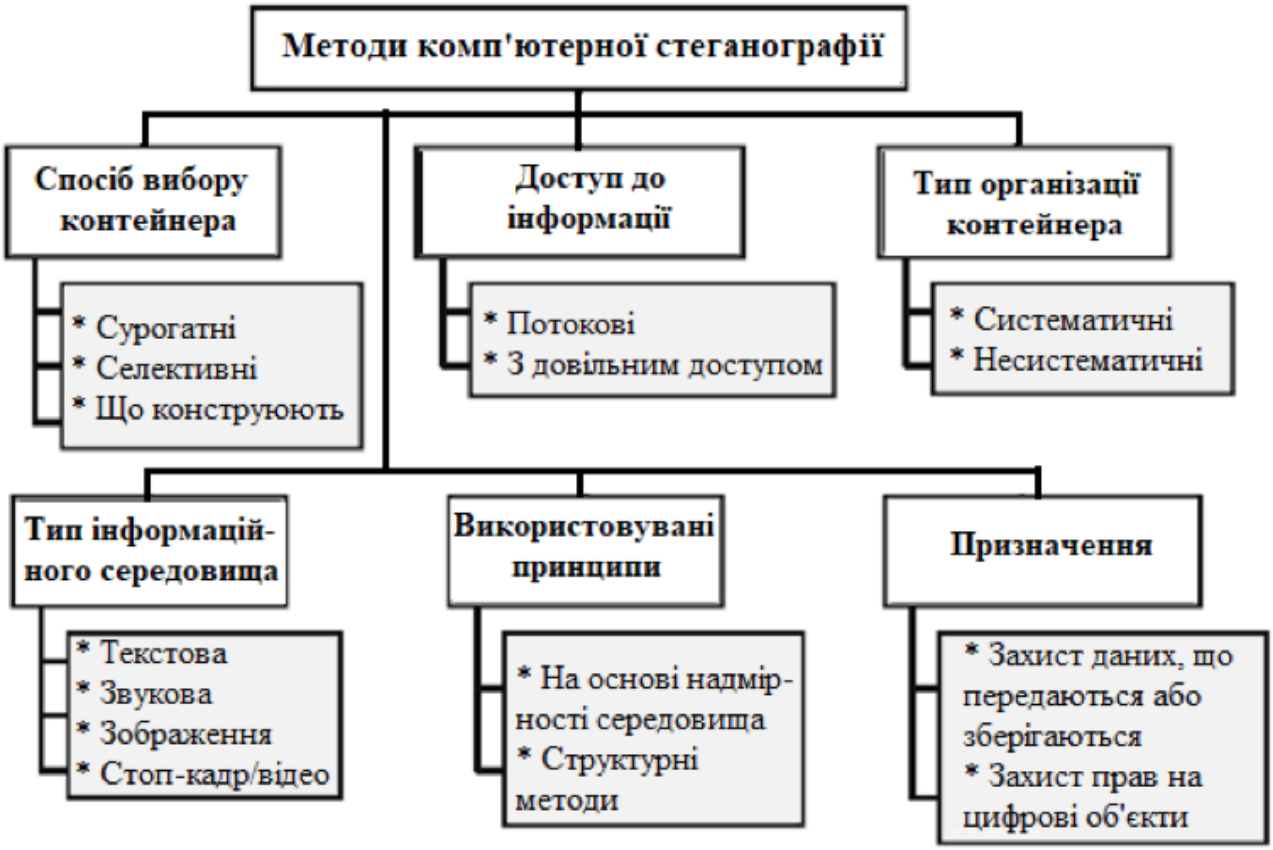

Рисунок 1.4 – Класифікація методів приховання інформації в мобільному пристрої

Окрім цього, нові технології, такі як розпізнавання обличчя та голосу, можуть створювати додаткові ризики для конфіденційності даних користувачів. Наприклад, збором даних про обличчя та голос можуть займатися рекламодавці та інші компанії з метою персоналізації реклами та продажу даних.

Щоб забезпечити конфіденційність даних мобільних пристроїв, користувачам необхідно бути уважними та використовувати різноманітні інструменти захисту даних, такі як паролі, відбитки пальців, шифрування даних, а також ретельно перевіряти дозволи, які вони надають додаткам та сервісам. Крім того, необхідно бути уважним при використанні нових технологій та слідкувати за змінами у законодавстві, які регулюють збір та зберігання даних користувачів.

На жаль, необережні або недосвідчені користувачі мобільних пристроїв також можуть установити зловмисне програмне забезпечення, яке може завдати шкоди людям або організаціям, на які вони працюють.

Зловмисники можуть отримати доступ до соціальних мереж, особистої та ділової електронної пошти, даних платіжних карток, списків контактів, заблокувати мобільні пристрої, щоб вимагати гроші, або використовувати їх для кібератак.

Забезпечення конфіденційності даних на мобільних пристроях може здійснюватися різними способами, які залежать від виробника пристрою, типу операційної системи, налаштувань безпеки та наявності відповідного програмного забезпечення. Основні способи забезпечення конфіденційності даних на мобільних пристроях такі[7]:

- Пароль та інші методи автентифікації: Використання пароля, PIN-коду, відбитка пальця, розпізнавання обличчя та інших методів автентифікації є першим кроком до захисту конфіденційних даних на мобільних пристроях. Ці методи забезпечують доступ до пристрою тільки для авторизованого користувача та запобігають несанкціонованому доступу до даних.
- Шифрування даних: Шифрування даних забезпечує їх захист від несанкціонованого доступу та зберігає їх в зашифрованому вигляді. Більшість сучасних мобільних пристроїв мають вбудовану функцію шифрування даних, яка дозволяє шифрувати дані на рівні пристрою.
- Віртуальні приватні мережі (VPN): Використання VPN дозволяє забезпечити безпеку та конфіденційність підключення до Інтернету на мобільному пристрої. Віртуальна приватна мережа зашифровує дані, що передаються з пристрою до Інтернету та забезпечує анонімність користувача.
- Контроль доступу до додатків: Більшість операційних систем мають вбудовані інструменти контролю доступу до додатків, які дозволяють користувачам контролювати доступ до конфіденційних даних. Наприклад, деякі додатки для зберігання паролів дозволяють встановлювати майстер-пароль або використовувати сканер відбитку пальця для доступу до даних.

- Оновлення програмного забезпечення: Виробники мобільних пристроїв регулярно випускають оновлення програмного забезпечення, які виправляють виявлені уразливості та забезпечують додаткові заходи безпеки. Користувачам рекомендується регулярно оновлювати операційну систему та додатки, щоб захистити свої дані від зловмисників.
- Використання програмного забезпечення для захисту даних: Крім вбудованих інструментів безпеки, існує велика кількість програм для мобільних пристроїв, які забезпечують захист конфіденційних даних. Наприклад, деякі програми для зберігання паролів або файлового менеджера мають вбудовані інструменти шифрування даних.

Загалом, захист конфіденційності даних на мобільних пристроях є складним процесом, який вимагає поєднання різних технологій та налаштувань безпеки. Користувачам рекомендується бути уважними та встановлювати на свої пристрої тільки довірені додатки та програмне забезпечення. Також важливо регулярно робити резервні копії своїх даних та зберігати їх в безпечному місці.

1.3 Огляд існуючих комплексних систем захисту інформації від несанкціонованого доступу

Комплексні системи захисту інформації від несанкціонованого доступу - це сукупність технологій, методів та процедур, які застосовуються для захисту інформації від несанкціонованого доступу, зломів та крадіжок. Основним завданням таких систем є забезпечення конфіденційності, цілісності та доступності інформації.

На сьогоднішній день існує велика кількість комплексних систем захисту інформації від несанкціонованого доступу, які можуть бути використані в різних сферах, включаючи державні установи, військові організації, фінансові установи та підприємства. Нижче розглянуто деякі з найбільш відомих та ефективних комплексних систем захисту інформації[12]:

- Cisco Security: Це комплексна система захисту інформації, яка включає різноманітні продукти, такі як мережеві файрволи, системи виявлення вторгнень, системи захисту від вірусів та шпигунського програмного забезпечення, інструменти моніторингу мережі та аналізу безпеки. Cisco Security використовує інтелектуальні алгоритми та технології машинного навчання для виявлення та блокування загроз безпеці мережі.
- Symantec Endpoint Protection: Система захисту інформації, яка включає антивірусні, антишпигунські та мережеві файрволи. Symantec Endpoint Protection також має вбудований інструмент моніторингу та аналізу поведінки програм для виявлення та блокування нових загроз, які не визнаються традиційними антивірусними програмами.
- IBM Security: Ця комплексна система захисту є широко відомою компанією, яка надає різноманітні послуги зі збереження безпеки та захисту даних. Їх продукти включають інструменти для моніторингу та аналізу поведінки користувачів, захисту від вірусів та шпигунського ПЗ, та захисту мереж від вторгнень.
- McAfee Total Protection: Система, яка включає антивірусні, антишпигунські та мережеві файрволи. McAfee Total Protection також має вбудований інструмент моніторингу та аналізу поведінки програм для виявлення та блокування нових загроз, які не визнаються традиційними антивірусними програмами.
- Check Point Security: Комплексна система захисту інформації, яка включає мережеві файрволи, системи виявлення вторгнень, захист від вірусів та шпигунського ПЗ, та інструменти моніторингу мережі та аналізу безпеки. Check Point Security використовує інтелектуальні алгоритми та технології машинного навчання для виявлення та блокування загроз безпеці мережі.
- Palo Alto Networks: Це комплексна система захисту інформації, яка включає мережеві файрволи, системи виявлення вторгнень та захисту

від вірусів та шпигунського ПЗ. Palo Alto Networks також має інструменти моніторингу мережі та аналізу безпеки, що дозволяє виявляти та блокувати загрози безпеці мережі з високою точністю.

Усі ці комплексні системи захисту інформації мають різні функції та можливості, які дозволяють забезпечити безпеку даних. Важливо зазначити, що жодна система захисту не може гарантувати повну безпеку даних. Незалежно від того, наскільки добре розроблена та встановлена система захисту, завжди є потенційна можливість для хакерів або зловмисників проникнути до системи та отримати доступ до даних.

Однак, використання комплексних систем захисту інформації може значно зменшити ризик несанкціонованого доступу до даних. Ці системи можуть виявляти підозрілу активність та блокувати атаки, перед тим як вони стануть серйозною загрозою для системи[13]. Крім того, комплексні системи захисту можуть автоматично оновлювати програмне забезпечення та виконувати інші проактивні заходи для забезпечення безпеки даних.

Загалом, використання комплексних систем захисту інформації від несанкціонованого доступу є критично важливим для забезпечення безпеки даних на мобільних пристроях. Вони допомагають зменшити ризик інцидентів з даними та можуть значно зменшити витрати на відновлення після атаки. Проте, важливо розуміти, що жодна система захисту не може гарантувати повну безпеку даних, тому важливо приділяти належну увагу безпеці даних та практикувати безпечний спосіб використання мобільних пристроїв.

1.4 Процес виявлення несанкціонованого доступу мобільних гаджетів

Процес виявлення несанкціонованого доступу до мобільних гаджетів є складним та потребує використання різноманітних методів та інструментів. Основна мета цього процесу - забезпечення безпеки даних та зменшення ризику порушення конфіденційності особистої інформації користувачів[14].

Першим етапом процесу виявлення несанкціонованого доступу є розуміння ризиків та можливих загроз для безпеки даних на мобільних пристроях. Користувач повинен бути свідомим про те, що відкриває для себе можливості атак з боку зловмисників, коли використовує мобільні пристрої та їх додатки.

Другим етапом є розгляд основних методів виявлення несанкціонованого доступу до мобільних гаджетів. Основними методами є[15]:

- Використання антивірусного програмного забезпечення - дозволяє виявляти шкідливі програми та інші загрози для безпеки даних на мобільних пристроях.
- Аналіз мережевої активності - дозволяє виявляти несанкціоновану активність у мережі та блокувати спроби несанкціонованого доступу до даних.
- Використання систем контролю доступу до додатків - дозволяє встановлювати обмеження щодо доступу до даних та функціоналу додатків.
- Аналіз поведінки додатків - дозволяє виявляти підозрілу активність додатків та виявляти можливі загрози для безпеки даних.
- Використання систем моніторингу - дозволяє відслідковувати дії користувачів та виявляти підозрілу активність на мобільних пристроях.

Наступним етапом є виконання аналізу зібраних даних для виявлення потенційних ознак несанкціонованого доступу до мобільного пристрою. Цей аналіз може включати перевірку виконання незвичайних дій або виявлення незвичайних поведінкових паттернів. Наприклад, система може виявити, якщо додаток має незвичайний доступ до приватних даних, надто часто отримує доступ до Інтернету, надто часто відкривається та закривається або використовує велику кількість ресурсів пристрою.

У разі виявлення потенційних ознак несанкціонованого доступу, система повинна сповістити власника пристрою або адміністратора системи. Деякі системи можуть також надавати можливість заблокувати додатки або обмежити їх доступ до приватних даних, щоб запобігти подальшій компрометації даних.

Останнім етапом процесу виявлення несанкціонованого доступу є захист даних та усунення вразливостей. Це може включати встановлення оновлень програмного забезпечення, зміну налаштувань безпеки, заблокування додатків або видалення шкідливих програм. За потреби може бути також виконана ручна перевірка пристрою для виявлення вразливостей та забезпечення безпеки даних.

У цілому процес виявлення несанкціонованого доступу до мобільних пристроїв є складним та вимагає використання різних інструментів та технологій.

Процес виявлення несанкціонованого доступу до мобільних гаджетів можна розділити на кілька етапів[16]:

- Моніторинг активності: Системи захисту можуть моніторити активність на мобільному пристрої, таку як використання додатків, з'єднання з мережами Wi-Fi і Bluetooth, та збирати дані про користувачів.
- Виявлення аномальних змін: Системи захисту можуть виявляти аномальні зміни у поведінці користувачів, такі як зміна режиму роботи пристрою, встановлення нових додатків, або збільшення обсягу передачі даних.
- Аналіз даних: Системи захисту можуть аналізувати дані, що збираються в процесі моніторингу, для виявлення можливих загроз.
- Виявлення загроз: Під час аналізу даних системи захисту можуть виявляти загрози, такі як шкідливі програми, віруси, або зловмисні атаки на мобільний пристрій.
- Захист від загроз: Після виявлення загрози системи захисту можуть приймати заходи для її запобігання, наприклад, блокування доступу до певних додатків або мереж.
- Усунення загроз: Якщо виявлено загрозу, система захисту може сповістити користувача та запропонувати рішення, які допоможуть усунути цю загрозу.

Важливо зазначити, що процес виявлення несанкціонованого доступу може бути різним для різних систем захисту інформації, але загальна схема залишається приблизно такою ж самою.

Висновки до розділу 1

У результаті вивчення першого розділу можна зробити висновок, що несанкціонований доступ до інформації на мобільних пристроях є серйозною загрозою для конфіденційності даних користувачів. Це може призвести до витоку приватної інформації, крадіжки особистих даних, фінансових втрат, та інших негативних наслідків.

Конфіденційність даних на мобільних пристроях є важливою проблемою безпеки. Несанкціонований доступ до цих даних може мати серйозні наслідки для користувача та його бізнесу. Для запобігання несанкціонованого доступу існують різні комплексні системи захисту, які надають різні функції та можливості. Процес виявлення несанкціонованого доступу на мобільних пристроях може бути виконаний з використанням різних методів та інструментів, які дозволяють виявити незвичайну поведінку та можливі загрози. Забезпечення безпеки даних на мобільних пристроях є актуальним завданням для користувачів та компаній, які працюють з цією інформацією.

Для забезпечення безпеки даних на мобільних пристроях використовуються різні методи та технології. Наприклад, комплексні системи захисту інформації, такі як Symantec, McAfee, та IBM Security, забезпечують багатофункціональний захист, який включає в себе різноманітні засоби захисту, такі як антивіруси, фаєрволи, захист від шпигунського ПЗ, та інші.

Однак, найбільш ефективним методом забезпечення безпеки даних на мобільних пристроях є ретельний контроль за доступом до даних та додатків. Користувачі повинні бути обережними при встановленні та використанні додатків на своїх пристроях, а також використовувати сильні паролі та інші методи аутентифікації для захисту від несанкціонованого доступу до даних.

Отже, забезпечення безпеки даних на мобільних пристроях є важливим завданням, яке вимагає уваги та ретельного підходу до виконання. Користувачі повинні бути свідомі про потенційні загрози та захистити свої пристрої та дані від несанкціонованого доступу.

2 ОГЛЯД ІСНУЮЧИХ МЕТОДІВ ДЛЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

2.1 Загрози несанкціонованого доступу до персональних даних в межах мобільних пристроїв

В контексті постійного росту значущості інформаційно-комунікаційних технологій у сучасному світі, надзвичайно важливо приділяти більше уваги питанням захисту даних від втрат, крадіжок, спотворень або пошкоджень. Враховуючи те, що більшість людей активно користується мобільними додатками, цей виклик набуває особливої ваги. Адекватні заходи для вирішення цієї проблеми підвищують рівень інформаційної безпеки не лише для окремих осіб чи організацій, а й для цілої країни.

Список ключових факторів, які впливають на ситуацію з інформаційною безпекою в контексті використання відкритих та соціально спрямованих ресурсів Інтернету:

1. Військова агресія Росії та асоційовані з нею глобальні кібератаки, великомасштабні антиукраїнські інформаційні втручання та їх психологічна впливність на користувачів української частини Інтернету, неавторизоване здобуття доступу до особистих даних та іншої відповідної інформації через електронну пошту, поштові скриньки та соціальні мережі і т.д.

2. Наявність ризику для державних органів (міністерств, департаментів, агентств, фінансових установ тощо) пов'язана з використанням співробітниками на роботі та в повсякденному житті програмного обладнання російського виробництва, а також електронних поштових сервісів та соціальних мереж, доступ до яких наразі обмежено згідно з Указом Президента України № 133/2017 від 15.05.2017 року.

3. Домінування у великих та впливових медіа осіб, які використовують ці ресурси для просування та захисту особистих, а не національних інтересів.

4. Інтенсивне заповнення соціальних мереж сфабрикованими повідомленнями відповідного змісту з допомогою мереж "ботів" та технології масового "тролінгу".

5. Використання маніпуляцій у засобах масової інформації та соціальних мережах з метою привернення більшої аудиторії через методи соціального інжинірингу.

6. Застосування соціальних мереж для розповсюдження ненадійної (фальшивої, спотвореної, деструктивної) інформації та реалізація маніпулятивного впливу на громадську свідомість користувачів української частини Інтернету.

Опис важливих ризикових факторів та пропозиції щодо їхнього вирішення.

Збереження та передача інформації.

Неуважне ставлення до безпеки під час виконання службових обов'язків працівниками органів виконавчої влади та місцевого самоврядування, керівництвом державних підприємств, установ, організацій, а також військовими може призвести до втрати або викрадення мобільних телефонів, персональних ноутбуків, магнітних носіїв даних і т.д. Така ситуація може загрожувати збереженню персональних даних і спричинити розголошення інформації з обмеженим доступом.

Щоб запобігти негативним наслідкам у разі втрати або крадіжки носіїв даних, рекомендується:

- надавати паролі для всіх пристроїв у власному використанні (PIN-коди, паролі для доступу до всіх аккаунтів, паролі для планшетів та лаптопів і так далі);

- регулярно створювати резервні копії критично важливих файлів;

- блокувати пристрої після завершення роботи з ними.

Соціальні мережі.

Соціальні мережі в сучасному світі є практичним та ефективним інструментом спілкування. З допомогою соціальних медіа можна обмінюватися повідомленнями, ділитися особистими фото та відео, публікувати інформацію про роботу, відпочинок, колег, друзів, освіту, відпочинок, політичні погляди тощо.

Така велика кількість особистої інформації може стати загрозою для професійної та особистої життєвої сфери службовців державних установ, керівників компаній, установ, організацій, працівників виконавчої влади та місцевого самоврядування, а також військових, якщо ця інформація потрапить до невідповідних осіб.

Щоб запобігти несанкціонованому доступу до особистих аккаунтів, зареєстрованих у соціальних медіа, вам потрібно:

- встановити надійний пароль для входу в свій аккаунт. Рівень захисту аккаунта та інформації, яка в ньому зберігається, залежить від складності встановленого паролю;

- використовувати двофакторну автентифікацію. При вході в профіль з незнайомого пристрою, сервіс вимагатиме додаткову перевірку власника аккаунта. Вам буде надіслано повідомлення з кодом підтвердження на вказаний номер телефону або на електронну пошту, або ви зможете ввести один з заздалегідь збережених паролів через вибраний спосіб підтвердження;

- використовувати додаткові налаштування профілю в соціальних медіа для отримання повідомлень про несанкціоновані входи в ресурси з невідомих пристроїв або браузерів;

- Під час реєстрації аккаунтів у соціальних мережах варто використовувати як "логін" електронну адресу відомого та довіреного сервісу ("Google", "Yahoo") або поштових служб України. Використання російських сервісів, до яких українським користувачам заборонено доступ, не рекомендується, оскільки через особисту електронну пошту можливий отримання паролю, а отже, доступ до профілів, зареєстрованих у соціальних мережах.

- уникайте входу в особисті або робочі, корпоративні профілі з невідомих або незахищених пристроїв. Є ймовірність, що після завершення роботи вийти з свого облікового запису не вийде, або пристрій запам'ятає вказаний при вході логін та пароль. Також існує ризик інфікування такого пристрою шкідливим програмним забезпеченням, яке може збирати і передавати інформацію про паролі та логіни зацікавленим особам.

У контексті гібридної агресії від Російської Федерації, соціальні мережі активно використовуються для збирання детальної інформації про особистість, включаючи регулярні місця її перебування, родину, колег, особисті смаки та іншу приватну інформацію. Водночас, через соціальні мережі проводиться збір та розповсюдження інформації про місця дислокації та склад окремих військових одиниць Збройних сил України, які задіяні у проведенні операції об'єднаних сил на Сході України, частина якої є конфіденційною.

Щоб запобігти отриманню додаткової особистої інформації про вас, вашу родину, колег та інтереси, а також інформації про місця дислокації та склад окремих військових підрозділів Збройних сил України, що беруть участь в операції об'єднаних сил на сході України, важливо дотримуватись таких правил:

- уникайте публікації в соцмережах інформації, що може загрожувати вашому особистому життю, життю вашої родини та інших осіб;

- військовослужбовцям та членам їх сімей слід утримуватися від публікації фото та відеоматеріалів, які можуть вказувати на місце дислокації військового підрозділу або окремих військових формувань, що беруть участь в операції об'єднаних сил на сході України. Такі дії можуть становити загрозу для життя та здоров'я людей;

- обмежте доступ до вашої особистої інформації в налаштуваннях конфіденційності соціальної мережі. Виберіть такі параметри, які найкраще захистять ваші персональні дані. Наприклад, не вказуйте свою геолокацію (місце перебування) та не дозволяйте пошук свого акаунта в соцмережах за номером мобільного телефону або електронною адресою;

- регулярно перевіряйте свій список друзів в соцмережах. Якщо ви знайдете незнайомців або підозрілих користувачів (акаунти), видаліть їх, оскільки статус "друг" часто дає доступ до більшої кількості вашої особистої інформації. Будьте обережні при додаванні нових користувачів до свого списку "друзів" у майбутньому.

Використовуючи додатки для смартфонів.

Коли ви встановлюєте різні додатки на свій телефон, ці програми можуть вимагати доступ до певної інформації на вашому пристрої, включаючи геолокацію, список контактів, акаунти в соціальних мережах та поштові скриньки.

Згідно з наявною інформацією, більшість шпигунського програмного забезпечення "вбудовується" саме в мобільні додатки, які цікавлять певну аудиторію. Отже, необхідно проявляти обережність при встановленні додатків, особливо з невідомих або неперевірених джерел.

Щоб уникнути завантаження шпигунського програмного забезпечення на ваш особистий пристрій, слід дотримуватись таких правил:

- встановлювати додатки тільки з офіційних та перевірених сервісів

- налаштуйте операційну систему вашого смартфона так, щоб вона не дозволяла автоматичне встановлення додатків з незнайомих джерел;

- регулярно проводьте очищення своїх особистих пристроїв від додатків, які ви більше не використовуєте.

Користування електронною поштою.

Електронні поштові скриньки виконують не лише роль засобу збереження великої кількості особистої та професійної інформації (у вигляді листів), але також часто використовуються для реєстрації аккаунтів у соціальних мережах, менеджерів, хмарних служб і так далі. Таким чином, несанкціонований вхід до поштової скриньки може призвести до серйозних проблем, включаючи отримання конфіденційної інформації, зміну паролів до різних сайтів та аккаунтів без відома їхніх власників, доступ до особистих фотографій і відео, розсилку спаму від імені інших і т.д.

Щоб знизити можливість несанкціонованого доступу до вашої електронної поштової скриньки, слід дотримуватися таких рекомендацій:

- увімкніть двофакторну автентифікацію, яка включає використання мобільного пристрою. Це гарантує, що при спробах третіми особами втрутитися в роботу вашої поштової скриньки, ви отримаєте SMS-повідомлення про таку спробу на свій мобільний телефон;

- використовуйте складні та надійні паролі;

- уникайте використання послуг для відновлення паролів, які належать російським компаніям ("Yandex.ru", "Mail.ru" тощо);

- уникайте відкриття та запуску додатків із сумнівних електронних листів, особливо якщо вони містять виконавчі файли з розширеннями підозрілими розширеннями.

Доступ до мережі Інтернет.

Доступ до мережі Інтернет.

Часто під час користування Інтернетом у громадських місцях люди підключаються до відкритих Wi-Fi точок доступу. Вони зазвичай безкоштовні та не потребують введення паролю для підключення. Відсутність паролю робить такі мережі більш вразливими для атак хакерів, які намагаються отримати доступ до персональних даних та інформації, збереженої на пристроях користувачів.

Щоб захистити свої дані від несанкціонованого доступу, рекомендується дотримуватися таких правил:

- при підключенні до мережі слід вибирати точки доступу до Wi-Fi, які підтримують протоколи безпеки WPA або WPA-2;

- у громадських місцях краще використовувати власний Wi-Fi модем або використовувати мобільний Інтернет, який надає ваш мобільний оператор;

- на мобільних пристроях рекомендується вимкнути автоматичне підключення до Wi-Fi мереж.

2.2 Багаторівнева модель захисту додатків мобільних пристроїв

Загалом, модель багаторівневого захисту визначає сукупність рівнів захисту для інформаційної системи. Така модель часто використовується компанією Microsoft у своїх настановах з безпеки. Правильне створення захисту

на кожному визначеному рівні може допомогти забезпечити систему від виконання потенційних загроз інформаційної безпеки.

Набір рівнів може неабияк відрізнятися в залежності від джерела, однак одним з можливих варіантів є той, що представлено на рис. 2.1.

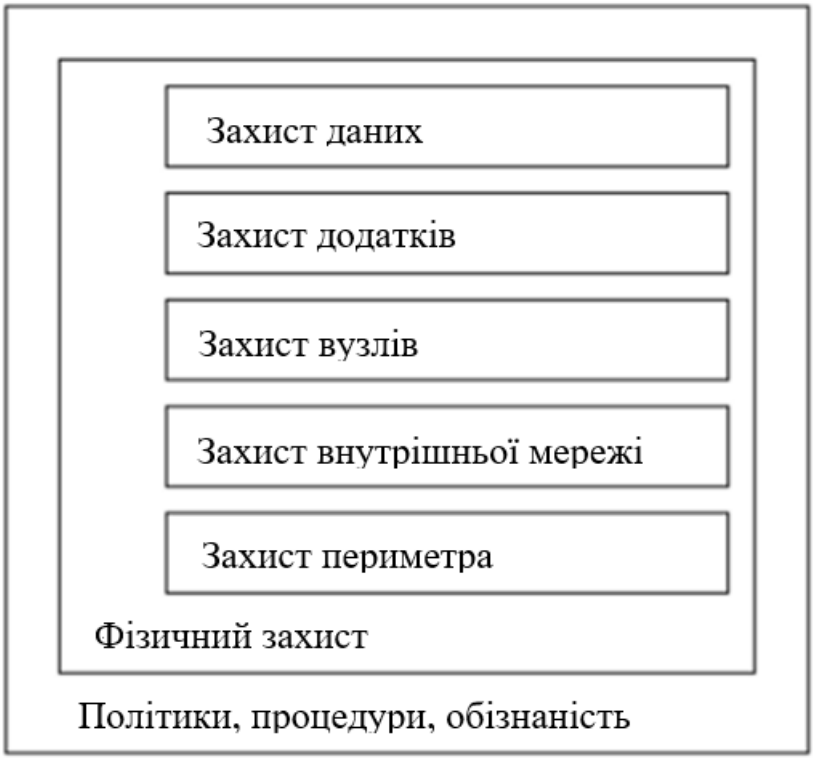

Рисунок 2.1 – Рівні багаторівневого захисту додатків мобільних пристроїв

З рисунку 2.1 видно, що політика безпеки повинна описувати всі аспекти роботи системи з точки зору забезпечення інформаційної безпеки.

Тому багаторівнева модель захисту додатків мобільних пристроїв має включати:

- рівень політики безпеки, який можна вважати фундаментальним, передбачає наявність документованих організаційних механізмів захисту (процедур), порядку повідомлення про інциденти, навчання користувачів в сфері інформаційної безпеки, та інших подібних дій (наприклад, тих, що рекомендовані стандартом ISO / IEC 17799);
- рівень фізичного захисту охоплює дії, спрямовані на обмеження прямого доступу до системних ресурсів - це захист приміщень, контроль доступу,

відеонагляд та ін. Також до цього рівня відносяться заходи захисту мобільних пристроїв, які використовуються працівниками для службових потреб;

- рівень захисту периметра описує безпекові заходи на "точках входу" в мережу, яка захищається від зовнішніх, потенційно небезпечних джерел. Традиційним засобом захисту периметра є мережевий брандмауер, який на основі встановлених правил визначає, чи може мережевий пакет пройти в захищену мережу. Додаткові приклади засобів захисту периметра включають системи виявлення вторгнень, а також антивірусні засоби для безпекових шлюзів;
- рівень захисту внутрішньої мережі бере на себе обов'язок забезпечення безпеки передачі даних в межах мережі та мережевої інфраструктури. Приклади інструментів та механізмів захисту на цьому рівні включають створення віртуальних локальних мереж (VLAN) за допомогою керованих комутаторів, захист переданих даних за допомогою протоколу IPSec. Часто в межах мережі також застосовуються засоби, які зазвичай використовуються для захисту периметра, наприклад, мережеві брандмауери, включаючи персональні. Це пов'язано з тим, що використання бездротових мережевих технологій та віртуальних приватних мереж (VPN) призводить до "розтікання" мережевого периметра. Наприклад, якщо нападник зміг підключитися до точки бездротового доступу всередині захищеної мережі, його дії вже не будуть контролюватися фаєрволом, розміщеним "на межі" мережі, хоча формально атака буде виконуватися з комп'ютера, що знаходиться за межами нашої мережі. Тому іноді при аналізі розглядається "рівень мережевого захисту", який включає як захист периметра, так і внутрішньої мережі;
- рівень захисту вузлів відноситься до нападів, спрямованих на окремий вузол мережі, і відповідно, до вжитих заходів для їх запобігання. Може бути врахована роль вузла і окремо розглянута охорона серверів та робочих станцій. Основний акцент слід зробити на захисті на рівні операційної системи - налаштуванні, що поліпшує безпеку конфігурації (включаючи вимкнення не використовуваних або потенційно небезпечних служб), організації встановлення

патчів і оновлень, надійній аутентифікації користувачів. Антивірусний захист відіграє вкрай важливу роль;

- рівень захисту додатків відповідає за захист від атак, спрямованих на конкретні програми – поштові сервери, web-сервери, сервери баз даних. Як приклад можна назвати SQL-ін'єкції - атаки на сервер БД, які полягають в тому, що у вхідні текстовий рядок включаються оператори мови SQL, що може порушити логіку обробки даних і привести до отримання порушником конфіденційної інформації. Сюди ж можна віднести модифікацію додатків комп'ютерними вірусами. Для захисту від подібних атак використовуються настройки безпеки самих додатків, установка оновлень, засоби антивірусного захисту;
- рівень захисту даних визначає порядок захисту обробляються і зберігаються в системі даних від несанкціонованого доступу та інших загроз. Як приклади контрзаходів можна назвати розмежування доступу до даних засобами файлової системи, шифрування даних при зберіганні і передачі.

У процесі ідентифікації ризиків багаторівнева модель визначає що є метою порушника, і на якому рівні або рівнях захисту можна йому протистояти. Відповідно вибираються і контрзаходи, при тому захист від загрози на декількох рівнях знижує ймовірність її реалізації, а значить, і рівень ризику.

2.3 Забезпечення безпеки додатків в системах iOS та Android

З появою додатків та великої кількості нових пристроїв, якими можна управляти за допомогою мобільних додатків, безпека смартфонів набуває особливого значення. Недоліки в системі безпеки ґаджетів можуть легко використовуватися зловмисниками для атак на “розумні” пристрої.

Забезпечення безпеки додатків в iOS:

1. Система контролю доступу: iOS використовує систему контролю доступу, яка обмежує функціональні можливості додатків та їх доступ до конфіденційних даних. Додатки на iOS мають обмежені права доступу до функцій

пристрою та повинні отримати дозвіл користувача для доступу до ресурсів, таких як камера, мікрофон або геолокація.

2. Верифікація додатків: Додатки для iOS повинні пройти процес верифікації перед тим, як вони стають доступними в App Store. Apple перевіряє додатки на наявність шкідливого коду, дотримання політик безпеки та конфіденційності, що зменшує ризик завантаження шкідливих додатків користувачами

3. Захист даних: iOS використовує різні методи шифрування для захисту даних, збережених на пристрої. Всі дані, які зберігаються в додатках, зашифровуються та зберігаються в зашифрованій формі на пристрої.

4. Sandboxing: iOS використовує концепцію пісковиці, що означає, що кожен додаток виконується у своєму власному, ізольованому середовищі. Додатки не мають доступу до даних інших додатків, якщо користувач спеціально цього не дозволив.

5. ASLR (Address Space Layout Randomization): Технологія, яка рандомізує розташування пам'яті додатків, щоб ускладнити використання помилок у безпеці зловмисниками.

6. Автоматичне оноволення: Apple регулярно випускає оновлення iOS, які включають виправлення помилок безпеки.

Забезпечення безпеки додатків в Android:

1. Перевірка додатків перед встановленням: Перед встановленням додатка з Google Play Market, Android проводить перевірку на наявність шкідливого коду та інших потенційних загроз безпеці. Це допомагає зменшити ризик встановлення шкідливих додатків.

2. Права доступу: Android також має систему контролю доступу, яка дозволяє користувачам контролювати права доступу додатків до різних функцій та ресурсів пристрою. Користувачі можуть надавати або відмовляти дозволу на доступ до камери, мікрофона, контактів та інших ресурсів.

3. Апаратна безпека: Багато сучасних Android-пристроїв підтримують апаратну безпеку, таку як модуль безпеки TrustZone, який забезпечує ізольовану

та безпечну область для зберігання конфіденційних даних та виконання захищених операцій.

4. Sandboxing: Подібно до iOS, Android також використовує технологію пісковиці для ізоляції додатків. Кожен додаток запускається в власному процесі з власними правами доступу, що обмежують можливості додатка взаємодіяти з іншими додатками і системою.

5. Application Signing: Всі додатки мають бути підписані цифровим сертифікатом перед тим, як їх можна буде встановити на пристрій Android. Це включає додатки з Google Play Store та інших джерел. Цифровий підпис допомагає визначити, хто відповідає за додаток, і захищає користувачів від підроблених додатків.

6. Безпечний режим: Android включає безпечний режим, який дозволяє запустити пристрій з мінімальним набором служб та додатків. Це може бути корисним для видалення шкідливих додатків або виправлення проблем системи.

7. ASLR: Також присутній в Android, цей механізм перетворює пам'ять у непередбачуваний шлях, що ускладнює напади.

Забезпечення безпеки додатків в системах iOS та Android - це складний і постійно розвиваючийся процес. Компанії, що розробляють операційні системи, постійно вдосконалюють свої методи захисту. Однак, безпека додатків залежить не тільки від розробників, але й від свідомості та обережності самого користувача. Правильне використання додатків та своєчасне оновлення операційної системи можуть суттєво зменшити ризики безпеки і захистити вашу інформацію.

2.4 Недоліки існуючих методів в контексті захисту інформації

У зв’язку зі збільшенням кількості потенційних загроз, захист мобільних ґаджетів потребує більшої уваги з боку користувачів. Хоча системи безпеки смартфонів розроблені з використанням найсучасніших механізмів захисту, ризики їх інфікування все одно існують.

Існуючі методи захисту інформації на мобільних гаджетах мають свої недоліки, які необхідно враховувати.

1. Паролі низького рівня складності: Багато користувачів використовують прості паролі або підбирають однакові паролі для різних сервісів. Це робить їх аккаунти на мобільних пристроях вразливими до атак методом "брутфорс". Такі паролі можна легко вгадати або зламати за допомогою спеціального програмного забезпечення.

2. Відсутність багатофакторної аутентифікації: Багато мобільних пристроїв не надають можливості використовувати багатофакторну аутентифікацію, яка є більш надійним методом захисту. Зазвичай, використовується лише пароль або PIN-код, що може бути легко підбито або вкрадено. Багатофакторна аутентифікація залучає додаткові елементи, такі як біометричні дані або фізичні токени, що збільшує рівень безпеки.

3. Нестійкість до фішингу та шкідливих програм: Багато користувачів мобільних пристроїв стають жертвами фішингових атак, коли шахраї використовують підроблені веб-сторінки або електронні повідомлення для виклику довіри і отримання особистої інформації. Деякі шкідливі програми також можуть бути встановлені на мобільні пристрої без відома користувача і збирати конфіденційні дані. Існуючі методи фільтрації фішингових атак та виявлення шкідливих програм не завжди є ефективними.

4. Вразливості операційних систем: Операційні системи мобільних пристроїв мають свої вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до інформації. Ці вразливості можуть включати помилки у коді операційної системи, недостатню автентифікацію або незашифрований обмін даними.

5. Низька обізнаність користувачів: Багато користувачів мобільних пристроїв не мають достатньої обізнаність про методи захисту інформації та навички керування безпекою. Їхні дії можуть не бути свідомими і вони можуть бути вразливими до ризиків, пов'язаних з відкриттям неперевірених посилань або завантаженням сумнівного програмного забезпечення.

Висновки до розділу 2

Оглянувши існуючі методи для захисту від несанкціонованого доступу, стає очевидним, що безпека інформації є надзвичайно важливим аспектом в сучасному цифровому світі. Існують різні підходи та технології, які можуть забезпечити надійний рівень захисту, але жоден метод не є повністю досконалим.

Важливо мати комплексний підхід до захисту інформації, починаючи зі сильних паролів та багатофакторної аутентифікації до використання шифрування даних та систем контролю доступу. Застосування оновлених версій операційних систем та додатків, а також регулярне оновлення захисного програмного забезпечення, також грають важливу роль у забезпеченні безпеки.

Незважаючи на те, що існують методи для захисту від несанкціонованого доступу, важливо також пам'ятати про особисту відповідальність кожного користувача. Користувачі повинні бути освіченими та свідомими щодо ризиків, пов'язаних з небезпечними практиками, такими як використання слабких паролів, недбале ставлення до оновлень та неперевірене завантаження додатків.

Усі ці методи і практики повинні працювати разом, забезпечуючи цілісний підхід до захисту від несанкціонованого доступу. Тільки за умови поєднання технічних заходів безпеки та свідомих дій користувачів ми зможемо забезпечити надійний рівень захисту від потенційних загроз і зберегти конфіденційність та цілісність нашої інформації

3 МЕТОДИ ВДОСКОНАЛЕННЯ ІСНУЮЧИХ СИСТЕМ

3.1 Практичне застосування методів удосконалення систем безпеки до персональних даних в межах мобільних пристроїв

У сучасному цифровому світі мобільні пристрої стали невід'ємною частиною нашого повсякденного життя. Зростаюча кількість людей використовує мобільні пристрої для зберігання та обміну особистою і конфіденційною інформацією. Однак із збільшенням використання мобільних пристроїв зростають також загрози безпеці персональних даних. Існують численні недоліки в існуючих системах безпеки, які можуть призвести до несанкціонованого доступу до особистих даних користувачів.

В рамках даного розділу будуть розглянуті різні методи вдосконалення систем безпеки персональних даних в межах мобільних пристроїв. Будуть розглянуті такі методи:

1. Використання біометричних технологій: Біометричні технології, такі як відбитки пальців, розпізнавання обличчя, розпізнавання ірису та інші, можуть бути використані для підвищення рівня безпеки мобільних пристроїв. Ці технології можуть забезпечити унікальну ідентифікацію користувача та запобігти несанкціонованому доступу до особистих даних.

2. Використання шифрування: Шифрування даних є ефективним методом захисту інформації на мобільних пристроях. Використання сучасних алгоритмів шифрування дозволяє захистити дані від несанкціонованого доступу навіть у випадку втрати або крадіжки пристрою.

3. Розвиток двофакторної аутентифікації: Двофакторна аутентифікація вимагає введення двох незалежних факторів ідентифікації для доступу до мобільного пристрою. Це може включати комбінацію пароля, відбитку пальця, смс-повідомлення з одноразовим кодом або використання спеціальних апаратних токенів. Використання двофакторної аутентифікації додає додатковий рівень безпеки до мобільних пристроїв.

4. Розробка антивірусного програмного забезпечення: Розробка спеціалізованого антивірусного програмного забезпечення для мобільних пристроїв є важливим методом вдосконалення систем безпеки. Це дозволяє виявляти та усувати загрози безпеці, такі як шкідливі програми, троянські коні, шпигунські програми та інші види шкідливого ПЗ.

Біометричні технології використовують унікальні фізичні або поведінкові характеристики людини для ідентифікації та автентифікації. У контексті мобільних пристроїв, використання біометричних технологій має великий потенціал для підвищення безпеки та запобігання несанкціонованому доступу до персональних даних. Деякі з найпоширеніших біометричних технологій, які можна використовувати на мобільних пристроях, включають:

1. Відбитки пальців: Відбитки пальців є однією з найпоширеніших біометричних характеристик, що використовуються для ідентифікації особи. Сучасні мобільні пристрої часто оснащені сканерами відбитків пальців, що дозволяють користувачам автентифікуватись та розблоковувати пристрій за допомогою свого відбитку пальця. Ця технологія є швидкою та зручною для користувачів.

2. Розпізнавання обличчя: Розпізнавання обличчя використовує унікальні риси обличчя людини, такі як форма обличчя, розташування очей, носа та рота, для ідентифікації особи. Мобільні пристрої зі вбудованими передніми камерами можуть використовувати цю технологію для розпізнавання обличчя користувача та автентифікації його.

3. Розпізнавання ірису: Розпізнавання ірису базується на унікальних характеристиках ірису ока, таких як візуальні структури та унікальні малюнки. Деякі мобільні пристрої оснащені технологією сканування ірису, що дозволяє використовувати цей біометричний параметр для автентифікації користувачів.

Використання біометричних технологій на мобільних пристроях має декілька переваг у порівнянні з традиційними методами автентифікації, такими як паролі або PIN-коди:

1. Унікальність індивідуальних характеристик: Біометричні характеристики, такі як відбитки пальців або риси обличчя, унікальні для кожної особи. Це робить їх важкими до підробки або підміни.

2. Зручність використання: Використання біометричних технологій для автентифікації є зручним для користувачів, оскільки вони можуть використовувати свої фізичні характеристики без необхідності запам'ятовування паролів або PIN-кодів.

3. Висока надійність: Біометричні технології зазвичай мають високу точність і надійність. Вони можуть ефективно розрізняти особи та запобігати несанкціонованому доступу до персональних даних.

Однак, використання біометричних технологій також має свої виклики та обмеження. Деякі з них включають:

1. Збереження та захист біометричних даних: Біометричні дані повинні бути належним чином збережені та захищені, оскільки вони є особистими та унікальними. Виникає ризик крадіжки або незаконного використання цих даних.

2. Імовірність помилок: Використання біометричних технологій може виявитись менш ефективним у випадку, коли знімки відбитків пальців, обличчя або ірису зіткнуться зі змінами особистої зовнішності, такими як поранення або старіння.

3. Практична застосовність: Використання біометричних технологій може потребувати додаткового обладнання, такого як сканери відбитків пальців або передні камери з розпізнаванням обличчя. Це може обмежити їх широке впровадження на всіх мобільних пристроях.

Враховуючи ці переваги та виклики, дослідження та вдосконалення використання біометричних технологій на мобільних пристроях є важливим методом удосконалення систем безпеки персональних даних. Враховуючи їх унікальність та високу надійність, ці технології можуть забезпечити більш безпечний спосіб автентифікації користувачів і захисту їх персональних даних на мобільних пристроях.

Шифрування є одним з найефективніших методів захисту інформації на мобільних пристроях. Воно забезпечує конфіденційність та цілісність даних, унеможливлюючи несанкціонований доступ або зміну інформації. У цьому розділі ми розглянемо різні аспекти шифрування, такі як симетричне шифрування, асиметричне шифрування та протоколи обміну ключами. Детально розглянемо використання шифрування в зберіганні даних, передачі даних та захисті приватності комунікацій.

Симетричне шифрування:

Симетричне шифрування використовує один ключ для як шифрування, так і розшифрування даних. Це означає, що той самий ключ використовується як відправником, так і отримувачем. Такий підхід є швидким і ефективним для шифрування великих обсягів даних на мобільних пристроях. Однак, важливим аспектом є безпечний обмін ключем між відправником і отримувачем, оскільки якщо ключ потрапить у несанкціоновані руки, це може призвести до порушення безпеки.

Асиметричне шифрування:

Асиметричне шифрування використовує два різні ключі: публічний і приватний. Публічний ключ використовується для шифрування даних, тоді як приватний ключ використовується для їх розшифрування. Цей підхід дозволяє безпечно обмінюватись даними, оскільки публічний ключ може бути розповсюдженим, а приватний ключ зберігається тільки у власника. Використання асиметричного шифрування забезпечує більш високий рівень безпеки, але може бути менш ефективним для шифрування великих обсягів даних.

Протоколи обміну ключами:

Протоколи обміну ключами використовуються для безпечного обміну ключами між комунікуючими сторонами. Наприклад, протоколи Diffie-Hellman та RSA дозволяють встановити спільний секретний ключ між відправником і отримувачем, який потім може бути використаний для симетричного шифрування

даних. Це дозволяє забезпечити безпечний обмін ключами, навіть якщо комунікуючі сторони працюють у вразливому середовищі.

Захист приватності комунікацій:

Шифрування використовується для захисту приватності комунікацій на мобільних пристроях. Коли дані передаються через мережу, вони можуть бути підвергнуті перехопленню або злому. Використання протоколів шифрування, таких як SSL/TLS, дозволяє зашифрувати дані, що передаються між пристроями, і забезпечити безпеку комунікацій. Це важливо для захисту конфіденційної інформації, такої як паролі, фінансові дані або особиста інформація.

Двофакторна аутентифікація є ефективним способом підвищення безпеки мобільних пристроїв. Вона вимагає використання двох незалежних факторів ідентифікації для підтвердження справжності користувача. У цьому розділі ми розглянемо різні методи двофакторної аутентифікації, такі як використання одноразових паролів, апаратних токенів і біометричних даних. Дослідимо переваги і недоліки кожного методу та його практичну застосовність.

Використання одноразових паролів:

Одноразові паролі (OTP) генеруються за допомогою спеціального пристрою або мобільного додатка і використовуються тільки один раз для аутентифікації. Користувач отримує OTP через SMS, електронну пошту або спеціальну програму. Цей метод додає додатковий шар безпеки, оскільки крім знання основного пароля, зловмиснику також потрібно мати доступ до OTP. Однак, недоліком є потреба в постійному доступі до пристрою або програми для отримання OTP, що може бути не зручним для користувачів.

Використання апаратних токенів:

Апаратні токени - це фізичні пристрої, такі як USB-ключі або смарт-карти, які містять унікальні ідентифікатори або сертифікати для аутентифікації. Користувач вставляє токен в мобільний пристрій або підключає його безпроводово через NFC-технологію. Для доступу до системи користувач повинен мати як фізичний токен, так і знання основного пароля. Використання апаратних токенів надає високий рівень безпеки, оскільки зловмисник не може отримати

доступ до системи без фізичного пристрою. Однак, цей метод може бути дорогим і вимагати додаткового обладнання.

Використання біометричних даних:

Біометричні дані, такі як відбитки пальців, розпізнавання обличчя, розпізнавання ірису та інші, використовуються для ідентифікації користувача. Мобільні пристрої все частіше використовують вбудовані датчики для збору біометричних даних і їх подальшого використання для аутентифікації. Цей метод забезпечує зручність для користувачів, оскільки вони можуть використовувати свої фізичні риси для аутентифікації. Однак, біометричні дані можуть бути піддаже ризику викрадення або злому, тому важливо забезпечити їх безпеку та надійність.

Кожен з цих методів двофакторної аутентифікації має свої переваги та недоліки, і вибір методу залежить від конкретних потреб і вимог користувача. Комбінація декількох методів може також забезпечити ще вищий рівень безпеки. Враховуючи ці аспекти, двофакторна аутентифікація відіграє важливу роль у підвищенні безпеки мобільних пристроїв та захисту персональних даних користувачів.

Зростання загроз від шкідливого програмного забезпечення на мобільних пристроях вимагає розробки спеціалізованого антивірусного програмного забезпечення. У цьому розділі ми оглянемо основні функції і можливості такого ПЗ, його роль у виявленні і блокуванні шкідливих програм, а також практичне застосування на мобільних пристроях.

Антивірусне програмне забезпечення для мобільних пристроїв є спеціалізованим інструментом, призначеним для виявлення, блокування і видалення шкідливих програм, таких як віруси, троянські програми, шпигунське ПЗ та інші види загроз. Основні функції антивірусного ПЗ включають:

1. Сканування: Антивірусне ПЗ виконує регулярні сканування мобільного пристрою для виявлення потенційно шкідливих програм. Це може бути як сканування в режимі реального часу під час використання пристрою, так і заплановані або ручні сканування. Під час сканування антивірусне ПЗ порівнює

програми та файли з базою даних відомих загроз і сповіщає користувача про виявлені потенційні загрози.

2. Блокування інфікованих програм: Якщо антивірусне ПЗ виявить шкідливу програму на мобільному пристрої, воно може заблокувати доступ до неї або надати користувачеві можливість видалити її. Це дозволяє запобігти поширенню інфекції і захистити пристрій від подальших атак.

3. Оновлення бази даних загроз: Антивірусне ПЗ має базу даних, яка містить інформацію про відомі загрози. Щоб ефективно виявляти нові шкідливі програми, важливо регулярно оновлювати цю базу даних. Антивірусні компанії надають оновлення бази даних через інтернет, що дозволяє програмному забезпеченню розпізнавати найновіші загрози.

4. Захист в режимі реального часу: Антивірусне ПЗ може працювати в режимі реального часу, постійно перевіряючи активні програми і файли на наявність шкідливого коду. Це дозволяє швидко реагувати на потенційні загрози і блокувати їх до виконання.

Розробка антивірусного програмного забезпечення для мобільних пристроїв вимагає глибокого розуміння мобільних платформ, їхніх операційних систем і специфіки шкідливого програмного забезпечення, що цілять на мобільні пристрої. Компанії, що розробляють антивірусне ПЗ, активно вивчають нові методи атак і шляхи їхнього запобігання.

На практиці антивірусне програмне забезпечення використовується на мобільних пристроях для забезпечення безпеки персональних даних, захисту від крадіжки інформації, а також попередження втрати або пошкодження даних через шкідливе програмне забезпечення. Користувачі мають можливість встановити антивірусне ПЗ з офіційних джерел, таких як магазини додатків для мобільних пристроїв, і налаштувати його для автоматичних сканувань та оновлень бази даних. Антивірусне ПЗ стає необхідним елементом комплексної системи безпеки мобільних пристроїв, який сприяє захисту особистих даних та збереженню приватності користувачів.

Виявлення та відстеження загроз безпеки на мобільних пристроях - це процес, який розробники програмного забезпечення використовують для ідентифікації потенційних загроз безпеки та моніторингу активності, що може вказувати на вразливості або атаки. Ось детальніше про кожну складову цього процесу:

1. Аналіз активності додатків: Розробники можуть збирати дані про активність додатків на мобільному пристрої, такі як доступ до різних ресурсів (камера, мікрофон, геолокація), використання мережі, взаємодія з файловою системою тощо. Ці дані можуть бути аналізовані з метою виявлення підозрілої або небажаної активності, яка може свідчити про можливі загрози.

2. Виявлення вразливостей: Розробники можуть використовувати автоматизовані інструменти та техніки для виявлення вразливостей в мобільних пристроях. Це може включати сканування додатків на наявність відомих вразливостей, перевірку на виконання небезпечних операцій або аналіз вразливих компонентів операційної системи.

3. Попередження про потенційні атаки: Якщо розробники виявляють підозрілу активність або вразливості, вони можуть відправляти попередження або сповіщення користувачам про потенційні атаки або небезпеку. Це може бути реалізовано через системні повідомлення, електронну пошту, повідомлення в додатках або інші канали сповіщення.

4. Моніторинг загроз: Розробники можуть збирати дані про нові загрози безпеки, такі як нові види шкідливих програм, методи атак або вразливості, і використовувати ці дані для покращення системи виявлення і відстеження загроз. Це може включати постійне оновлення бази даних загроз, аналіз статистики атак або співпрацю зі спільнотою безпеки для обміну інформацією про нові загрози.

5. Реагування на загрози: Виявлені загрози можуть спричиняти розробку патчів, оновлення або виправлення, які розробники можуть випустити для усунення вразливостей або зменшення ризику атаки. Швидка реакція на виявлені загрози може допомогти забезпечити безпеку персональних даних на мобільних пристроях.

Вся ця діяльність має на меті виявлення потенційних загроз безпеки на мобільних пристроях та реагування на них шляхом вдосконалення системи безпеки і захисту персональних даних.

Управління правами доступу є важливим аспектом забезпечення безпеки персональних даних на мобільних пристроях. Ось детальніше про цей процес:

1. Дозволи на рівні додатків: Мобільні операційні системи надають можливість користувачам керувати дозволами, які надаються окремим додаткам. Користувач може встановлювати дозволи для кожного додатка окремо, забезпечуючи контроль над доступом до різних функціональних можливостей та персональних даних, таких як контакти, камера, мікрофон, геолокація і т.д. Наприклад, користувач може дозволити певному додатку доступ до геолокації, але відмовити у доступі до контактів.

2. Обмеження доступу до конкретних даних: Деякі мобільні операційні системи також надають можливість обмежувати доступ до конкретних категорій персональних даних в межах додатка. Наприклад, користувач може встановити, що додаток має доступ тільки до фотографій, але не до відео або інших файлів.

3. Запити на дозвіл: При встановленні нового додатка або під час виконання певних операцій деякі мобільні операційні системи можуть відображати запити на дозвіл. Користувач повинен затвердити ці запити, перш ніж додаток отримає доступ до певних даних або функціональності пристрою. Це дозволяє користувачеві усвідомлювати, яку інформацію отримує додаток і яким чином він її використовує.

4. Повторне перегляд дозволів: Крім того, користувачі мають можливість переглядати та змінювати дозволи, надані додаткам, в будь-який момент. Це дає їм змогу відкликати або змінювати доступ до своїх персональних даних в разі потреби.

Управління правами доступу дозволяє користувачам контролювати, які додатки мають доступ до їх персональних даних і як ці дані використовуються. Це є важливим кроком у підвищенні безпеки мобільних пристроїв і захисту приватності користувачів.

Можна зробити висновок, що всі вищезазначені методи удосконалюють безпеку персональних даних в межах мобільних пристроїв. Найефективніший буде результат якщо використовувати ці методи одночасно послідовно.

3.2 Критерії оцінки ефективності методів

Оцінка ефективності методу в системах безпеки мобільних пристроїв є важливим кроком у процесі розробки та впровадження нових заходів безпеки. Для оцінки ефективності можна використовувати критерії, такі як:

Рівень захисту: Ефективність методу може бути виміряна його здатністю запобігати несанкціонованому доступу до персональних даних. Чим вищий рівень захисту, тим ефективнішим вважається метод.

Швидкодія: Оцінка ефективності також може включати аналіз швидкодії методу. Наприклад, якщо використання певного методу безпеки суттєво зменшує продуктивність мобільного пристрою, це може вплинути на безпеку ваших даних та викликати незадоволення користувача.

Вартість: Вартість впровадження і підтримки методу також є важливим фактором при оцінці його ефективності. Метод повинен бути ефективним з фінансової точки зору, щоб бути прийнятним для широкого використання.

Оцінка ефективності може включати експериментальні дослідження, аналіз статистичних даних, взаємодію з користувачами та інші методи дослідження. Це дозволить зробити обґрунтовані висновки щодо ефективності методу і прийняти рішення про його використання в мобільних пристроях.

Далі буде проведений огляд різних методів вдосконалення систем безпеки персональних даних в межах мобільних пристроїв, а також надана рекомендація оцінки їх ефективності на основі вищезазначених критеріїв. Результати оцінки допоможуть визначити найбільш ефективні методи для покращення систем безпеки мобільних пристроїв.

Оцінка ефективності методу використання біометричних технологій для забезпечення безпеки на мобільних пристроях може включати такі критерії:

1. Рівень захисту: Використання біометричних технологій, таких як відбитки пальців, розпізнавання обличчя, розпізнавання ірису і т.д., може забезпечити високий рівень ідентифікації та запобігти несанкціонованому доступу до особистих даних. Оцінка ефективності буде включати оцінку надійності і точності розпізнавання, а також оцінку вразливостей до можливих атак, таких як використання фотографій або відбитків пальців.

2. Зручність використання: Ефективний метод повинен бути зручним для користувача. Використання біометричних технологій може забезпечити зручний спосіб ідентифікації, оскільки користувачу потрібно лише використовувати свої фізичні характеристики. Оцінка ефективності буде включати оцінку швидкості і простоти процесу розпізнавання, а також оцінку відсутності незручностей для користувача, наприклад, в разі поганого освітлення або фізичних обмежень.

3. Надійність і безпека: Використання біометричних технологій повинно забезпечувати надійність і безпеку даних користувача. Оцінка ефективності буде включати оцінку рівня захисту біометричних даних від несанкціонованого доступу і можливості їх підробки. Важливо також враховувати способи збереження і обробки біометричних даних, щоб уникнути їх використання в інших цілях або неправомірного доступу до них.

4. Сумісність та масштабованість: Ефективний метод повинен бути сумісним з різними мобільними пристроями і операційними системами, а також здатним масштабуватися для використання великою кількістю користувачів. Оцінка ефективності буде включати оцінку сумісності з різними пристроями і операційними системами, а також оцінку пропускної здатності системи при обробці великої кількості запитів.

Загальна оцінка ефективності методу використання біометричних технологій буде залежати від успішності виконання цих критеріїв та їх відповідності потребам та очікуванням користувачів мобільних пристроїв.

Оцінка ефективності методу використання шифрування для захисту даних на мобільних пристроях може включати такі критерії:

1. Рівень безпеки: Ефективність методу шифрування буде оцінюватися залежно від його здатності до надійного захисту даних від несанкціонованого доступу. Використання сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), який забезпечує високий рівень криптографічної безпеки. Оцінка ефективності включатиме оцінку стійкості шифрування до атак, включаючи брутфорс і криптоаналітичні атаки.

2. Захищеність інформації після втрати або крадіжки пристрою: Метод шифрування повинен забезпечувати захист даних, навіть якщо пристрій був втрачений або викрадений. Ефективність оцінюватиметься здатністю шифрування залишатися непорушеним при втраті фізичного доступу до пристрою, що запобігає несанкціонованому доступу до конфіденційних даних.

3. Продуктивність: Оцінка ефективності включатиме аналіз впливу шифрування на продуктивність мобільного пристрою. Шифрування даних може збільшити обчислювальне навантаження на пристрої, що може вплинути на швидкість роботи і час відгуку. Ефективний метод шифрування має бути оптимізований для мобільних пристроїв, забезпечуючи надійний захист і мінімальний вплив на продуктивність.

4. Управління ключами: Ефективність методу шифрування також буде визначатися його здатністю до ефективного управління ключами шифрування. Безпека шифрування залежить від безпечного зберігання та обміну ключами шифрування. Оцінка ефективності буде включати аналіз методів управління ключами та їх надійності.

Загальна оцінка ефективності методу використання шифрування буде залежати від успішності виконання цих критеріїв та їх відповідності вимогам до безпеки та функціональності мобільних пристроїв.

Оцінка ефективності методу розвитку двофакторної аутентифікації для мобільних пристроїв може включати наступні критерії:

1. Захист від несанкціонованого доступу: Ефективність методу двофакторної аутентифікації буде оцінюватися залежно від його здатності надійно захищати мобільний пристрій від несанкціонованого доступу.

Використання двох незалежних факторів ідентифікації, які можуть бути важкими для зламу або підробки, додає додатковий рівень безпеки.

2. Зручність використання: Оцінка ефективності включатиме аналіз зручності використання методу двофакторної аутентифікації для користувачів мобільних пристроїв. Метод повинен бути легким у налаштуванні та використанні, а також не надмірно обтяжувати користувача при авторизації.

3. Надійність факторів ідентифікації: Оцінка ефективності буде включати оцінку надійності факторів ідентифікації, які використовуються в методі двофакторної аутентифікації. Наприклад, використання відбитку пальця чи розпізнавання обличчя повинно бути достатньо точним і несхильним до підробки.

4. Масштабованість: Оцінка ефективності включатиме аналіз масштабованості методу двофакторної аутентифікації для використання великою кількістю користувачів. Метод повинен бути здатний обробляти багато запитів на авторизацію та підтримувати швидку і стабільну роботу в умовах великого навантаження.

5. Захист від атак: Оцінка ефективності буде включати аналіз захисту методу двофакторної аутентифікації від різних видів атак, таких як фішинг, перехоплення одноразового коду або злам пароля. Метод повинен мати механізми, які ускладнюють атаки та забезпечують безпеку користувачів.

Загальна оцінка ефективності методу розвитку двофакторної аутентифікації буде залежати від успішності виконання цих критеріїв та їх відповідності вимогам до безпеки та зручності використання мобільних пристроїв.

Оцінка ефективності методу розробки антивірусного програмного забезпечення для мобільних пристроїв може включати наступні критерії:

1. Виявлення шкідливого ПЗ: Ефективність методу буде оцінюватися залежно від його здатності виявляти різні види шкідливого програмного забезпечення, такі як віруси, троянські коні, шпигунські програми, рекламний софт та інші загрози безпеці. Метод повинен мати актуальні бази даних,

ефективні алгоритми та механізми виявлення для ефективного боротьби з шкідливим ПЗ.

2. Усунення загроз: Оцінка ефективності включатиме аналіз здатності методу до ефективного усунення виявлених загроз безпеці. Це може включати блокування, видалення або нейтралізацію шкідливого ПЗ, щоб запобігти його впливу на мобільний пристрій та дані користувача.

3. Захист в реальному часі: Оцінка ефективності буде включати аналіз здатності методу працювати в режимі реального часу, тобто постійно моніторити активність та перевіряти файли та додатки на наявність шкідливого ПЗ. Це дозволить виявляти та блокувати загрози миттєво, надаючи максимальний рівень захисту.

4. Вплив на продуктивність: Оцінка ефективності включатиме аналіз впливу методу на продуктивність мобільного пристрою. Відмінність полягає в здатності розробленого антивірусного програмного забезпечення до працювати ефективно та швидко, не сповільнюючи роботу пристрою або не викликаючи зайвих завантажень.

5. Оновлення та підтримка: Ефективність методу також буде оцінюватися залежно від наявності системи оновлень та підтримки. Розробник повинен регулярно надавати оновлення баз даних, сигнатур вірусів та програмного забезпечення, щоб забезпечити актуальний рівень захисту.

Загальна оцінка ефективності методу розробки антивірусного програмного забезпечення буде залежати від успішності виконання цих критеріїв та їх відповідності вимогам до безпеки, швидкості та ефективності застосування на мобільних пристроях.

3.3 Розробка методу, його перевірка та оцінка

Перед початком реалізації методу було створено емулятор Android девайсу за допомогою Android Studio та Virtual Device Manager.

Рисунок 3.1 – Запуск Android емулятора

Для реалізації було взято метод моніторингу різних параметрів та дій за допомогою ADB (Android Debug Bridge), мови програмування Python, Mitmproxy та Wireshark.

Спочатку було написано код, який за допомогою утиліти Frida підключається до нашого девайсу. Далі було створено функцію get_ip_address(), яка дізнається IP адресу нашого комп'ютера, для виконання функції enable_proxy(), яка налаштовує пристрій Android на використання вказаної IP-адреси та порту 8080 для HTTP-проксі. Також на даному фрагменті створюється функція run_command(), яка за допомогою команд, які будуть в неї передаватися, буде виконувати їх у командному рядку cmd. Та в кінці йде їх виконання, яке дає нам адресу комп'ютера, встановлення проксі, створення та перенос сертифікату для довіреного з'єднання.

```
import frida
import subprocess
import socket
import pyshark

device = frida.get_usb_device()
print(device.name)


def get_ip_address():
    hostname = socket.gethostname()
    ip_address = socket.gethostbyname(hostname)
    return ip_address


def enable_proxy(ip, port="8080"):
    output = run_adb_command(f"adb shell settings put global http_proxy {ip}:{port}")
    enable_proxy = output.split("\n")
    return enable_proxy


def run_command(command):
    path = " cd C:/Users/User/.mitmproxy"
    full_command = "C: && "+ path + " && " + command
    process = subprocess.Popen(full_command, stdout=subprocess.PIPE, stderr=subprocess.PIPE, shell=True)
    output, error = process.communicate()
    return 1


ipadr = get_ip_address()
enable_proxy(ipadr)


run_command("copy mitmproxy-ca.pem file.pem")
run_command("openssl x509 -inform PEM -text -in mitmproxy-ca.pem -out nul >> file.pem")
run_command("adb shell mount -o rw,remount,rw /system")
run_command("adb push file.pem /system/etc/security/cacerts/")
run_command("adb shell mount -o ro,remount,ro /system")
run_command("adb reboot")
```

Рисунок 3.2 – Основні налаштування програми

Далі були розроблені функції, які допомогають отримати різну інформацію про мобільний пристрій. Ця інформація може бути використана для аналізу та виявлення потенційно шкідливих чи несанкціонованих дій.

```
def logcat():
    output = run_adb_command('adb logcat -d')
    logcat = output.split('\n')
    return logcat


def memory_info():
    output = run_adb_command('adb shell dumpsys meminfo')
    meminfo = output.split('\n')
    return meminfo


def ps():
    output = run_adb_command('adb shell ps')
    pss = output.split('\n')
    return pss


def active_services():
    output = run_adb_command('adb shell dumpsys activity services')
    services = output.split('\n')
    return services


def installed_packages():
    output = run_adb_command('adb shell pm list packages | findstr /v "android"')
    packages = output.split('\n')
    return packages


def filesystem_info():
    output = run_adb_command('adb shell df')
    filesystem_info = output.split('\n')
    return filesystem_info


def tcp_connections():
    output = run_adb_command('adb shell su root netstat -tulpn')
    connections = output.split('\n')
    return connections

def capture_and_save():
    output = run_adb_command('adb shell su root timeout 15 "/data/local/tmp/tcpdump -w /sdcard/dump.pcap -s 0 -v" && adb pull /sdcard/dump.pcap')
    print("ok")
    return True
```

Рисунок 3.3 – Розроблені функції

logcat(): Ця функція використовує команду ADB 'logcat -d' для отримання логів системи. Логи можуть містити інформацію про різні події та повідомлення, включаючи помилки, попередження, інформаційні повідомлення тощо.

memory_info(): Ця функція використовує ADB 'shell dumpsys meminfo' для отримання інформації про використання пам'яті на пристрої. Це може бути корисно для визначення, чи є якісь процеси, які використовують надзвичайно велику кількість пам'яті, що може вказувати на несанкціоновану активність.

ps(): Ця функція використовує ADB 'shell ps' для отримання списку всіх запущених процесів на пристрої. Це може допомогти визначити, чи виконуються якісь підозрілі процеси у фоновому режимі.

installed_packages(): Ця функція використовує ADB 'shell pm list packages' для отримання списку всіх встановлених пакетів (додатків) на пристрої. Ця інформація може бути корисною для визначення, чи встановлено якийсь підозрілий або невідомий додаток.

active_services(): Ця функція використовує ADB 'shell dumpsys activity services' для отримання списку всіх активних сервісів на пристрої. Сервіси зазвичай працюють у фоновому режимі та виконують завдання, такі як синхронізація даних, виконання завантажень тощо. Наявність невідомих чи підозрілих служб може вказувати на несанкціоновану активність.

filesystem_info(): Ця функція використовує команду ADB 'shell df' для отримання інформації про файлову систему пристрою, включаючи використання дискового простору. Це може бути корисним для визначення, чи є якісь незвичайні зміни у використанні дискового простору, які можуть вказувати на несанкціоновану активність.

tcp_connections(): Ця функція використовує команду ADB 'adb shell su root netstat -tulpn' для отримання списку активних TCP-з'єднань на пристрої. Ця інформація може бути корисною для визначення активного мережевого спілкування на пристрої, що може вказувати на несанкціоновану активність.

capture_and_save(): Ця функція використовує команду ADB 'adb shell su root timeout * "/data/local/tmp/tcpdump -w /sdcard/dump.pcap -s 0 -v" && adb pull /sdcard/dump.pcap' для створення дампа пакетів на емуляторі на протязі певного часу і збереження цього дампа на пристрої де запускається скрипт. Ця інформація може бути корисною для аналізу трафіку, що проходить через пристрій, для виявлення можливої несанкціонованої мережевої активності.

Також було написано функцію за допомогою бібліотики pyshark, яка робить перевірку на наявність Malformed в пакетах, для виявлення підозрілих дій. Данна

інформація може допомогти, коли ми будемо дивитися пакети у Wireshark та аналізувати їх.

```
def malformed_check():
    capture = pyshark.FileCapture('dump.pcap')
    for packet in capture:
        if 'Malformed' in str(packet):
            print(packet)
```

Рисунок 3.4 - Функція перевірки дампу

Mitmproxy - це вільний та відкритий мережевий проксі, який дозволяє перехоплювати, переглядати та модифікувати HTTP та HTTPS трафік. Це корисний інструмент для налагодження мережевих запитів, тестування безпеки та навчання.

В нашому випадку його було налаштовано для перехоплення підозрілого трафіку на мобільному пристрої, для подальшого аналізу.

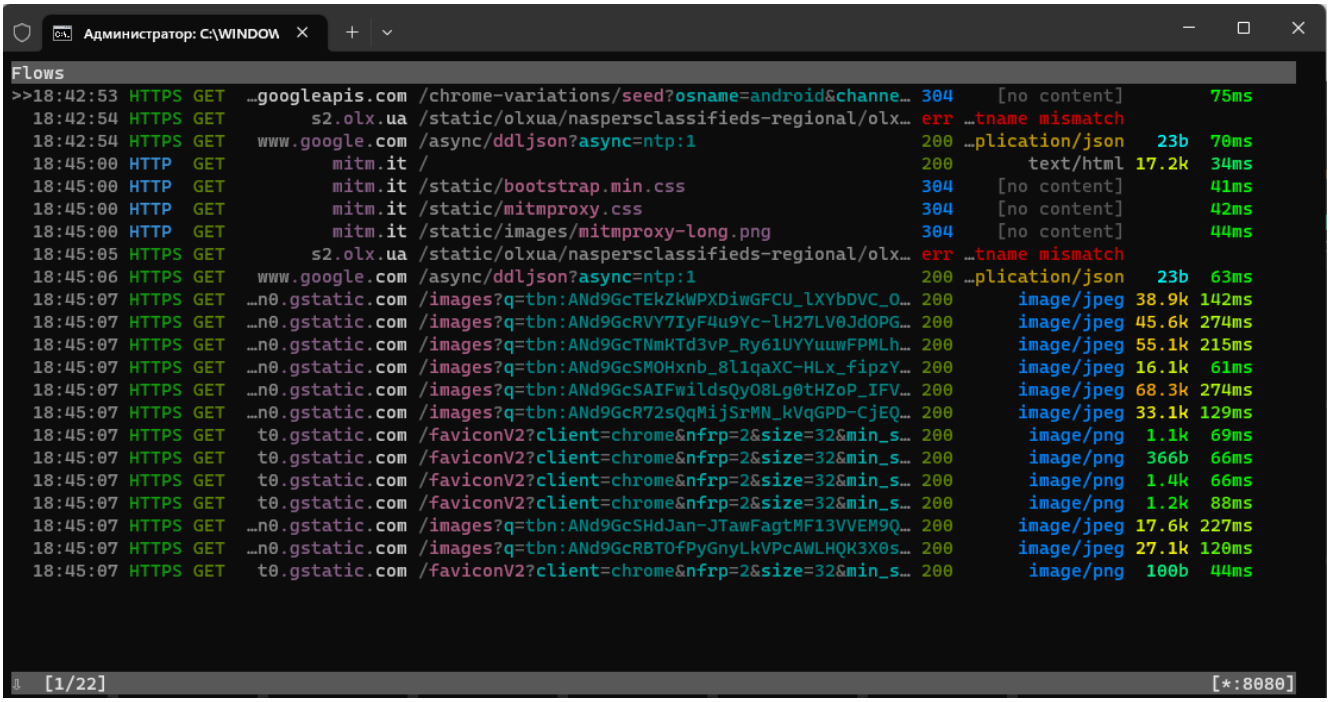

Рисунок 3.5 – Перехват трафік за допомогою MitmProxy

Комбінування результатів цих функцій та аналізу перехвату трафіку дозволяє виявити підозрілу активність та вжити відповідних заходів щодо забезпечення безпеки мобільного пристрою.

Перевірка методу:

Для перевірки методу було використано троянське програмне забезпечення AndroRat, яке завантажилось на наш емулятор.

AndroRAT (Android Remote Administration Tool) це шкідливе програмне забезпечення, призначене для віддаленого керування пристроєм Android без відома користувача. AndroRAT дозволяє атакуючому отримати доступ до інформації на пристрої, такому як SMS, дзвінки, камера, мікрофон, і навіть керувати функціями пристрою, такими як дзвінки та SMS.

AndroRAT може бути прихований всередині програми та встановлено на пристрій без відома користувача. Коли це відбувається, атакуючий може керувати пристроєм віддалено та отримувати доступ до особистої інформації користувача.

Для початку було розгорнуто віртуальну машину Kali Linux, з якої буде виконуватися несанкціонований доступ до нашого емулятора. Після цього було склоновано та налаштовано AndroRAT з такого ресурсу як GitHub[25].

Потім було створено APK файл, який буде в майбутньому завантажений на наш емулятор Android

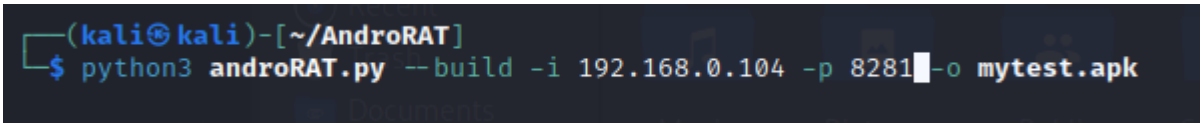

Рисунок 3.6 – Створення APK файлу

Наступним кроком було запуск прослуховувача, який буде чекати на підключення емулятора телефону.

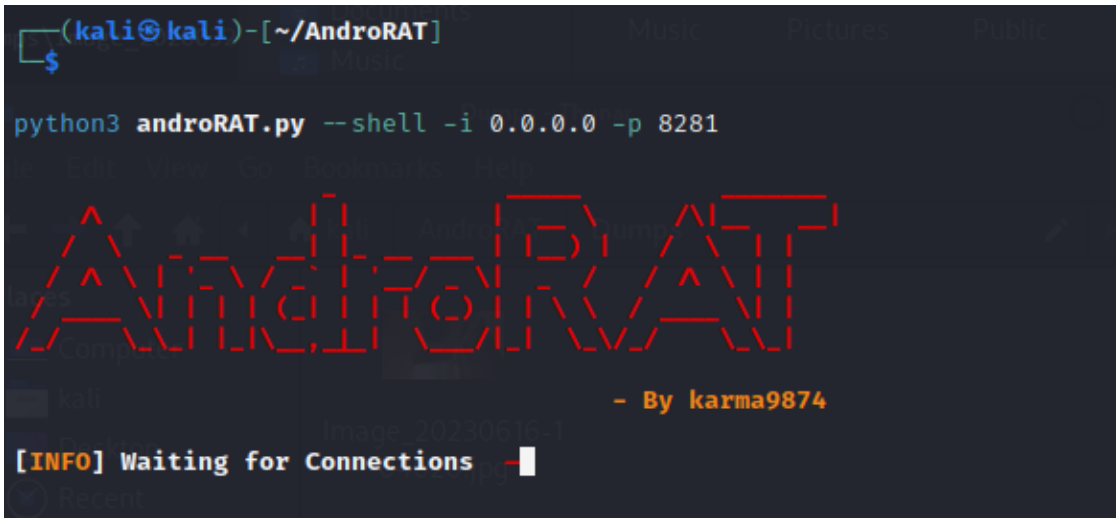

Рисунок 3.7 – Запуск прослуховувача

Було зроблено перекидку APK файлу, та завантажено його на емулятор.

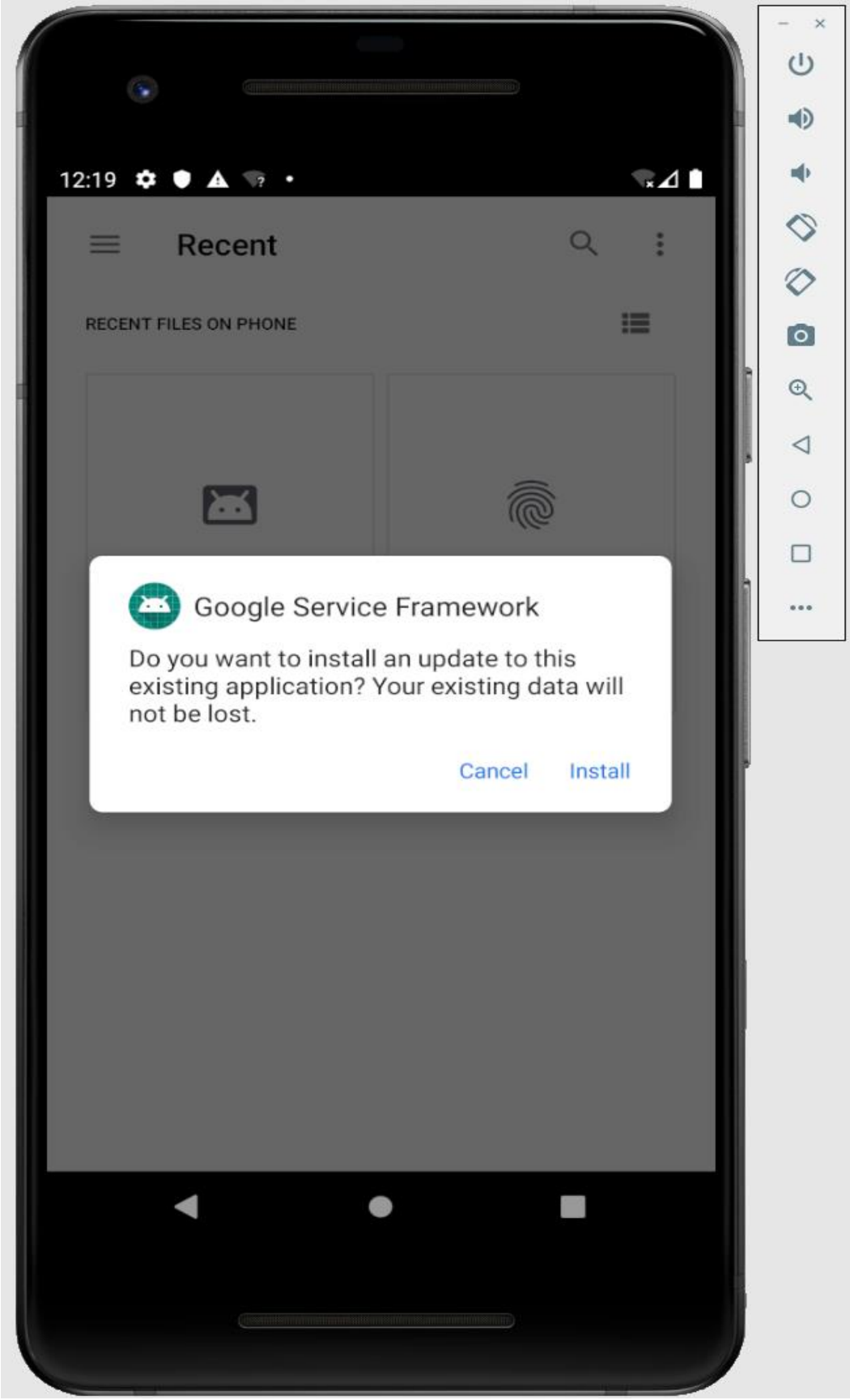

Рисунок 3.8 – Встановлення емулятора

Після встановлення на емулятор, на віртуальній машині оновлюється консоль і отримується несанкціонований доступ до мобільного пристрою. Можна побачити функціонал ПЗ у консолі.

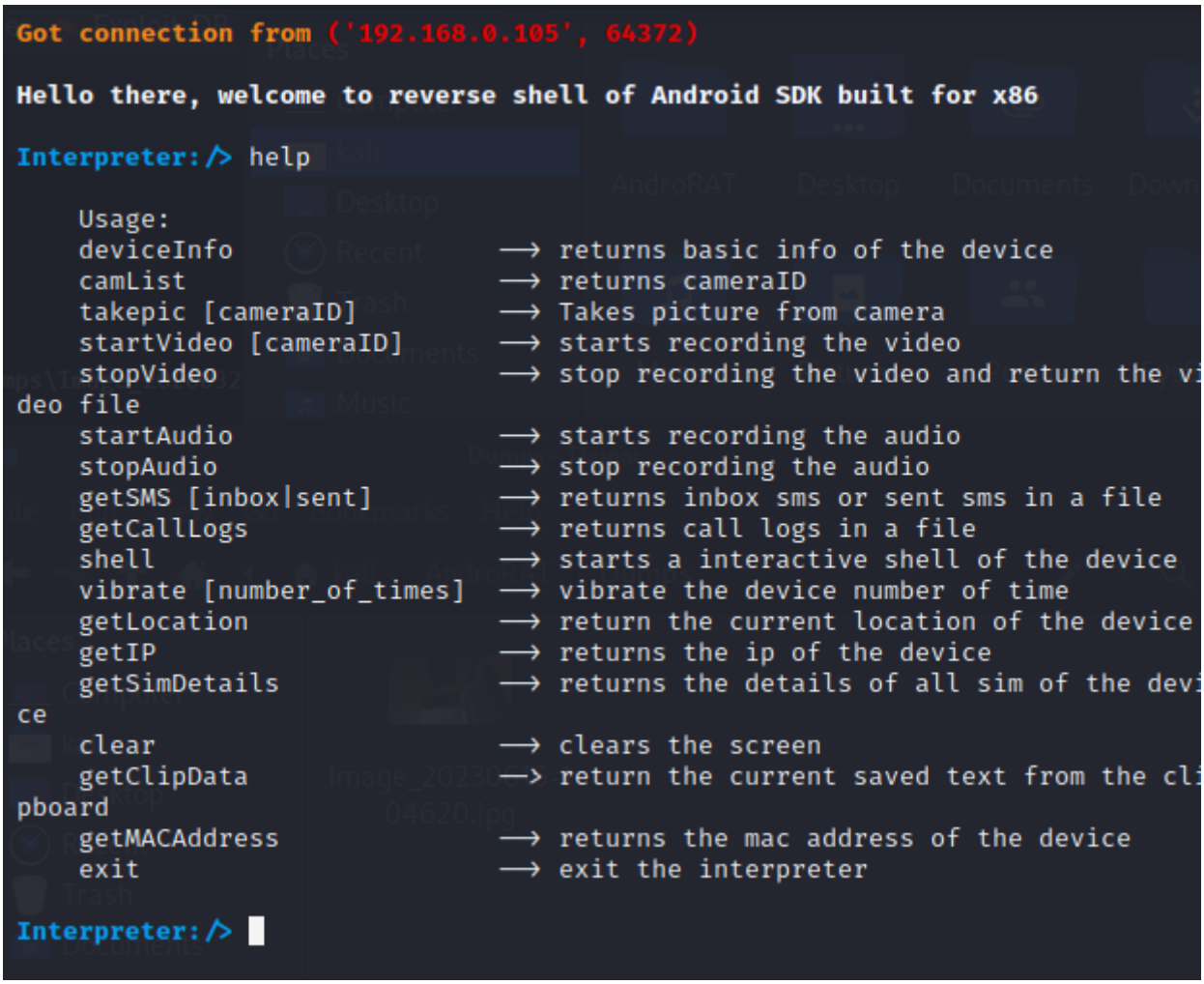

Рисунок 3.9 - Функціонал ПЗ AndroRat

Для прикладу було зроблено декілька дій відносно гаджету.

Першим було зроблено фото з нашого мобільного пристрою через камеру.

Рисунок 3.10 – Виконная фото на мобільному пристрою.

Результат зберігається у папці Dumps на віртуальній машині

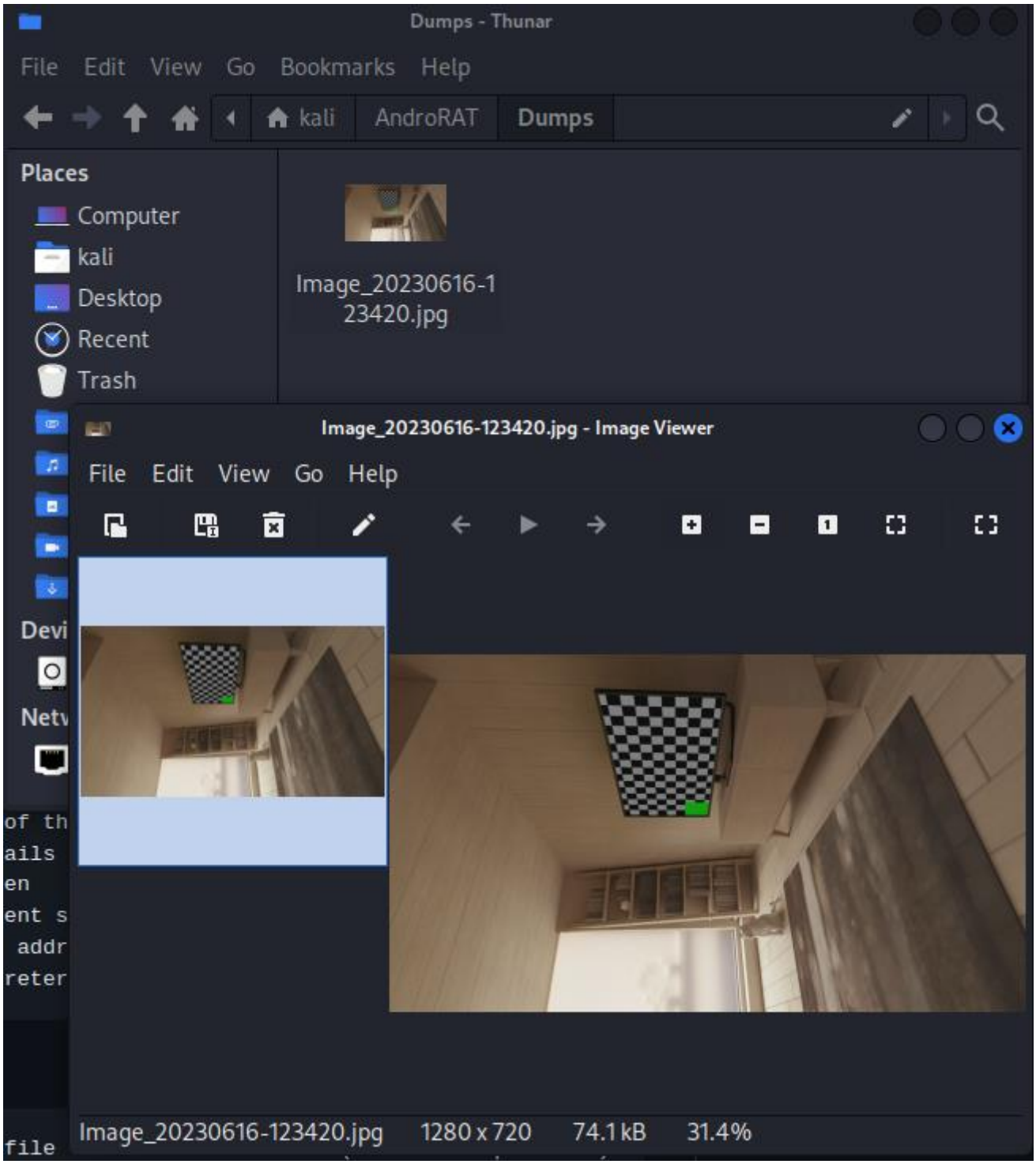

Рисунок 3.11 - Зберігання фото на віртуальній машині

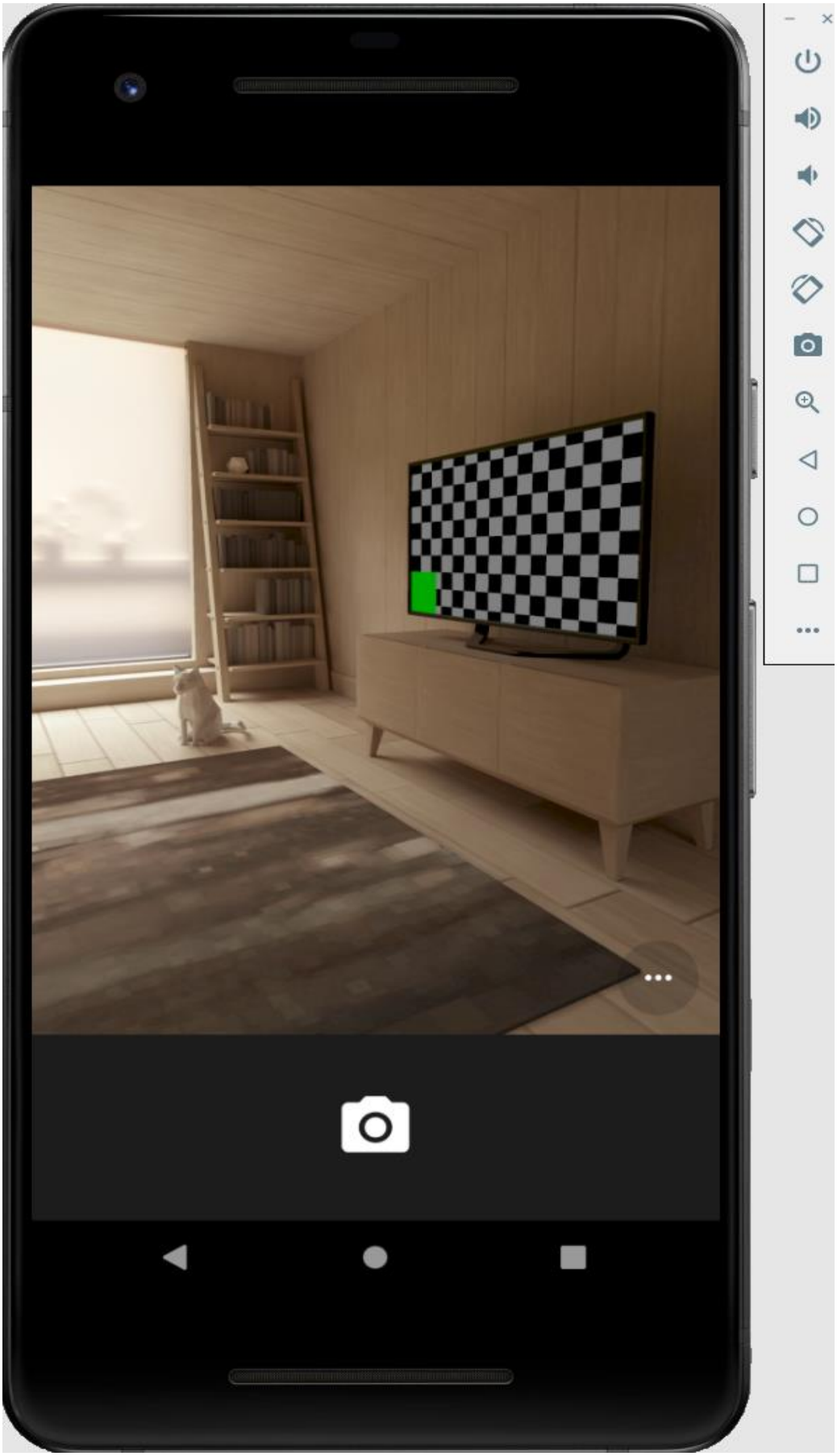

Рисунок 3.12 - Фото на емуляторі телефона

Потім було записано аудіо з мобільного пристрою.

```
Interpreter:/> startAudio
Started Recording Audio

Interpreter:/> stopAudio
[INFO] Downloading Audio
[SUCCESS] Succesfully Saved in /home/kali/AndroRAT/Dumps/Audio_20230616-124059.mp3
```

Рисунок 3.13 - Запис аудіо

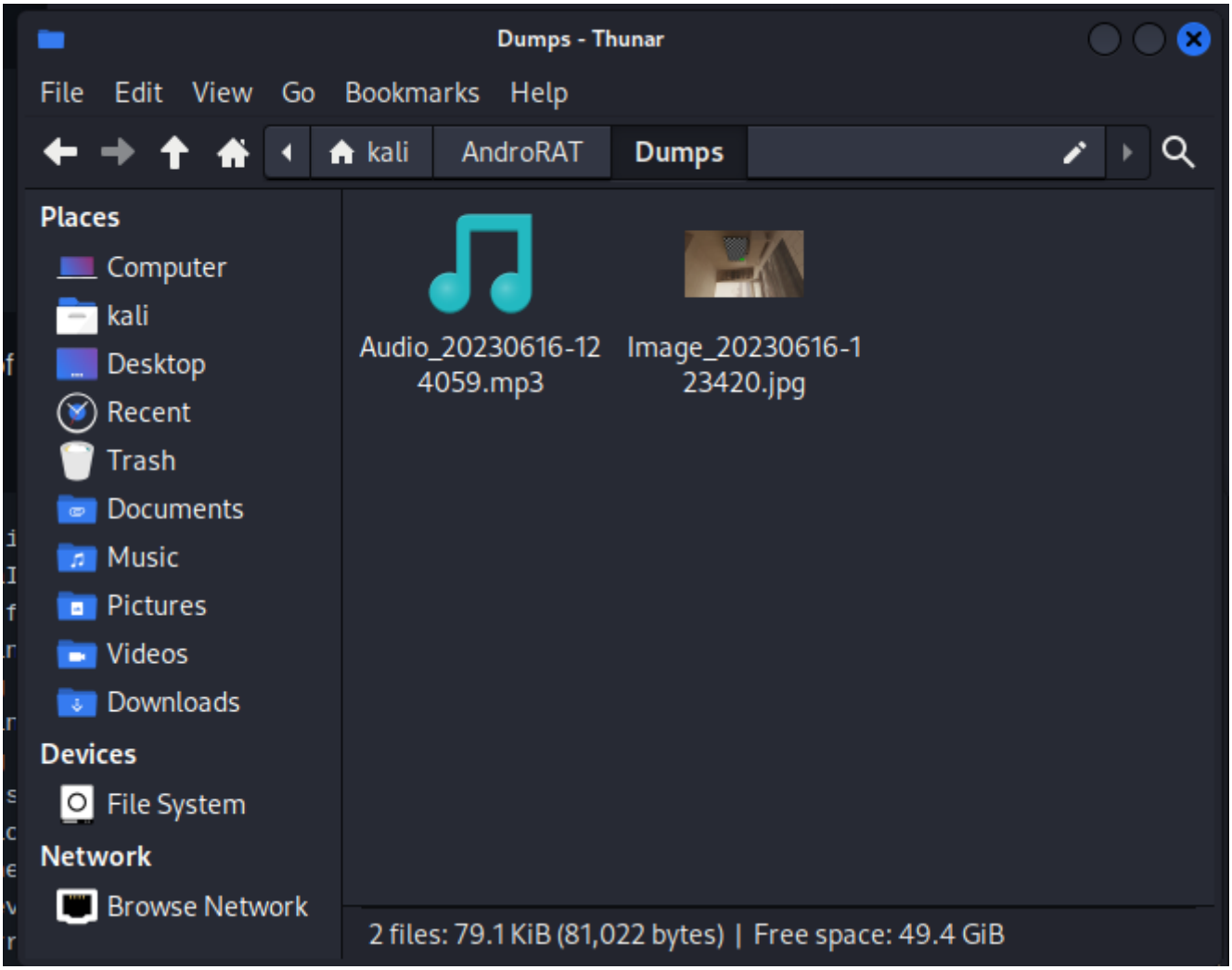

Рисунок 3.14 - Результат аудіо на віртуальній машині

Та останнім було імітуватування вібрації на мобільному пристрої дистанційно.

```
Interpreter:/> vibrate 2
Vibrating 2 time successful.
```

Рисунок 3.15 – Вібрація на телефоні

Тепер ми можемо перевірити метод.

Для початку використаємо функцію logcat(), щоб подивитися наші логи, та проведемо їх аналіз.

Під час аналізу логів було виявлено підозрілу активність, яка може вказувати на несанкціонований доступ мобільного пристрою. Було помічено виконання таких дій, які вмикали камеру та робили з неї фото, робили запис аудіо, та змушували гаджет вмикати функцію вібрації без втручання самого власника пристрою.

```
06-16 12:34:19.780  6562 17133 D tcpConnectionClass: takepic 0
06-16 12:34:19.780  1865  2302 I CameraService: CameraService::connect call (PID -1 "com.example.reverseshell2", camera ID 0) for HAL version defa
06-16 12:34:19.784  1865  2302 I Camera2ClientBase: Camera 0: Opened. Client: com.example.reverseshell2 (PID 6562, UID 10134)
06-16 12:34:19.791  1784  1784 W HwBinder:1784_3: type=1400 audit(0.0:162): avc: denied { read } for name="u:object_r:default_prop:s0" dev="tmpfs"
06-16 12:34:19.791  1784  1784 W HwBinder:1784_3: type=1400 audit(0.0:163): avc: denied { read } for name="u:object_r:default_prop:s0" dev="tmpfs"
06-16 12:34:19.800  1784  1941 E libc    : Access denied finding property "ro.camera.req.fmq.size"
06-16 12:34:19.800  1784  1941 E libc    : Access denied finding property "ro.camera.res.fmq.size"
06-16 12:34:19.812  1865  2302 E Camera2-Parameters: Error finding static metadata entry 'android.distortionCorrection.availableModes' (1b0001)
06-16 12:34:19.812  1865  2302 I Camera2-Parameters: Camera 0: Disabling ZSL mode
06-16 12:34:19.812  1865  2302 I Camera2-Parameters: initialize: allowZslMode: 0 slowJpegMode 0
06-16 12:34:19.823  1865  3526 E Camera3-Device: configureStreams: Stream 1: DataSpace override not allowed for format 0x21
06-16 12:34:19.825  1865  3526 D Camera3-Device: Set real time priority for request queue thread (tid 18323)
```

Рисунок 3.16 – Вмикання камери, та виконання фото

```
06-16 12:38:20.390  6562 18467 D tcpConnectionClass: startAudio
06-16 12:38:20.414  1792  2249 E GnssHAL_GnssInterface: gnssSvStatusCb: a: input svInfo.flags is 8
06-16 12:38:20.414  1792  2249 E GnssHAL_GnssInterface: gnssSvStatusCb: b: input svInfo.flags is 8
06-16 12:38:20.415  1792  2249 E GnssHAL_GnssInterface: gnssSvStatusCb: a: input svInfo.flags is 8
06-16 12:38:20.415  1792  2249 E GnssHAL_GnssInterface: gnssSvStatusCb: b: input svInfo.flags is 8
06-16 12:38:20.419  1879  1960 W StagefrightRecorder: stop while neither recording nor paused
06-16 12:38:20.422  1879  1960 I Codec2Client: Creating a Codec2 client to service "software"
06-16 12:38:20.422  1879  1960 I Codec2Client: Client to Codec2 service "software" created
```

Рисунок 3.17 – Запуск записування аудіо

```
06-16 12:38:27.137  6562 18467 D tcpConnectionClass: stopAudio
06-16 12:38:27.163  1879  1960 D MPEG4Writer: Audio track stopping. Stop source
06-16 12:38:27.163  1879  1960 D MPEG4Writer: Audio track source stopping
06-16 12:38:27.163  1879 18504 I MediaCodecSource: encoder (audio) stopping
06-16 12:38:27.168  1879 18513 I MPEG4Writer: Received total/0-length (333/0) buffers and encoded 333 frames. - Audio
06-16 12:38:27.168  1879 18513 I MPEG4Writer: Audio track drift time: 0 us
06-16 12:38:27.171  1879 18504 I MediaCodecSource: encoder (audio) stopped
06-16 12:38:27.186  1879  1960 D MPEG4Writer: Audio track source stopped
06-16 12:38:27.186  1879  1960 D MPEG4Writer: Audio track stopped. Stop source
06-16 12:38:27.186  1879  1960 D MPEG4Writer: Stopping writer thread
06-16 12:38:27.186  1879 18511 D MPEG4Writer: 0 chunks are written in the last batch
06-16 12:38:27.186  1879  1960 D MPEG4Writer: Writer thread stopped
```

Рисунок 3.18 – Завершення записування аудіо

```
06-16 12:48:44.348  6562 19093 D tcpConnectionClass: vibrate 2
06-16 12:48:44.395  2021  4677 E VibratorService: vibratorOff command failed (1).
06-16 12:48:44.399  1679  1679 I hwservicemanager: getTransport: Cannot find entry android.hardware.vibrator@1.0::IVibrator/default in either fra
06-16 12:48:44.400  2021  4677 E VibratorService: vibratorOn command failed (1).
06-16 12:48:44.902  2021  2021 E VibratorService: vibratorOff command failed (1).
06-16 12:48:45.201  2021  4677 E VibratorService: vibratorOff command failed (1).
06-16 12:48:45.201  2021  4677 E VibratorService: vibratorOn command failed (1).
```

Рисунок 3.19 – Вмикання функції вібрації

Як ми можемо бачити, підозрілі дії виконуються за допомогою команд, які використовують через tcp з’єднання. Тому ми можемо створити за допомогою capture_and_save() дамп пакетів на емуляторі і зберегти цей дамп на пристрій, де запускається скрипт, для подальшого аналізу.

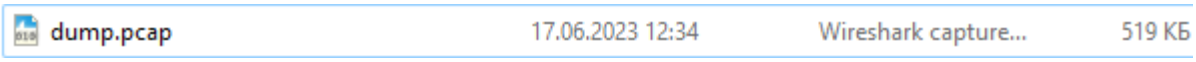

Рисунок 3.20 – Дамп створений на емуляторі

Після цього ми можемо зробити його аналіз, запустимо функцію malformed_check(). Ми бачемо, що виявило Malformed пакет.

```
    TCP payload (10 bytes)
Layer _WS.MALFORMED
:   Expert Info (Error/Malformed): Malformed Packet (Exception occurred)
    Malformed Packet (Exception occurred)
    Severity level: Error
    Group: Malformed
```

Рисунок 3.21 - Malformed пакет

Тут ми можемо провести аналіз цього пакету. Отримуємо IP адресу звідки та куди йшла команда, та порти, з якого і на який відправлялася команда.

```
    Protocol: TCP (6)
    Header Checksum: 0x3615 [validation disabled]
    Header checksum status: Unverified
    Source Address: 192.168.0.104
    Destination Address: 10.0.2.17
Layer TCP
:   Source Port: 8282
    Destination Port: 40104
```

Рисунок 3.22 – IP та порти

Зробимо аналіз у Wireshark з отриманих даних. Введемо фільтр по адресі, та по malformed пакетам. Як можемо побачити, це та сама команда

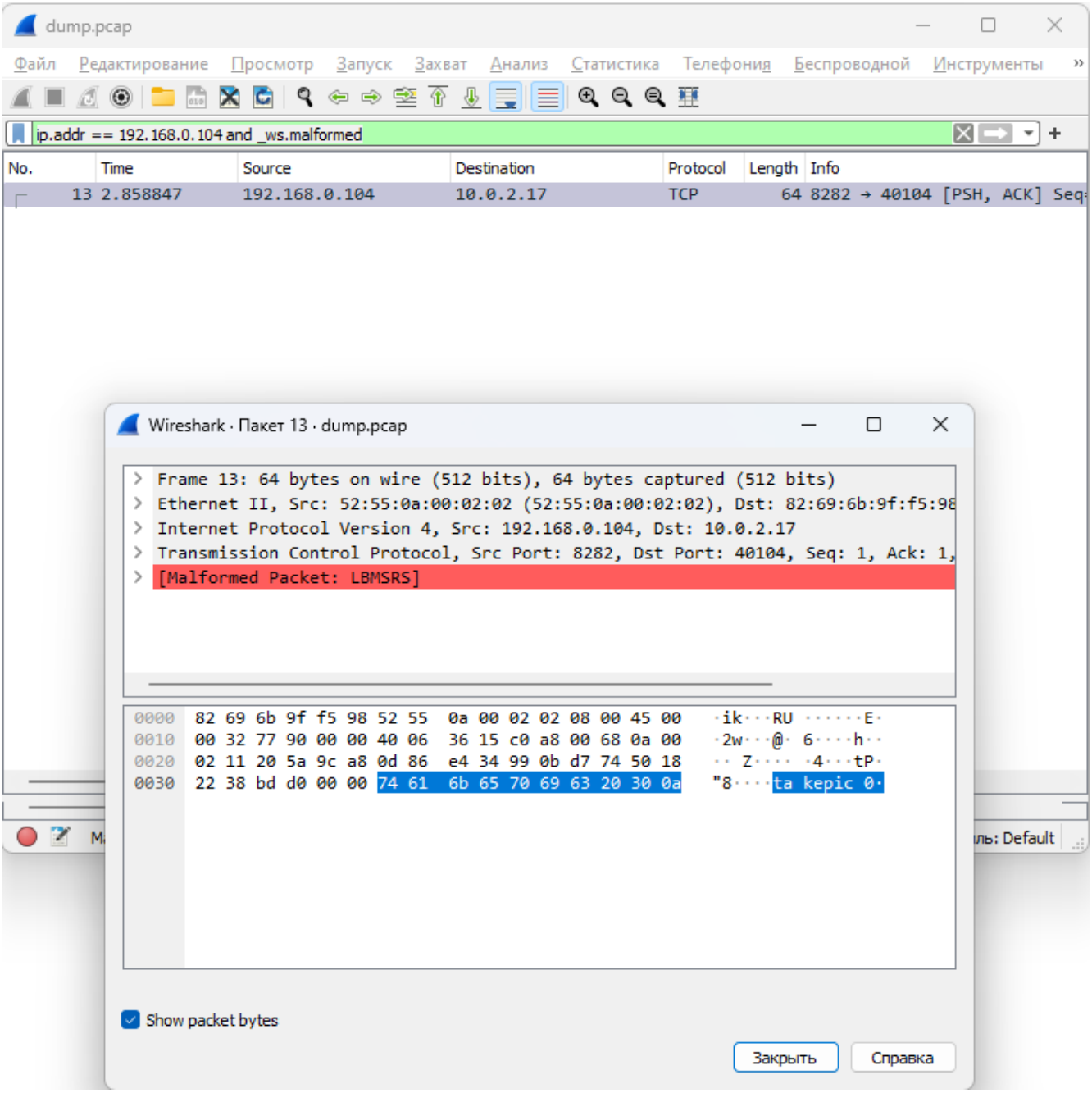

Рисунок 3.23 – Перегляд пакету у Wireshark

Дивимось що в нас працює на порті 40104 мобільного емулятора за допомогою функцію tcp_connections().

```
Android Emulator 5556
TCP-Підключення:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp6       0      0 ::ffff:10.0.2.17:42650  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42640  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:40104  ::ffff:192.168.0.1:8282 ESTABLISHED 7183/com.example.reverseshell2
tcp6       0      0 ::ffff:10.0.2.17:42638  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42664  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42644  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42632  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42634  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42652  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42646  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42660  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42656  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:42658  ::ffff:192.168.0.1:8080 TIME_WAIT   -
tcp6       0      0 ::ffff:10.0.2.17:53368  ::ffff:108.177.14.:5228 ESTABLISHED 2530/com.google.android.gms.persistent
udp        0      0 0.0.0.0:40812           0.0.0.0:*                           1826/mdnsd
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           1826/mdnsd
udp6       0      0 :::35825                ::::*                               1826/mdnsd
udp6       0      0 :::5353                 ::::*                               1826/mdnsd
```

Рисунок 3.24 – Отримання наявних TCP з’єднань

Як можна побачити, на пристрої працює якийсь підозрілий пакет.

Також можна цей пакет подивитися за допомогою функції installed_packages().

```
package:com.android.theme.color.orchid
package:com.android.systemui
package:com.android.theme.color.purple
package:com.android.bluetoothmidiservice
package:com.example.reverseshell2
package:com.android.traceur
package:com.android.bluetooth
```

Рисунок 3.25 - Встановлений пакет

Цей пакет може виявитись шкідливий ПЗ, тому краще за все позбутися його.

Для доказу, що це те саме шкідливе ПЗ, дізнаємося package name APK файлу. Зі скріншоту видно, що це він.

```
┌──(kali㉿kali)-[~/AndroRAT]
└─$ aapt dump badging mytest.apk | grep package:\ name
package: name='com.example.reverseshell2' versionCode='1' versionName='1.0' c
ompileSdkVersion='29' compileSdkVersionCodename='10'
```

Рисунок 3.26 – Package name APK файлу

На прикладі троянської програми AndroRat можна зробити висновок, що метод працює, але для його успіху потрібно робити додатковий аналіз з отриманої інформації, як це було продемонстровано вище. Метод включає в себе багато способів виявлення несанкціонованого доступу, проте не всі вони можуть видавати потрібний результат одночасно. Залежно від ситуації та загрози, кожен спосіб з цього методу може дати корисну інформацію для виявлення несанкціонованого доступу, будь-то підозрілий процес, сервіс, пакет, трафік і т.д.

Оцінка ефективності методу

Після реалізації цього методу можно зробити оцінку за критеріями, які були розроблені в пункті 3.2.

Рівень захисту:

Метод може бути корисним для моніторингу стану системи, але він має обмежену ефективність для виявлення несанкціонованого доступу в реальному часі. Цей метод дозволяє виявити підозрілі процеси або застосунки, але він не зможе запобігти вторгненню або заблокувати зловмисний софт в реальному часі. Таким чином, рівень захисту може бути оцінений як помірний.

Швидкодія:

Цей метод базується на виконанні команд ADB та перехваті мережового трафіку, які в основному не вимагають значного обсягу ресурсів, тому вони не повинні значно впливати на продуктивність пристрою. Проте залежно від кількості і частоти виконання команд, вони можуть стати витратними. Швидкодія цього методу вважається помірною.

Вартість:

ADB, Mitmproxy, Wireshark являються відкритими інструментами, доступними безкоштовно, тому вартість впровадження цього методу є низькою. Оскільки він вимагає лише програмного забезпечення, не потрібно жодних додаткових витрат на обладнання. Водночас, враховуючи потребу в професійних навичках для використання цього методу, можливі додаткові витрати на навчання персоналу, якщо метод використовується у компанії. Враховуючи це, оцінка вартості цього методу може бути визнана високою.

Висновки до розділу 3

Один з найважливіших напрямків вдосконалення полягає в установці сильних паролів і механізмів аутентифікації. Використання багатофакторної аутентифікації, включаючи відбитки пальців, розпізнавання обличчя або коди доступу, дозволяє забезпечити високий рівень безпеки та запобігти несанкціонованому доступу до персональних даних. Також важливо вдосконалювати заходи безпеки на рівні операційної системи мобільного пристрою. Регулярні оновлення програмного забезпечення та встановлення оновлень безпеки дозволяють заповнювати вразливості і захищати пристрій від нових загроз.

Врахування конфіденційності та приватності користувачів є ще одним важливим аспектом удосконалення систем безпеки. Розробка та впровадження політик захисту персональних даних, включаючи збирання та обробку даних лише з необхідною метою, може забезпечити користувачам контроль над їхніми персональними даними та зменшити ризики порушення приватності.

Застосування цих методів удосконалення систем безпеки до персональних даних на мобільних пристроях дозволяє забезпечити високий рівень захисту та довіру користувачів. Ці методи вимагають постійного вдосконалення та оновлення, оскільки загрози безпеці постійно еволюціонують. Важливо підтримувати усвідомлення про безпеку серед користувачів та впроваджувати найновіші технології та методики для захисту персональних даних на мобільних пристроях та запобігати несанкціонованому доступу до персональних даних.

В даному розділі було реалізовано метод моніторингу різних параметрів та дій за допомогою ADB (Android Debug Bridge), мови програмування Python, Mitmproxy та Wireshark.

Метод було перевірено на практиці, за допомогою нього, вдалося виявити підозрілу активність на мобільному пристрої, яка виконувалася через троянське ПЗ AndroRat.

Також метод було оцінено за створеними критеріями ефективності.

ВИСНОВКИ

У даній бакалаврській роботі була розглянута тема "Методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів". Метою дослідження було розроблення методу, що дозволяє виявляти несанкціонований доступ до мобільних гаджетів з використанням динамічного аналізу та зробити оцінку даного методу за розробленими критеріями

У ході виконання роботи було проведено аналіз існуючих методів виявлення несанкціонованого доступу до мобільних гаджетів, включаючи статичний та динамічний аналіз програмного забезпечення. Були проаналізовані сучасні технології та інструменти для забезпечення безпеки мобільних пристроїв.

На основі проведеного аналізу було розроблено метод динамічного виявлення несанкціонованого доступу, який поєднує в собі переваги існуючих підходів ефективного виявлення шкідливого програмного забезпечення та несанкціонованого доступу до мобільних гаджетів. Цей метод було перевірено на практиці та оцінено за критеріями та рекомендаціями, які були розроблені під час виконання роботи.

Отже, розроблений метод, критерії та рекомендації для оцінки ефективності мають практичне значення для захисту мобільних гаджетів від несанкціонованого доступу та потенційно шкідливих програм. Вони можуть бути використані в організаціях та використовуватися звичайними користувачами мобільних пристроїв для забезпечення безпеки та конфіденційності даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Андреєв В.І. Стратегія управління інформаційною безпекою / В.І. Андреєв, С.Д. Козюра, Л.М. Скачек, В.О. Хорошко – К: ДУІКТ, 2007. – 277 с. Бурячок В.Л. Політика інформаційної безпеки / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко – К: ВПП «Задруга», 2014. – 222 с. Коженевський С.Р. Термінологічний довідник з технічного захисту інформації на об’єктах інформаційної діяльності / С.Р. Коженевсь- кий, Г.В. Кузнєцов, В.О. Хорошко, Д.В. Чирков / К: ДУІКТ, 2007. – 365 с.

2. Головань С.М. Нормативно – правове забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко – Луганськ: ВИД Наука, 2012. – 480 с.
Андреєв В.І. Основи інформаційної безпеки. Вид. 2-е / В.І. Андреєв, С.Д., В.О. Хорошко, В.С. Чередніченко, М.Є. Шелест – К: ДУІКТ, 2009. – 292 с.

3. Дудикевіч В.Б. Основи інформаційної безпеки / В.Б. Дудикевіч, В.О. Хорошко, Ю.Є. Яремчук – Вінниця: ВНТУ, 2018. – 316 с.
Єжова Л.Ф. Управління інформаційною безпекою: підручник : у 2 т., Т. 1 / Л.Ф.Єжова, А.О. Корченко, І.О. Мачалін, Л.М. Скачек, В.О. Хорошко. - К., 2012. - 369 с.

4. Антивірусний захист комп'ютерних систем. URL: http://www.intuit.ru/studies/courses/2259/155/info

5. Віруси та засоби боротьби з ними. URL:: http://www.intuit.ru/studies/courses/1042/154/info

6. Фейнштайн К. Захист ПК від спаму, вірусів, спливаючих вікон та шпигунських програм / Кен Фейнштайн; Пров. з англ. О.Б.Версіної. - М.: НТ Прес, 2005. - 240 с.

7. Лєнков С.В. Методи та засоби захисту інформації. У 2-х томах/С.В. Лєнков, Д.А. Перегудов, В.А. Хорошо - К: Арій, 2008.

8. Блаватська Н.М. Програмне забезпечення систем захисту інформації/Н.М. Блаватська, В.Д. Козюра, В.О. Хорошо - К: Вид. ДУІКТ, 2011. - 330 с.

9. Указ Президента України від 22.05.1998 р. No 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні».

10. Указ Президента України від 11.02.1998 р. No 110/98 «Про заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних та інформаційних системах».

11. Діффі У., Хеллмен М.Е. Нові напрямки у криптографії. TIIEP, No 22, 1976, с. 644-654.

12. Шеннон К. Теорія зв'язку у секретних системах. У «Роботи з теорії інформації та кібернетиці», с. 333-402, - М.: Изд. ІЛ, 1963. Мухачов В.А., Хорошко В.А. Методи практичної криптографії. - К.: ТОВ "Поліграф-Консалтинг", 2005. - 215 с.

13. Кузнецов О.О. Захист інформації в інформаційних системах – О.О. Кузнецов, С.П. Євсеєв, О.Г. Король – Харків: ХНЕУ, 2011. – 512 с.

14. Гулак Г.М. Основи криптографічного захисту інформації / Г.М. Гу- лак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук – Вінниця: ВНТУ, 2011. – 199 с.

15. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Ме- льник, Р. Попович – Львів: БаК, 2003. – 144 с.

16. Горбенко І.Д. Прикладна криптографія. Теорія, практика, застосування / І.Д. Горбунко, Ю.І. Горбенко – Харків: ВИД. «Форт», 2012. – 880 с.

17. Кравчук Г. Т. Проблеми інформаційної безпеки. Інформатика, 10. 2020. URL: https://sites.google.com/view/distance-informatics-10/%D0%B1%D0%B0%D0%B7%D0%BE%D0%B2%D0%B8%D0%B9-%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96-

%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97-%D0%B2-%D1%81%D1%83%D1%81%D0%BF%D1%96%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D1%96/%D1%83%D1%80%D0%BE%D0%BA-3?pli=1

18. Куперштейн Л.М., Войтович О.П., Остапенко-Боженов А.В., Прокопчук С.А. Багаторівневий підхід до захисту від несанкціонованого використання додатків в операційній системі Android. Радіоелектроніка та інформатика. 2018. № 2. С. 45-50. URL: https://www.researchgate.net/publication/337852710_BAGATORIVNEVIJ_PIDHID_DO_ZAHISTU_VID_NESANKCIONOVANOGO_VIKORISTANNA_DODATKIV_V_OPERACIJNIJ_SISTEMI_ANDROID

19. Загрози при роботі в Інтернеті і їх уникнення.URL: https://naurok.com.ua/zagrozi-pri-roboti-v-interneti-i-h-uniknennya-257244.html

20. Інформаційна безпека. Загрози при роботі в Інтернеті і їх уникнення. URL: https://www.miyklas.com.ua/p/informatica/10-klas/informatciini-tekhnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71

21. Кращі поради для захисту Вашого смартфону та персональних даних на 2023 рік. URL: https://cybercalm.org/novyny/krashhi-porady-dlya-zahystu-vashogo-smartfonu-ta-personalnyh-danyh-na-2020-rik/

22. Шифрування даних: все, про що ви повинні знати, щоб захистити дані. URL: sim-networks.com/ukr/blog/data-encryption-best-practices

23. Шифрування. URL: eset.com/ua/support/information/entsiklopediya-ugroz/shifrovaniye/

24. Біометричні технології ідентифікації особистості - їх значення і переваги. URL: https://worldvision.com.ua/articles/biometricheskie-tehnologii-identifikatsii-lichnosti-ih-znachenie-i-preimushchestva

25. AndroRat. URL: https://github.com/karma9874/AndroRAT

ДОДАТОК А Код Методу

```
import frida
import subprocess
import socket
import pyshark

device = frida.get_usb_device()
print(device.name)


def get_ip_address():
    hostname = socket.gethostname()
    ip_address = socket.gethostbyname(hostname)
    return ip_address


def enable_proxy(ip, port="8080"):
    output = run_adb_command(f"adb shell settings put global http_proxy {ip}:{port}")
    enable_proxy = output.split("\n")
    return enable_proxy


def run_command(command):
    path = " cd C:/Users/User/.mitmproxy"
    full_command = "C: && "+ path + " && " + command
    process = subprocess.Popen(full_command, stdout=subprocess.PIPE, stderr=subprocess.PIPE, shell=True)
```

```
    output, error = process.communicate()
    return 1


ipadr = get_ip_address()
enable_proxy(ipadr)


run_command("copy mitmproxy-ca.pem file.pem")
run_command("openssl x509 -inform PEM -text -in mitmproxy-ca.pem -out nul
>> file.pem")
run_command("adb shell mount -o rw,remount,rw /system")
run_command("adb push file.pem /system/etc/security/cacerts/")
run_command("adb shell mount -o ro,remount,ro /system")
run_command("adb reboot")


def run_adb_command(command):
    process = subprocess.Popen(command, stdout=subprocess.PIPE,
stderr=subprocess.PIPE, shell=True)
    output, error = process.communicate()
    if error:
        try:
            print("Error: ", error.decode('utf-8'))
        except UnicodeDecodeError:
            print("Error: ", error.decode('cp866'))
    res = output.decode().strip()
    return res
```

```
def logcat():
    output = run_adb_command('adb logcat -d')
    logcat = output.split('\n')
    return logcat


def memory_info():
    output = run_adb_command('adb shell dumpsys meminfo')
    meminfo = output.split('\n')
    return meminfo


def ps():
    output = run_adb_command('adb shell ps')
    pss = output.split('\n')
    return pss


def active_services():
    output = run_adb_command('adb shell dumpsys activity services')
    services = output.split('\n')
    return services


def installed_packages():
    output = run_adb_command('adb shell pm list packages | findstr /v "android"""')
    packages = output.split('\n')
    return packages
```

```
def filesystem_info():
    output = run_adb_command('adb shell df')
    filesystem_info = output.split('\n')
    return filesystem_info



def tcp_connections():
    output = run_adb_command('adb shell su root netstat -tulpn')
    connections = output.split('\n')
    return connections

def capture_and_save():
    output = run_adb_command('adb shell su root timeout 15 "/data/local/tmp/tcpdump -w /sdcard/dump.pcap -s 0 -v" && adb pull /sdcard/dump.pcap')
    print("ok")

def malformed_check():
    capture = pyshark.FileCapture('dump.pcap')
    for packet in capture:
        if 'Malformed' in str(packet):
            print(packet)

logcat = logcat()
print("Системний журнал: ")
for log in logcat:
    print(log)



meminfo = memory_info()
```

```
print("Інформація про пам'ять: ")
for info in meminfo:
    print(info)


pss = ps()
print("Список запущених процесів: ")
for ps in pss:
    print(ps)


active_services = active_services()
print("Активні сервіси: ")
for service in active_services:
    print(service)


installed_packages = installed_packages()
print("Встановлені пакети: ")
for package in installed_packages:
    print(package)


filesystem_info = filesystem_info()
print("Інформація про файлову систему: ")
for info in filesystem_info:
    print(info)


tcp_connections = tcp_connections()
```

```
print("TCP-Підключення: ")
for connection in tcp_connections:
    print(connection)

capture_and_save()
malformed_check()
```