МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»
Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»

Форма навчання: *очна (денна)*
очна (денна),заочна, дистанційна

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему «Засоби захисту від витоку інформації на мобільних пристроях»
(назва теми)

здобувача Моргушко Вячеслава Сергійовича
(ПІБ, підпис)

Науковий керівник: доцент Пархоменко Іван Іванович
(науковий ступень, вчене звання, ПІБ)

(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.-м.н., професор Джалладова І.А.
(науковий ступень, вчене звання, ПІБ)

(підпис)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО:	**ЗАТВЕРДЖУЮ:**
Керівник проектної групи (гарант) освітньо-професійної програми «Кібербезпека» к.ф.н, доцент Г.В. Мамонова	Завідувач кафедри системного аналізу та інформаційної безпеки д.ф.-м.н., проф. І.А. Джалладова
_____ *(підпис) (ініціали,призвище)*	_____ *(підпис) (ініціали,призвище)*
_____20___р.	_____ 20___р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти_____Моргушко Вячеслава Сергійовича_____
(прізвище, ім'я, по батькові)

_____*очної (денної)*_____**форми навчання**
очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи

на тему «Засоби захисту від витоку інформації на мобільних пристроях»
(назва теми)

Тему затверджено наказом ректора Університету від «___»_____20__р.№___

План кваліфікаційної бакалаврської роботи

Розділ 1 | Програмні і апаратні забезпечення мобільних пристроїв
(назва розділу)
Розділ 2 | Типи загроз мобільних пристроїв
(назва розділу)
Розділ 3 | Засоби захисту мобільних пристроїв
(назва розділу)
Об'єкт дослідження: | засоби та технології, що використовуються для захисту мобільних пристроїв від витоку інформації.
Предмет дослідження: | методи, технології та підходи, які використовуються для запобігання витоку інформації на мобільних пристроях.
Мета кваліфікаційної | бакалаврської роботи:| полягає у вивченні, аналізі та оцінці сучасних засобів захисту від витоку інформації на мобільних пристроях.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:
У розділі 1 | Програмні і апаратні забезпечення мобільних пристроїв
(назва розділу)
розглянути операційні системи мобільних пристроїв
перерахувати типи мобільних застосунків та їх функціонал
дослідити апаратну частину мобільних пристроїв
навести інструменти розробки додатків
У розділі 2 | Типи загроз мобільних пристроїв
(назва розділу)
дати характеристику програмним загрозам, web-загрозам, мережевим загрозам, з'єднанню з недовіреним сервісом, GPS/Місцезнаходженню, небезпечному зберіганню даних, ненавмисному витоку даних, проблемам авторизації та аутентифікації
У розділі 3 | Засоби захисту мобільних прострої в
(назва розділу)
надати характеристику наступним засобам захисту від витоку інформації на мобільних пристроях: антивірусне програмне забезпечення; браузери з підтримкою захищеного з'єднання (SSL / TLS); віртуальна приватна мережа; перевірка рейтингів та відгуків про сервіси; функція «псевдонімізації» для приховування точного місцезнаходження; шифрування для захисту конфіденційної інформації на пристрої; моніторінг активності додатків; використання двофакторної аутентифікації для забезпечення додаткового рівня захисту

Завдання підготував
науковий керівник

_____ Пархоменко І. І.
(підпис) (прізвище, ініціали)

Завдання одержав
здобувач

_____ Моргушко В.С.
(підпис) (прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна бакалаврська робота: 80 С., 8 РИС., 2 ТАБЛ., 31 ДЖЕРЕЛО.

Об’єкт дослідження: засоби та технології, що використовуються для захисту мобільних пристроїв від витоку інформації.

Мета кваліфікаційної роботи: полягає у вивченні, аналізі та оцінці сучасних засобів захисту від витоку інформації на мобільних пристроях.

Методи дослідження: написання бакалаврської роботи включало наступні методи дослідження: теоретичні (класифікація, синтез, аналіз), практичні (вимірювання, порівняння), спеціальні методи (інтелектуальний, дослідницький, прогнозний аналіз даних), а також аналіз отриманих результатів шляхом статистичної обробки, узагальнення.

У спеціальній частині дана характеристика основних засобів захисту мобільних пристроїв.

В роботі проведено аналіз основних засобів захисту мобільних пристроїв, включаючи антивірусне програмне забезпечення, браузери з підтримкою SSL/TLS, віртуальні приватні мережі (VPN), перевірку рейтингів та відгуків про сервіси, функцію «псевдонімізації» для приховування місцезнаходження, шифрування даних, моніторинг активності додатків та використання двофакторної аутентифікації.

Запропоновано комплексний підхід до захисту мобільних пристроїв, що включає використання різних інструментів і методів.

Побудовано структуровану систему захисту мобільних пристроїв, яка інтегрує різні засоби захисту, такі як антивірусне програмне забезпечення, шифрування даних, двофакторна аутентифікація, а також моніторинг активності додатків і функцію «псевдонімізації».

Розроблено рекомендації щодо ефективного застосування антивірусного програмного забезпечення, шифрування даних, двофакторної аутентифікації та інших заходів захисту для забезпечення надійної безпеки мобільних пристроїв.

Практичне значення одержаних результатів полягає у підвищенні рівня безпеки мобільних пристроїв, покращенні політик та стандартів безпеки в організаціях, підвищенні обізнаності користувачів, розробці нових засобів захисту, впливі на регуляторні акти та зменшенні економічних втрат від кібератак.

Результати цієї роботи можуть бути використані для подальших досліджень в галузі безпеки мобільних пристроїв, розробки нових методів захисту та вдосконалення існуючих підходів.

Наукова новизна полягає у виявленні та аналізі актуальних загроз та застосуванні новаторських рішень для їх протидії.

Напрямки подальших досліджень можуть включати розробку більш ефективних методів аутентифікації, аналіз нових загроз та розвиток адаптивних систем захисту.

Ключові слова: мобільні пристрої, захист даних, антивірусне програмне забезпечення, шифрування, двофакторна аутентифікація, псевдонімізація,

моніторинг активності.

Відгук

про кваліфікаційну бакалаврську роботу здобувача навчально-наукового інституту «Інститут інформаційних технологій в економіці» освітньо-професійної програми «Кібербезпека» Моргушко Вячеслава Сергійовича на тему Засоби захисту від витоку інформації на мобільних пристроях

1. Актуальність теми: Актуальність дослідження визначається широким застосуванням цифрових технологій в сучасному світі. Відкриті джерела інформації стають все більш важливими у контексті кібербезпеки, оскільки вони дозволяють збирати, аналізувати та використовувати дані для різноманітних цілей, включаючи засоби захисту від витоку інформації. Однак, незважаючи на це, багато аспектів використання методів захисту залишаються недостатньо дослідженими. Ця робота пропонує дослідити використання методів захисту від витоку інформації на мобільних пристроях на основі відкритих джерел, що допоможе покращити розуміння цієї важливої області та розробити ефективні стратегії та методи для її використання.

2. Позитивні риси кваліфікаційної роботи: Було присвячено достатньо уваги на аналіз існуючих методів захисту від витоку інформації, враховуючи актуальні методи та технології, пов'язані з захистом мобільних пристроїв, та детально проаналізовано використання методів. Це дозволило провести огляд різноманітних підходів та вибрати найбільш ефективні методи для використання.

3. Наявність самостійних розробок автора: Результати дослідження дозволяють розширити теоретичне розуміння сучасних методів захисту мобільних пристроїв та їхню ефективність у запобіганні витоку конфіденційної інформації, що сприяє розвитку наукових знань у галузі кібербезпеки, зокрема захисту мобільних пристроїв.

4. Цінність теоретичних висновків та практичних рекомендацій: Цінність даної роботи полягає в узагальненні інформації, пов'язаної з використанням методів захисту в сучасному кіберсередовищі. Робота спрямована на оптимізацію та підвищення ефективності захисту від збору, аналізу та використання даних з відкритих джерел.

5. Наявність недоліків: В даній роботі автор міг би приділити більше уваги оптимізації використання методів захисту, щоб покращити безпеку від витоку інформації.

6. : Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК:

Критерії оцінювання	*Шкала, балів*	Оцінка, балів
1. Логіко-структурний рівень	*0 – 6 – 8 – 10*	8
2. Рівень пошукової глибини	*0 – 6 – 8 – 10*	9
3. Науково-теоретичний рівень *(розділ 1)*	*0 – 6 – 8 – 10*	9
4. Аналітико-методичний рівень *(розділ 2)*	*0 – 6 – 8 – 10*	9
5. Конструктивний рівень *(розділ 3)*	*0 – 6 – 8 – 10*	8
6. Рівень наукової етики	*0 – 6 – 8 – 10*	9
7. Організаційний рівень	*0 – 6 – 8 – 10*	8
Загальна оцінка	***0 – 70***	60

Науковий керівник _____ к.т.н., доцент Пархоменко І.І.
(підпис) *(науковий ступінь, учене звання)* *(прізвище, ініціали)*

доцент кафедри системного аналізу та кібербезпеки
(посада)

"15" червня 2024 р.

Рецензія
на кваліфікаційну бакалаврську роботу
здобувача вищої освіти
Моргушко Вячеслава Сергійовича

Тема
Засоби захисту від витоку інформації на мобільних пристроях

Актуальність теми кваліфікаційної роботи і доцільність її розроблення пояснюється зростанням кількості кіберзагроз, таких як шкідливе програмне забезпечення, фішингові атаки, експлойти та інші методи зловмисників, робить захист мобільних пристроїв від витоку інформації критично важливим. Часті випадки кібератак, витоків даних та зламів пристроїв підкреслюють необхідність застосування ефективних засобів захисту.

Якість проведеного дослідження: результати демонструють високу якість та глибину дослідження. В роботі було враховано широкий спектр наукових джерел, що свідчить про ґрунтовну підготовку та добре обґрунтовану підбірку літературних джерел. Було враховано актуальні методи та технології, пов'язані з захистом мобільних пристроїв, та детально проаналізовано використання методів для збору, аналізу та використання даних з відкритих джерел.

Позитивні риси кваліфікаційної роботи: теоретичні (класифікація, синтез, аналіз), практичні (вимірювання, порівняння), спеціальні методи (інтелектуальний, дослідницький, прогнозний аналіз даних), а також аналіз отриманих результатів шляхом статистичної обробки, узагальнення.

Зауваження: В даній роботі автор міг би приділити більше уваги оптимізації використання методів захисту, що допомогло б зробити процес витоку інформації менш ефективним.

Практична значимість висновків і рекомендацій: аналіз роботи свідчить про глибоке бачення автора проблеми захисту інформації, це дозволяє зробити висновок про те, що кваліфікаційна бакалаврська робота «Засоби захисту від витоку інформації на мобільних пристроях» відповідає всім вимогам, що висуваються до кваліфікаційних робіт та заслуговує на оцінку добре.

к.т.н., доцент, доцент кафедри
кібербезпеки та захисту інформації
факультету
інформаційних технологій
КНУ імені Тараса Шевченка Микола БРАЙЛОВСЬКИЙ

Підпис доцента М.М. Браіловського засвідчую:

заступник декана з наукової роботи
факультету інформаційних технологій
Київського національного університету
імені Тараса Шевченка Григорій ГНАТІЄНКО

«____» _____2024 року

ЗМІСТ

ВСТУП

Актуальність теми роботи. В сучасному світі мобільні пристрої стали невід'ємною частиною повсякденного життя, використовуючись для комунікації, роботи, розваг та доступу до Інтернету. Разом з цим, мобільні пристрої зберігають значну кількість конфіденційної інформації, включаючи особисті дані, фінансову інформацію, корпоративні документи та інші важливі дані. Витік такої інформації може мати серйозні наслідки як для окремих користувачів, так і для організацій.

Зростання кількості кіберзагроз, таких як шкідливе програмне забезпечення, фішингові атаки, експлойти та інші методи зловмисників, робить захист мобільних пристроїв від витоку інформації критично важливим. Часті випадки кібератак, витоків даних та зламів пристроїв підкреслюють необхідність застосування ефективних засобів захисту.

Крім того, розвиток технологій, таких як Інтернет речей (IoT), 5G, та хмарні сервіси, збільшує кількість точок входу для можливих атак і підвищує важливість надійних методів захисту інформації. Впровадження нових засобів захисту дозволяє мінімізувати ризики і забезпечити більш високий рівень безпеки для користувачів.

Важливість теми також зумовлена нормативними вимогами і стандартами безпеки, які висуваються до збереження та обробки персональних даних. Закони про захист даних, такі як GDPR в Європейському Союзі, вимагають від організацій дотримання суворих правил щодо безпеки інформації, що зберігається на мобільних пристроях.

Отже, тема захисту від витоку інформації на мобільних пристроях є надзвичайно актуальною і потребує всебічного дослідження та розробки ефективних рішень. Сучасні методи захисту, включаючи антивірусне програмне забезпечення, шифрування даних, використання двофакторної аутентифікації, VPN, а також моніторинг активності додатків, є необхідними для забезпечення безпеки та конфіденційності мобільних пристроїв.

Мета дослідження полягає у вивченні, аналізі та оцінці сучасних засобів

захисту від витоку інформації на мобільних пристроях.

Завдання дослідження:

– розглянути операційні системи мобільних пристроїв;

– перерахувати типи мобільних застосунків та їх функціонал;

– дослідити апаратну частину мобільних пристроїв;

– навести інструменти розробки додатків;

– дати характеристику програмним загрозам, web-загрозам, мережевим загрозам, з'єднанню з недовіреним сервісом, GPS/Місцезнаходженню, небезпечному зберіганню даних, ненавмисному витоку даних, проблемам авторизації та аутентифікації;

– надати характеристику наступним засобам захисту від витоку інформації на мобільних пристроях: антивірусне програмне забезпечення; браузери з підтримкою захищеного з'єднання (SSL / TLS); віртуальна приватна мережа; перевірка рейтингів та відгуків про сервіси; функція «псевдонімізації» для приховування точного місцезнаходження; шифрування для захисту конфіденційної інформації на пристрої; моніторінг активності додатків; використання двофакторної аутентифікації для забезпечення додаткового рівня захисту.

Об'єктом дослідження є засоби та технології, що використовуються для захисту мобільних пристроїв від витоку інформації.

Предмет дослідження – методи, технології та підходи, які використовуються для запобігання витоку інформації на мобільних пристроях.

Методи дослідження. Написання бакалаврської роботи включало наступні методи дослідження: теоретичні (класифікація, синтез, аналіз), практичні (вимірювання, порівняння), спеціальні методи (інтелектуальний, дослідницький, прогнозний аналіз даних), а також аналіз отриманих результатів шляхом статистичної обробки, узагальнення.

Теоретична і методична значущість отриманих результатів. Результати дослідження дозволяють розширити теоретичне розуміння сучасних методів захисту мобільних пристроїв та їхню ефективність у запобіганні витоку

конфіденційної інформації, що сприяє розвитку наукових знань у галузі кібербезпеки, зокрема захисту мобільних пристроїв. Отримані результати можуть служити основою для подальшого розвитку методології дослідження в галузі кіберзахисту, включаючи підходи до аналізу загроз, оцінки ризиків та розробки заходів захисту. Це сприяє удосконаленню наукових методів і підходів у дослідженнях кібербезпеки.

Практичне значення одержаних результатів полягає у підвищенні рівня безпеки мобільних пристроїв, покращенні політик та стандартів безпеки у організаціях, підвищенні обізнаності користувачів про безпеку мобільних пристроїв, розробці нових засобів та технологій захисту, впливі на розробку та впровадження регуляторних та нормативних актів, а також зменшенні економічних втрат від кібератак та витоків даних. Впровадження рекомендацій щодо використання сучасних антивірусних програм, протоколів захищеного з’єднання (SSL/TLS), VPN та інших технологій дозволить суттєво знизити ризик витоку інформації та захистити мобільні пристрої від кіберзагроз.

РОЗДІЛ 1
ПРОГРАМНІ І АПАРАТНІ ЗАБЕЗПЕЧЕННЯ МОБІЛЬНИХ ПРИСТРОЇВ

1.1. Операційні системи мобільних пристроїв

Мобільні пристрої є неодмінною складовою сучасного суспільства та різноманітних аспектів повсякденної життєдіяльності. Вони стали невід'ємною частиною комунікації, розваг, освіти, роботи та інших сфер діяльності величезної кількості людей на планеті. Зростаюча популярність та розповсюдженість мобільних пристроїв породжує високий попит на операційні системи, що працюють на них.

Операційна система (ОС) – це програмне забезпечення, яке керує ресурсами комп'ютера або іншого пристрою і забезпечує взаємодію між користувачем та апаратним обладнанням. ОС відповідає за управління процесами, пам'яттю, введенням-виведенням, мережевими підключеннями та іншими аспектами роботи пристрою. Вона також надає користувачам інтерфейс для взаємодії з пристроєм та запуску додатків. Операційні системи використовуються на різних типах пристроїв, включаючи персональні комп'ютери, сервери, мобільні телефони, планшети, «розумні» годинники, побутові та промислові пристрої тощо.

Мобільна операційна система – операційна система для смартфонів, планшетів, КПК або інших мобільних пристроїв. Мобільні операційні системи об'єднують в собі властивості і функції ОС для ПК і функціональні характеристики мобільних і кишенькових пристроїв: сенсорний екран, стільниковий зв'язок, Bluetooth, Wi-Fi, GPS-навігація, камера, відеокамера, розпізнавання мови, диктофон, музичний плеєр, NFC і інфрачервоне дистанційне керування [1].

ОС для мобільних пристроїв відрізняє ряд особливостей, знання про які важливі при їх використанні. До таких особливостей відносять:

– обмеження по пам'яті і невисоку швидкість процесора,

– своєрідність екранів і екранних навігаторів різних моделей мобільних пристроїв,

– сумісність з усіма основними форматами файлів,

– механізми обробки мультимедійної інформації,

– підтримка актуальних комунікаційних і мережевих технологій.

На сьогоднішній день існує досить великий вибір мобільних операційних систем. Серед них можна виділити найбільш популярні:

– Android;

– iOS;

– Windows Mobile.

Платформа Android – це мобільна операційна система з відкритим кодом, яка розробляє платформу Google. Вона заснована на ядрі Linux і спроектована для мобільних пристроїв з сенсорним екраном, так як містить карти і планшети. Вперше ОС побачила світ у вересні 2008 року.

Android встановлюється на величезну кількість як бюджетних, так і дорогих пристроїв. Серед них смартфони, планшети, розумні годинники, телевізори та автомобільні медіа системи.

Дана платформа є найпоширенішою ОС в світі. Це обумовлено всебічним розвитком системи корпорацією Гугл, а також відкритим вихідним кодом, який дає можливість виробникам електроніки легко адаптувати і модифікувати систему під свої пристрої. Щороку для платформи виходять нові оновлення і API-інтерфейсу, які додають новий функціонал в систему, а також дають більш зручні інструменти для розробки, що істотно полегшує створення додатків. Можливо, це допоможе зробити вибір між динамічно розвивається версією API і пошуком, чим молодша версія, тим більше користувачів буде будь ласка, зверніть на це увагу. Починаючи з версії Android 5.0 (API 21), в системі впроваджується постійний дизайн всіх додатків Material Design. Для розробки додатків використовується мова Java [2].

Для установки нових додатків користувач може скористатися офіційним магазином додатків Google Play Market. Також існують сторонні магазини додатків, які створюються виробниками техніки з метою зменшення залежності їх пристроїв

від продуктів корпорації Google. Також додатки можна встановлювати прямо з пам'яті телефону або SD карти, що дає широкі можливості по використанню ресурсів системи і налагодження. Але тим самим з'являється можливість установки піратських додатків.

Для розробки додатків використовується Android Studio – середовище розробки, випущена корпорацією Google в 2014 році і заснована на продукті IntelliJ Idea від компанії JetBrains.

Переваги:

– відкритий вихідний код;
– висока швидкодія системи;
– підтримка багатозадачності;
– зручна розробка і налагодження.

Недоліки:

– високий рівень піратства;
– погана захищеність системи від вірусів.

Платформа iOS – закрита мобільна операційна система, доступна тільки на пристроях від компанії Apple, таких як iPhone, iPad і iPod Touch. Перша версія системи була представлена на початку 2007 року. Вона заснована на ядрі власної розробки XNU і володіє високим рівнем захисту від вірусів та інших шахрайських програм.

Операційна система є другою за поширеністю, поступаючись лише Android. Вона має фірмовий магазин додатків App Store. Усі програми в цьому магазині попередньо модеруються співробітниками Apple для перевірки безпеки програми.

Переваги:

– висока захищеність системи від вірусів;
– висока швидкодія системи;
– є низький рівень піратства.

Недоліки:

– обмеженість використання стороннього софта;
– є довга модерація при релізі додатка в App Store.

Платформа Windows Mobile – закрита мобільна операційна система, але володіє більш широким спектром налаштувань елементів інтерфейсу, ніж iOS. Ця система була представлена компанією Microsoft в 2010 році, але останнім часом система майже не підтримується. Серед інших розглянутих систем Windows Mobile має набагато меншу поширеність, оскільки ця ОС не отримала широку підтримку серед розробників і користувачів [3].

Система має свій унікальний інтерфейс, іменований Metro. Він складається з квадратних динамічних плиток різного розміру. Подібний інтерфейс викликав безліч суперечок серед споживачів і став однією з головних причин низької популярності операційної системи.

Windows Mobile має власний магазин додатків Windows Phone Store. Він володіє досить великою кількістю додатків, але деяких важливих додатків, які користувачам необхідні, там немає.

Для розробки додатків для Windows Mobile використовуються мови сімейства c, наприклад C++, C#. Основним інструментом розробки є Microsoft Visual Studio.

Переваги:

– одне ядро з десктопною версією Windows;
– зручність розробки.

Недоліки:

– високі вимоги до мобільного пристрою;
– невелика поширеність системи.

Symbian OS – платформа була популярна до 2014 року, після чого її почала витісняти Android.

Palm OS – платформа, створена в 1996 році, була відома як Garnet OS. Являла собою операційну систему серії портативних комп'ютерів PalmPilot зі стилусом.

BlackBerry OS – операційна система з основним набором додатків для смартфонів, що випускаються компанією Research In Motion Limited.

Bada OS – запатентована операційна система для смартфонів Samsung, була представлена в 2009 році [4].

Згідно зі статистикою від компанії Gartner на кінець 2023 року частка мобільних пристроїв на базі ОС Android становить 84,1%. На другому місці стоїть операційна система iOS – 14,8%. Трійку замикає операційна система Windows Mobile – 1,41% користувачів.

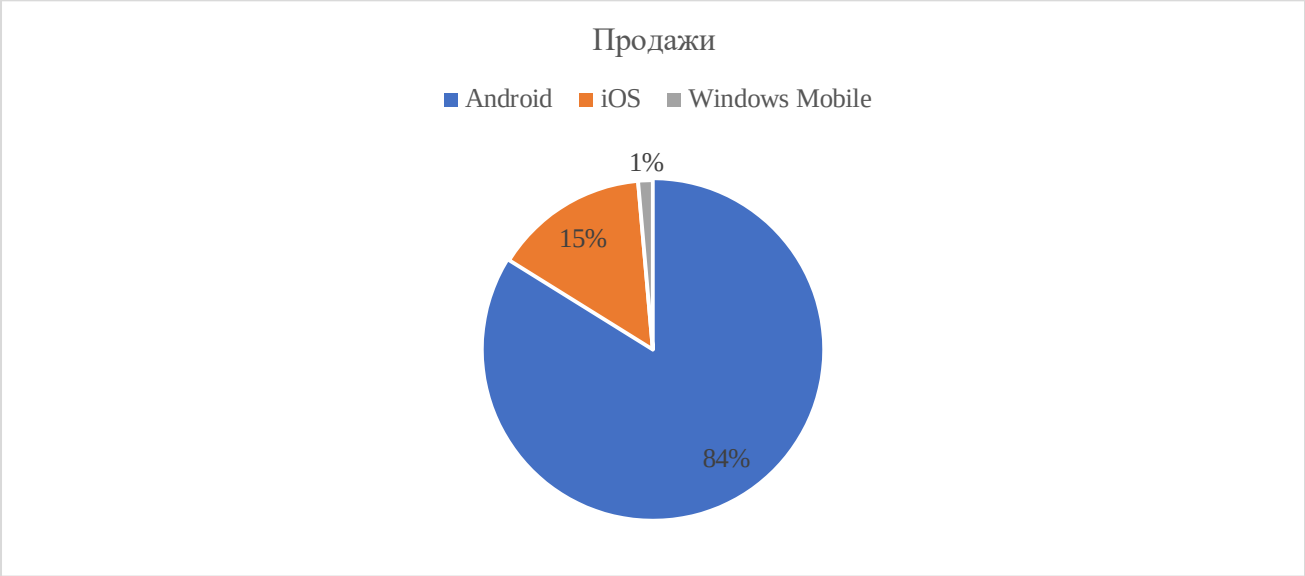

Рисунок 1.1 – Статистика використання мобільних операційних систем [5]

Тому, платформа Android, розроблена компанією Google, представляє собою мобільну операційну систему з відкритим вихідним кодом, яка базується на ядрі Linux і призначена для різноманітних мобільних пристроїв з сенсорними екранами. Заснована у вересні 2008 року, вона встановлюється на широкий асортимент пристроїв, включаючи смартфони, планшети, розумні годинники, телевізори та автомобільні медіа-системи. На сьогоднішній день Android є найпоширенішою мобільною операційною системою у світі, завдяки всебічному розвитку та відкритому вихідному коду, що дозволяє виробникам електроніки адаптувати та модифікувати систему під свої пристрої.

Android постійно оновлюється за рахунок нових версій та API-інтерфейсів, що додають нові функціональні можливості та полегшують розробку додатків. Отже, користувачам доступні різноманітні інструменти та можливості, що покращують їх досвід використання мобільних пристроїв. Проте, серед недоліків системи слід відзначити високий рівень піратства та погану захищеність від вірусів.

Платформа iOS, у свою чергу, є закритою мобільною операційною системою, доступною лише на пристроях компанії Apple, таких як iPhone, iPad і iPod Touch. Вона відрізняється високим рівнем захисту від вірусів та шахрайських програм, а також має власний фірмовий магазин додатків App Store. Однак, вона обмежена використанням стороннього софту та піддається довгій мацерації під час релізу додатків.

Платформа Windows Mobile, хоча має власні особливості та унікальний інтерфейс Metro, має значно меншу поширеність і підтримку серед розробників та користувачів порівняно з Android і iOS. Її використання дещо обмежене, але вона має свою аудиторію та використовується на деяких пристроях.

Таким чином, на сучасному ринку мобільних пристроїв Android, iOS та Windows Mobile є основними операційними системами, кожна з яких має свої переваги та обмеження, але Android, завдяки своїй широкій розповсюдженості, відкритому вихідному коду та розвитку, визнаний як найпопулярніший інструмент у цій сфері.

1.2. Типи мобільних застосунків та їх функціонал

Мобільний застосунок є програмним забезпеченням, яке спеціально розроблено для конкретної мобільної платформи (iOS, Android, Windows Phone та ін). Призначений для застосування на смартфоні, планшеті, розумних годинниках та інших мобільних пристроях. Процес створення мобільних застосунків протікає наступним чином:

1) написання мовою програмування високого рівня;

2) компіляція в машинний код операційної системи для максимальної продуктивності.

При розробці застосунків необхідно враховувати деякі особливості: робота мобільних пристроїв здійснюється на батарейках і оснащені не такими потужними продуктивними процесорами, як у персональних комп'ютерів. Крім цього, сучасні смартфони та планшети універсально мають додаткові пристрої, як гіроскопи,

акселерометри і камери, які надають унікальні можливості для розширення функціональності програми. Як правило, продають мобільні пристрої з деякими, заздалегідь встановленими застосунками.

Кількість мобільних застосунків похило зростає і їх загальна кількість тільки в загальнодоступних репозитаріях (iOS App Store і Google Play) досягає більше 5,5 млн. одиниць. Для класифікації всього величезного безлічі доступних для використання мобільних застосунків використовуються наступні основні ознаки:

1) роль мобільного застосунку для його власника;

2) виконувані мобільним застосунком функції;

3) технологія розробки мобільного застосунку;

4) спосіб отримання вигоди від поширення мобільного застосунку.

Також класифікувати мобільні застосунки можна за цільовою аудиторією мобільного застосунку, його вартістю та іншими ознаками.

Мобільний застосунок може вводиться його власником в господарський оборот або як економічний ресурс, або як товар. У першому випадку воно виступає як корпоративний мобільний застосунок, у другому – як комерційний мобільний застосунок.

Корпоративний мобільний застосунок є невід'ємною частиною системи автоматизації бізнес-процесів підприємства, забезпечуючи для його власників, співробітників і партнерів рішення наступних завдань:

1) доступ до оперативної інформації (наприклад, до даних про продукцію, клієнтів, замовлення та угоди);

2) здійснення господарських операцій (наприклад, виписка рахунку, електронний підпис накладних);

3) здійснення управління підприємством і партнерськими взаємовідносинами (наприклад, забезпечення оперативних комунікацій, фінансове планування).

Комерційні мобільні застосунки є товаром і призначені для реалізації на ринку тим чи іншим способом. Способи отримання вигоди від поширення мобільного застосунку як товару називаються моделями монетизації.

З точки зору виконуваних функцій мобільні застосунки можуть бути

віднесені до однієї з наступних категорій:

1) розваги (ігрові програми, мультимедіа, музика, замовлення квитків в театр, кіно і т. п.);

2) подорожі (замовлення готелю, оренда авто, послуги гіда, сервіс онлайн-перекладача і т. п.);

3) бізнес (фінансові додатки, планування, торгівля, додатки для міста, пошук роботи і т. п.);

4) соціальні додатки (соціальні мережі, глобальні брендовані мережі, спеціалізовані (клубні) мережі і т. п.);

5) їжа (замовлення і доставка їжі, геолокація закладу харчування, рецепти);

6) спорт (спортивні новини, купівля квитків на спортивні заходи, ігрові симулятори);

7) освіта (навчальні програми, інтерактивні курси і т. п.);

8) новини (дайджести, стрічки, рейтинги).

Залежно від технології розробки розрізняють наступні види мобільних застосунків:

1) нативні (особливістю даного виду мобільних застосунків є те, що створюються вони під конкретну операційну систему і встановлюються безпосередньо на мобільний пристрій користувача);

2) кросплатформні (особливістю даного виду мобільних застосунків є те, що вони створюються як веб-додаток і не потрібно встановлювати їх на мобільний пристрій користувача);

3) гібридні (особливістю даного виду мобільних застосунків є те, що вони створюються як комбінація нативних і кросплатформних застосунків).

Нативні мобільні застосунки мають повний доступ до функціоналу мобільного пристрою (наприклад, геолокації, дзвінків, SMS, камері, мікрофону). Швидкість роботи даного виду мобільних додатків висока. Поширення здійснюється, як правило, через магазини додатків.

Кросплатформні мобільні застосунки не мають доступу до функціоналу мобільного пристрою і швидкість їх роботи визначається параметрами мережевого

підключення [6].

Спосіб отримання вигоди від поширення мобільного застосунку залежить від того яку роль мобільний застосунок виконує для його власника.

Якщо мова йде про корпоративний мобільний застосунок, то вигода від його використання полягає в зниженні операційних і транзакційних витрат, пов'язаних з доступом до оперативної інформації, роботи з первинною документацією, а також з управлінням бізнес процесами.

Для комерційних мобільних застосунків існує кілька ключових способів отримання вигоди від їх поширення (моделей монетизації):

1) платні застосунки (суть даної моделі монетизації полягає в тому, що перед тим, як завантажити мобільний застосунок користувач повинен його оплатити);

2) умовно-безкоштовні додатки (суть даної моделі монетизації полягає в тому, що користувачеві спочатку безкоштовно доступний базовий функціонал мобільного застосунку, а додаткові можливості доступні тільки після оплати);

3) модель підписки (суть даної моделі монетизації полягає в тому, що користувач отримує новий доступний в мобільному застосунку інформаційний контент на основі його періодичної оплати);

4) рекламна модель (суть даної моделі монетизації полягає в тому, що всередині мобільного застосунку продаються рекламні місця або рекламується власна продукція розробника);

5) модель виконання рекламних дій (суть даної моделі монетизації полягає в тому, що за вчинення певних дій користувачеві мобільного застосунку надаються додаткові функціональні можливості або інформаційний контент).

Функціонал типів мобільних застосунків наведено у табл. 1.1.

Таблиця 1.1 – Функціонал типів мобільних застосунків

Тип застосунку	Основний функціонал	Приклади застосунків
Соціальні мережі	Обмін повідомленнями (текст, фото, відео), публікація та перегляд зображень та відео, групи, чати, реакції.	Facebook, Instagram, Twitter
Месенджери	Обмін текстовими, аудіо та відео повідомленнями, групові та однобічні	WhatsApp, Messenger, Telegram

	чати, відео дзвінки, стікери, емодзі.	
Мультимедійні	Відтворення аудіо та відео, перегляд фотографій, редагування мультимедійного контенту.	YouTube, Spotify, Adobe Photoshop Express
Ігри	Різноманітні жанри ігор, онлайн та офлайн геймплей, глобальні рейтинги, кастомізація персонажів.	Candy Crush, PUBG Mobile, Among Us
Продуктивність	Створення та редагування документів, керування завданнями, календар та нагадування про події.	Microsoft Office, Todoist, Google Calendar
Фінансові	Керування бюджетом, моніторинг транзакцій, оплата рахунків, відслідковування фінансових цілей.	Mint, PayPal, Revolut
Подорожі	Планування маршрутів, бронювання готелів, пошук ресторанів, рецензії та рейтинги місць для відпочинку.	Airbnb, TripAdvisor, Uber
Освіта та навчання	Доступ до навчальних матеріалів, взаємодія з викладачами, вправи та тести, відстеження прогресу.	Duolingo, Khan Academy, Quizlet
Здоров'я та фітнес	Відстеження фізичної активності, моніторинг сну, планування тренувань, медичні поради.	Fitbit, MyFitnessPal, Headspace
Навігація та мапи	Визначення маршрутів, пошук місць, перегляд розкладів транспорту, автоматична побудова оптимальних маршрутів.	Google Maps, Waze, Citymapper

Мобільні застосунки включають в себе широкий спектр функціоналу, який відповідає потребам різних груп користувачів та їхнім повсякденним задачам. Від соціальних мереж і месенджерів для комунікації до продуктивних ігор та застосунків для управління фінансами або здоров'ям, кожен тип застосунку надає користувачам інструменти для досягнення їхніх цілей та полегшення їхнього повсякденного життя [7].

Застосунки соціальних мереж і месенджери створюють можливості для вільної комунікації та обміну інформацією, тоді як мультимедійні застосунки дозволяють користувачам споживати контент та створювати його. Ігри надають розвагу та можливість зануритися у віртуальний світ, а застосунки для продуктивності та фінансові додатки допомагають у керуванні робочим процесом та фінансовими ресурсами. Подорожні застосунки дозволяють легко планувати подорожі та відпочинок, а освітні та навчальні застосунки допомагають вдосконалювати навички та отримувати нові знання. За допомогою застосунків

здоров'я та фітнесу користувачі можуть вести здоровий спосіб життя, а навігаційні та мапові застосунки спрощують переміщення та орієнтування у просторі.

У цілому, різноманітність типів мобільних застосунків відображає широкий спектр інтересів та потреб сучасного суспільства, а їхні можливості допомагають користувачам зберігати зв'язок, бути продуктивними, навчатися, розважатися та керувати своїм життям більш ефективно і зручно.

1.3. Апаратна частина мобільних пристроїв

Апаратна частина мобільних пристроїв – це фізичні компоненти, які складаються на пристрої і забезпечують його функціональність та можливості. Ці компоненти включають в себе процесори, пам'ять, дисплей, камери, батареї, датчики, модулі зв'язку (такі як Wi-Fi, Bluetooth і мобільні мережі), а також різноманітні роз'єми та порти. Апаратна частина відповідає за обробку даних, вивід інформації на екран, забезпечення зв'язку з іншими пристроями та користувачами, а також за живлення та заряджання пристрою.

Основні складові апаратної частини мобільного пристрою включають:

1. Процесор, відомий також як центральний процесор (ЦП), є ключовим елементом апаратної частини мобільних пристроїв. Він відповідає за виконання обчислювальних операцій та управління роботою всього пристрою. Характеристика процесора включає:

– обчислювальні операції. Процесор виконує широкий спектр математичних та логічних операцій, таких як додавання, віднімання, множення, ділення, порівняння та інші, що необхідні для виконання завдань та запуску програм на пристрої;

– управління роботою пристрою. Процесор координує роботу різних компонентів пристрою, таких як пам'ять, датчики, камери та інші. Він відповідає за розподіл ресурсів, управління енергозбереженням та координацію роботи всіх підсистем пристрою;

– швидкість та ефективність. Швидкість роботи процесора визначається

його тактовою частотою (вимірюється в гігагерцах) та кількістю ядер. Вища тактова частота дозволяє виконувати більше операцій за одиницю часу, а наявність більшої кількості ядер дозволяє виконувати багатозадачні операції більш ефективно. Ефективність процесора також залежить від архітектури, оптимізації коду програм, налаштувань операційної системи та інших факторів;

– графічні можливості. Деякі процесори мають вбудовані графічні підсистеми (GPU), які відповідають за обробку графічних операцій, відтворення відео, рендерінг ігор та інші графічні завдання;

– енергоефективність. Сучасні процесори розробляються з урахуванням енергоефективності, що дозволяє продовжити час автономної роботи пристрою за рахунок оптимізації споживання енергії.

В цілому, процесор відіграє ключову роль у функціонуванні мобільних пристроїв, і його якість і продуктивність суттєво впливають на загальний досвід використання пристрою [8, с.132].

2. Оперативна пам'ять (ОЗП), відома також як RAM (Random Access Memory), є одним з ключових компонентів мобільних пристроїв і виконує ряд важливих функцій, пов'язаних з тимчасовим зберіганням даних та програм, які виконуються на пристрої. До ролі та функцій ОЗП входять:

– тимчасове зберігання даних. ОЗП використовується для тимчасового зберігання даних, які використовуються програмами під час їх роботи. Це може включати в себе тексти, зображення, відео, аудіо, тимчасові файли, стан програми тощо. ОЗП є тимчасовим сховищем для даних, які необхідні для швидкого доступу під час роботи з пристроєм;

– робота програм та операційна система. ОЗП використовується для завантаження та виконання операційної системи та програм, що запущені на пристрої. Велика кількість ОЗП дозволяє використовувати більше програм одночасно та запускати більш об'ємні програми без збоїв чи зависань;

– швидкий доступ до інформації. ОЗП забезпечує швидкий доступ до необхідних даних та програм, оскільки вона працює на принципах випадкового доступу до пам'яті. Це дозволяє пристрою оперативно відповідати на дії

користувача та виконувати запити програм;

– підвищення продуктивності. Більша кількість ОЗП дозволяє пристрою підтримувати більше програм у пам'яті, що забезпечує плавну роботу і підвищує загальну продуктивність. Крім того, ОЗП дозволяє прискорити виконання завдань за рахунок швидкого доступу до даних;

– втрати при вимкненні. ОЗП є типом волатильної пам'яті, що означає, що дані втрачаються при вимкненні пристрою або перезавантаженні. Це відрізняє її від постійної пам'яті, такої як внутрішня пам'ять пристрою.

ОЗП відіграє важливу роль у роботі мобільних пристроїв, забезпечуючи швидкий доступ до даних та програм, що потрібні для ефективної роботи пристрою та задоволення потреб користувача.

3. Внутрішня пам'ять мобільного пристрою є однією з основних компонентів, яка забезпечує простір для зберігання різноманітної інформації, включаючи операційну систему, програми, медіафайли та інші дані:

– зберігання операційної системи. Внутрішня пам'ять використовується для зберігання операційної системи пристрою, такої як Android, iOS або Windows Mobile. Операційна система встановлюється на внутрішню пам'ять під час виробництва пристрою і використовує цей простір для свого функціонування;

– установка та зберігання програм. Користувач може встановлювати різні програми з магазину додатків або інших джерел на внутрішню пам'ять пристрою. Програми також зберігають свої дані та конфігураційні файли в цьому просторі;

– медіафайли та інші дані користувача. Внутрішня пам'ять використовується для зберігання медіафайлів, таких як фотографії, відео та аудіофайли, які користувачі зберігають на своєму пристрої. Крім того, сюди також можуть зберігатися інші дані, такі як контакти, календарні події, папки з документами тощо;

– постійна пам'ять. Внутрішня пам'ять пристрою є типом постійної пам'яті, що означає, що дані зберігаються навіть при вимкненні пристрою. Це відрізняє її від оперативної пам'яті, яка втрачає дані при вимкненні;

– розширення пам'яті. Деякі пристрої можуть мати можливість розширення

внутрішньої пам'яті за допомогою використання карт пам'яті, таких як microSD. Це дозволяє користувачам розширювати доступний простір для зберігання даних за допомогою встановлення карт пам'яті в спеціальний слот на пристрої.

Внутрішня пам'ять є важливим елементом мобільного пристрою, який забезпечує простір для зберігання різноманітної інформації, необхідної для його коректної роботи та задоволення потреб користувача.

4. Дисплей, також відомий як екран, є одним з найбільш важливих компонентів мобільних пристроїв, оскільки він відображає інтерфейс користувача, текст, зображення та відео:

– відображення інтерфейсу користувача. Дисплей дозволяє відображати інтерфейс користувача пристрою, включаючи додатки, меню, іконки та інші елементи, необхідні для взаємодії з пристроєм;

– текст, зображення та відео. Дисплей відтворює текст, зображення та відео, що дозволяє користувачам переглядати контент, використовувати додатки та взаємодіяти з пристроєм за допомогою відображених елементів;

– розмір. Розмір дисплея визначається діагоналлю екрана, виміряною у дюймах або сантиметрах. Більший розмір дозволяє відображати більше контенту одночасно, що може поліпшити зручність використання;

– роздільна здатність. Роздільна здатність визначає кількість пікселів, що вміщуються на екрані. Вона вимірюється у пікселях на дюйм (PPI) або у ширинах та висотах (наприклад, 1920x1080). Вища роздільна здатність забезпечує більш чітке та деталізоване відображення зображень;

– технологія дисплея. Існує кілька технологій дисплея, таких як LCD (рідкокристалічний дисплей), OLED (органічний світлодіодний дисплей), AMOLED (активно-матричний OLED), Super AMOLED тощо. Кожна з цих технологій має свої переваги і недоліки, такі як яскравість, контрастність, кольорова гамма та споживання енергії.

– сенсорні можливості. Більшість сучасних дисплеїв мобільних пристроїв є сенсорними, що дозволяє користувачам взаємодіяти з пристроєм шляхом торкання, рухів пальцями або використанням стилуса.

Характеристики дисплея, такі як розмір, роздільна здатність та технологія, впливають на зручність використання та якість відображення контенту на мобільному пристрої [9, с.81].

5. Батарея є одним із найважливіших компонентів мобільного пристрою, оскільки вона надає живлення для роботи всіх його електронних компонентів:

– надання живлення; Основна функція батареї полягає в тому, щоб забезпечувати потрібну електричну енергію для роботи пристрою. Без батареї пристрій не може працювати автономно та навіть не зможе включитися;

– капацитет батареї. Капацитет батареї вимірюється в міліампер-годинах (mAh) і визначає, скільки електричної енергії може зберігати батарея. Більший капацитет означає, що пристрій зможе працювати довше без підзарядки;

– тривалість роботи без підзарядки. Капацитет батареї прямо впливає на тривалість роботи пристрою без підзарядки. Чим більший капацитет, тим довше пристрій зможе працювати без підзарядки. Однак це також залежить від споживання енергії пристроєм та іншими факторами, такими як яскравість дисплея та активність додатків;

– технології швидкої зарядки. Деякі сучасні пристрої обладнані технологіями швидкої зарядки, такими як Qualcomm Quick Charge або VOOC Flash Charge. Ці технології дозволяють заряджати батарею пристрою значно швидше, що є корисним у випадках, коли час зарядки обмежений;

– тип батареї. Більшість сучасних мобільних пристроїв використовують літій-іонні або літій-полімерні батареї, оскільки вони мають високу енергетичну щільність та невеликий розмір. Ці типи батарей є стандартом у більшості сучасних смартфонів та планшетів.

Батарея є ключовим компонентом мобільного пристрою, який забезпечує живлення для його роботи. Капацитет батареї та технології швидкої зарядки впливають на зручність та продуктивність користувача, дозволяючи пристрою працювати довше без підзарядки та швидше відновлювати енергію.

6. Камери є важливою складовою мобільних пристроїв, оскільки вони дозволяють користувачам знімати фотографії та відео безпосередньо зі свого

пристрою. Ось більш детальний опис ролі та характеристик камер:

– фотографування та відеозапис. Камери використовуються для захоплення зображень у форматі фотографій або відео. Користувач може використовувати камеру для створення знімків різних об'єктів, сцен або подій, а також для запису відео зі звуком;

– роздільна здатність камер. Роздільна здатність камери вимірюється у мегапікселях (MP) і визначає кількість пікселів у фотографії. Чим вища роздільна здатність, тим більше деталей може бути захоплено на зображенні. Сучасні мобільні пристрої мають камери з роздільною здатністю від 8 MP до 108 MP і більше;

– оптичні характеристики. Оптичні характеристики камер включають такі параметри, як діафрагма (апертура), фокусна відстань, оптичний зум тощо. Ці параметри впливають на якість та характеристики зображення, такі як глибина різкості, ефект розфокусування, відтінки кольорів тощо;

– програмне забезпечення для обробки зображень. Більшість мобільних пристроїв поставляються з програмним забезпеченням для обробки та редагування зображень прямо на пристрої. Ці програми можуть включати такі функції, як фільтри, корекція кольору, ретушування, обрізка, зміна рівнів експозиції тощо, що дозволяє користувачам покращувати та модифікувати свої фотографії без додаткового програмного забезпечення.

Камери в мобільних пристроях відіграють ключову роль у захопленні зображень та відео, і якість їхньої роботи має велике значення для задоволення потреб користувача. Чим кращі оптичні та програмні характеристики камери, тим якісніші зображення можна отримати за допомогою мобільного пристрою.

7. Система підтримки мереж, відома також як модем, є важливим компонентом мобільних пристроїв, який відповідає за забезпечення підключення до мобільних та бездротових мереж для доступу в Інтернет та передачі даних. Ось більш детальний опис ролі та характеристик модему:

– підтримка мереж. Модеми зазвичай підтримують різні типи мобільних мереж, такі як 2G (GSM), 3G (UMTS), 4G (LTE) та 5G. Вони також можуть

підтримувати бездротові мережі Wi-Fi для підключення до місцевих мереж та точок доступу;

– передача даних. Модеми відповідають за передачу даних між мобільним пристроєм та мережею. Вони забезпечують стабільне та швидке з'єднання для передачі інформації, такої як веб-сторінки, електронні листи, медіафайли та інші дані;

– швидкість передачі даних. Швидкість передачі даних через модем залежить від типу мережі та технологій, які підтримує пристрій. Новіші версії мобільних мереж, такі як 4G та 5G, забезпечують вищі швидкості передачі даних порівняно зі старішими версіями, такими як 2G та 3G;

– робота в різних мережах. Модеми можуть автоматично перемикатися між різними мобільними мережами в залежності від доступності сигналу та якості з'єднання. Це дозволяє пристрою підтримувати зв'язок навіть у рухомому стані або в областях з обмеженою покриттям мережі;

– бездротовий доступ до Інтернету. Модем також може підтримувати підключення до бездротових мереж Wi-Fi, що дозволяє пристрою підключатися до місцевих мереж та точок доступу для отримання доступу в Інтернет.

8. Датчики є важливою складовою мобільних пристроїв, оскільки вони забезпечують збір різних параметрів оточуючого середовища та взаємодію з додатками та сервісами для реалізації різноманітних функцій. Ось більш детальний опис ролі та характеристик різних типів датчиків:

– акселерометр – датчик вимірює прискорення пристрою в трьох основних напрямках: вздовж осей X, Y та Z. Акселерометр використовується для визначення орієнтації пристрою, виявлення руху, визначення кроків, автоматичного повороту екрана та взаємодії з іграми та додатками, які вимагають контролю жестів;

– гіроскоп вимірює кутову швидкість обертання пристрою навколо трьох осей: X, Y та Z. Цей датчик використовується для визначення точного положення пристрою в просторі, виявлення кутів нахилу, орієнтації та стабілізації зображення при використанні камери;

– датчик освітлення вимірює рівень освітленості навколишнього

середовища. Використовується для автоматичного регулювання яскравості дисплея, включення/вимикання автоматичного підсвічування клавіатури, управління функцією автоматичного регулювання екрана та вимірювання відстані обличчя під час використання функції розблокування за допомогою обличчя;

– датчик зближення вимірює відстань між пристроєм та об'єктом навколо нього. Використовується для автоматичного вимикання дисплея під час розмови телефоном, управління функцією автоматичного вимикання екрана під час розмови телефоном, а також для реалізації функцій розблокування пристрою за допомогою розпізнавання відбитка пальця;

– датчик геолокації використовується для визначення точного місцезнаходження пристрою. Використовується для навігації, визначення місця розташування на мапі, створення маршрутів та отримання інформації про оточуючі об'єкти.

Датчики в мобільних пристроях грають ключову роль у взаємодії з додатками та сервісами, що забезпечує більш широкий та зручний функціонал пристрою для користувачів [10, с.92].

9. Роз'єми:

– micro USB/USB-C – стандартні роз'єми для підключення мобільних пристроїв до комп'ютерів, зарядних пристроїв, а також для передачі даних та заряджання акумулятора. Роз'єм USB-C стає все більш поширеним через свою універсальність та швидкодію передачі даних;

– роз'єм для навушників (3,5 мм або USB-C). Використовується для підключення навушників або гарнітур до пристрою для прослуховування аудіо;

– слот для карт пам'яті (microSD). Дозволяє розширити обсяг внутрішньої пам'яті пристрою за допомогою карти пам'яті microSD;

– SIM-слот. Використовується для встановлення SIM-карти для доступу до мобільної мережі.

10. Бездротові інтерфейси:

– wi-fi – дозволяє підключати пристрій до мереж Wi-Fi для доступу до Інтернету та обміну даними з іншими пристроями в межах однієї мережі;

– Bluetooth – використовується для безпровідного обміну даними між пристроями, такими як навушники, гарнітури, колонки, клавіатури та миші;

– NFC (Near Field Communication) – дозволяє бездротово обмінюватися даними між пристроями на короткій відстані (до 10 см), що дуже зручно для проведення платежів, передачі файлів та обміну контактами;

– Infrared (ІЧ-порт) – використовується для безпровідного керування побутовою електронікою, такою як телевізори, кондиціонери, DVD-плеєри тощо.

Роз'єми та бездротові інтерфейси роблять мобільні пристрої більш універсальними та зручними для використання, дозволяючи користувачам підключати їх до різних пристроїв та обмінюватися даними з ними без необхідності використання дротів або кабелів [11, с.129].

Таким чином, апаратна частина мобільних пристроїв є ключовою для їхньої функціональності та ефективності. Вона включає в себе процесор, пам’ять, дисплей, батарею, камери, систему підтримки мереж, датчики, роз’єми та бездротові інтерфейси. Кожен з цих компонентів грає свою роль у забезпеченні оптимальної роботи пристрою, а їх збалансоване використання забезпечує зручне та продуктивне використання мобільного пристрою в різних сферах життя користувача.

1.4. Інструменти розробки додатків

Мобільні додатки стали невід'ємною частиною сучасного цифрового світу, і для їх успішного розроблення потрібно мати доступ до потужних інструментів, які спрощують процес розробки, тестування та розгортання додатків. Інструменти розробки додатків є ключовими для створення якісного та ефективного програмного забезпечення для мобільних пристроїв.

Android Studio – інтегроване середовище розробки додатків, створене компанією Google для операційної системи Android. Наданий продукт покликаний забезпечити розробників новими інструментами для створення додатків. При створенні нового проекту в Android Studio, зображена структура проекту з усіма

потрібними файлами, що містяться в каталозі SDK. Цей перехід до системи управління Gradle надає процесу розробки більшу гнучкість, Android studio дозволяє побачити можливі візуальні зміни, які здійснює в реальному часі в додатку. Також можна побачити, як додаток буде в той же час виглядати на різних пристроях під управлінням Android, з різноманітними настройками і дозволом екрану. Studio володіє новими інструментами для створення і маркування коду.

У програмі також задіяна функція перетягування, за допомогою якої можна переміщати компоненти засобами користувальницького інтерфейсу. До всього іншого середовище розробки має в своєму розпорядженні функцію Google Cloud Messaging. Ця функція дозволяє відсилати дані з сервера на Android-пристрої через хмару. Існує можливість за допомогою програми локалізувати додатки, що дозволяє писати код, і контролювати додаток.

Можливості Android Studio:

1. Надійне та просте середовище розробки.

2. Є можливість вільно перевірити продуктивність програми на різних типах пристроїв.

3. Помічники та шаблони для багатьох елементів програмування для Android.

4. Багатофункціональний редактор з масою додаткових інструментів, що сприяють збільшенню розробки додатків.

Xcode є основним інтегрованим середовищем розробки (Integrated Development Environment, IDE) для створення додатків для платформ iOS, macOS, watchOS та tvOS, що розробляється компанією Apple. Це потужний інструмент, який надає розробникам широкий спектр можливостей для розробки програмного забезпечення для різних пристроїв Apple. Основні характеристики Xcode включають наступне:

– інтерфейс розробки;
– редактор коду;
– інструменти для розробки інтерфейсу користувача;
– система управління версіями;
– симулятори пристроїв;

– інструменти для тестування та налагодження;

– інструменти для розгортання.

Загалом, Xcode є важливим інструментом для розробки додатків для екосистеми пристроїв Apple, надаючи розробникам усе необхідне для ефективної роботи над їхніми проектами [12, с.4].

Visual Studio – це інтегроване середовище розробки (Integrated Development Environment, IDE), розроблене компанією Microsoft, яке підтримує розробку додатків для різних платформ, включаючи Android, iOS, Windows та інші. Це потужний інструмент, який надає розробникам широкий спектр можливостей для розробки програмного забезпечення для різних платформ.

Основні характеристики Visual Studio включають зручний інтерфейс розробки, потужний редактор коду з підсвічуванням синтаксису та автодоповненням, підтримку різних мов програмування (таких як C#, C++, Visual Basic), а також інструменти для розробки мобільних додатків для платформ Android та iOS.

Крім того, Visual Studio інтегрується з іншими продуктами Microsoft, що дозволяє розробникам ефективно використовувати хмарні сервіси та інші ресурси компанії. Воно також підтримує командну роботу та розгортання додатків у хмарних сервісах.

Visual Studio має велику розширюваність та доповнення, що дозволяє розробникам налаштовувати середовище розробки під свої потреби та вимоги проекту. Загалом, Visual Studio є потужним інструментом для розробки додатків для різних платформ, який надає розробникам зручне та продуктивне середовище для створення програмного забезпечення.

Flutter – це фреймворк для розробки крос-платформових мобільних додатків, розроблений компанією Google. Основна особливість Flutter полягає в тому, що він дозволяє розробникам використовувати один і той же код для створення додатків для різних платформ, таких як Android та iOS. Це робить процес розробки більш ефективним та швидким, оскільки розробнику не потрібно писати окремий код для кожної платформи.

Flutter базується на власній віртуальній машині і має власний набір віджетів та інструментів для розробки інтерфейсу користувача. Цей набір віджетів є одним з ключових переваг Flutter, оскільки він дозволяє розробникам швидко та легко створювати красивий та функціональний інтерфейс для своїх додатків. Flutter має високу продуктивність і швидкість роботи завдяки своєму власному движку рендерингу, що надає можливість плавної анімації та відзначається швидким відгуком на дії користувача.

Іншою важливою особливістю Flutter є гарний набір інструментів для розробки, які включають у себе редактор коду, систему управління станами додатків, інструменти для тестування та налагодження, а також розширений набір документації та ресурсів для розробників.

Узагальнюючи, Flutter є потужним фреймворком для створення крос-платформових мобільних додатків, який надає розробникам зручні інструменти та можливості для швидкої та ефективної розробки додатків для різних платформ.

React Native – це фреймворк для розробки крос-платформових мобільних додатків, створений компанією Facebook. В основі React Native лежить використання мови програмування JavaScript, що дозволяє розробникам створювати додатки, які можуть працювати як на платформі Android, так і на iOS.

Однією з ключових особливостей React Native є використання компонентів, які є основними будівельними блоками додатків. Ці компоненти дозволяють створювати віджети інтерфейсу користувача, які автоматично адаптуються під різні платформи. Однією з головних переваг React Native є можливість гарячої перезавантаження (hot reloading), що дозволяє розробникам швидко переглядати зміни у додатку під час розробки без необхідності повного перезавантаження додатку.

Крім того, React Native надає доступ до багатофункціональних сторонніх бібліотек та модулів, що значно спрощує розробку та розширення функціональності додатків. Ще однією важливою перевагою React Native є активна спільнота розробників, яка підтримує та розвиває фреймворк, надає допомогу у вирішенні проблем та швидко реагує на нові тенденції та вимоги ринку.

AppCode – це інтегроване середовище розробки (IDE), розроблене компанією JetBrains, призначене для створення додатків для платформ iOS та macOS. Це середовище базується на популярній платформі розробки IntelliJ IDEA і надає розробникам зручні інструменти для швидкого та ефективного створення програмного забезпечення для продуктів Apple.

Основні функції AppCode включають у себе підтримку різних мов програмування, зокрема Objective-C, Swift, а також розширений набір інструментів для написання, тестування та налагодження коду. Воно також забезпечує розробників можливістю взаємодії з іншими середовищами розробки, такими як Xcode, для більшої гнучкості та зручності.

Однією з ключових переваг AppCode є його інтелектуальні функції, такі як автодоповнення коду, рефакторинг, аналіз коду на льоту, що допомагають розробникам писати якісний та ефективний код без зайвих зусиль. AppCode має широкий набір інтегрованих інструментів для тестування додатків, включаючи підтримку автоматичних тестів, профілювання та налагодження додатків для досягнення оптимальної продуктивності та якості [13, с.416].

Характеристика приведених інструментів наведена у табл. 1.2.

Таблиця 1.2 – Порівняльна характеристика інструментів розробки додатків

Функції	AppCode	Xcode	Android Studio	Visual Studio	Flutter	React Native
Операційні системи	iOS, macOS	iOS, macOS	Android, iOS, Windows, macOS	Windows, macOS	Android, iOS, Windows, macOS	Android, iOS, Windows
Мови програмування	Objective-C, Swift	Swift, Objective-C	Java, Kotlin, C++, XML	C#, Visual Basic, C++, JavaScript	Dart	JavaScript, TypeScript
Інтеграція	Інтеграція з Xcode, можливе використання з IntelliJ IDEA	Інтегроване середовище для розробки Apple	Інтегроване середовище для розробки Android	Інтегроване середовище для розробки Microsoft	Інтегроване середовище для розробки крос-платформових додатків	Інтегроване середовище для розробки крос-платформових додатків

Функціональність	Інтелектуальні функції, автодоповнення, рефакторинг, аналіз коду	Великий набір інструментів для розробки, тестування та налагодження	Розширені можливості розробки Android-додатків, широкий вибір інструментів	Інтеграція з різними сервісами та технологіями Microsoft, підтримка різних мов програмування	Швидка розробка крос-платформових додатків, гарнітурна сумісність	Використання JavaScript для швидкої розробки крос-платформових додатків
Тестування	Підтримка автоматичних тестів, профілювання, налагодження	Інструменти для тестування додатків	Інструменти для тестування та профілювання додатків	Інструменти для тестування та профілювання додатків	Вбудовані засоби тестування	Інструменти для тестування додатків

Аналізуючи таблицю порівняння інструментів розробки додатків, можна визначити їхні основні характеристики та функціональність. Кожен з інструментів, таких як AppCode, Xcode, Android Studio, Visual Studio, Flutter та React Native, спеціалізується на розробці для певних платформ, таких як iOS, Android, Windows, або на крос-платформовій розробці. Вони підтримують різні мови програмування, такі як Swift, Objective-C, Java, Kotlin, Dart, JavaScript, що дає розробникам можливість вибору залежно від їхніх потреб і вподобань. Кожен інструмент також має свої унікальні функціональні можливості, такі як інтелектуальні функції, інструменти тестування, підтримка різних мов програмування. Вибір інструменту для розробки додатків залежить від ряду факторів, таких як платформа, мова програмування, функціональні вимоги проекту, а також власних уподобань і навичок розробника. Кожен інструмент має свої переваги і обмеження, і важливо обрати той, який найкраще відповідає конкретним потребам та вимогам проекту.

Висновки за розділом 1

Операційні системи мобільних пристроїв є краєважливим елементом для їхньої ефективної роботи та функціональності. Android, як найбільш розповсюджена операційна система, відкриває широкі можливості для користувачів та розробників завдяки своїй відкритій архітектурі. iOS, з іншого

боку, славиться своєю безпекою та оптимізацією для пристроїв Apple, пропонуючи унікальний досвід використання. У той час як Windows Mobile, хоча й не досяг такого рівня популярності, пропонує інші підходи до інтерфейсу та інтеграції з іншими сервісами Microsoft. Враховуючи ці відмінності, вибір операційної системи залежить від індивідуальних потреб користувача та специфіки проекту.

Різноманітність типів мобільних застосунків відображає різноманітність потреб користувачів. Від соціальних мереж до фінансових та подорожніх додатків, кожна категорія надає унікальні можливості для взаємодії та задоволення потреб користувачів. Розуміння цього різноманіття дозволяє розробникам створювати додатки, які ефективно відповідають на запити та очікування аудиторії.

Апаратна частина мобільних пристроїв відіграє ключову роль у їхньому функціонуванні та продуктивності. Висока якість дисплею, потужний процесор, ефективна батарея та інші складові забезпечують зручність користування та високу продуктивність. Зростаюча складність та функціональність мобільних пристроїв вимагає постійного вдосконалення апаратної складової для задоволення потреб сучасних користувачів.

Вибір правильного інструменту залежить від потреб та вимог конкретного проекту, а також від власних навичок та вподобань розробника. Розуміння функціональності та можливостей кожного інструменту дозволяє здійснювати обгрунтований вибір та забезпечує успішну розробку додатків для мобільних пристроїв.

РОЗДІЛ 2
ТИПИ ЗАГРОЗ МОБІЛЬНИХ ПРИСТРОЇВ

Мобільні пристрої, такі як смартфони та планшети, стали невід'ємною частиною нашого повсякденного життя. Однак разом із їх зручністю і функціональністю приходять і різноманітні загрози. Поняття типів загроз мобільних пристроїв відноситься до різних видів потенційних небезпек, які можуть виникнути під час використання мобільних пристроїв, таких як смартфони, планшети, носимі гаджети тощо. Ці загрози можуть включати в себе шкідливі програми, атаки на безпеку, витік конфіденційної інформації, втрату пристроїв та інші. Такі загрози можуть бути спрямовані на використання особистої інформації користувача, отримання доступу до конфіденційних даних, або завдання шкоди пристрою чи його користувачеві.

Огляд «BYOD & Mobile Security Report» на основі опитування 1 100 респондентів наводить статистику найбільш небезпечних проблем, пов'язаних з використанням мобільних пристроїв (рис.2.1).

Рисунок 2.1 – Найбільш небезпечні проблеми, пов'язані з використанням мобільних пристроїв [14, с.32]

Згідно з оглядом «BYOD & Mobile Security Report», найбільш небезпечними проблемами, пов'язаними з використанням мобільних пристроїв, є: втрата даних компанії або клієнтів, що становить 67%, свідчить про серйозні наслідки для компаній та їх клієнтів у випадку витоку конфіденційної інформації. Несанкціонований доступ до даних і систем компанії представляє загрозу безпеці, яка може призвести до витоку чутливої інформації або порушення конфіденційності даних. Завантаження користувачами додатків або контенту з вбудованими «дірками» може стати вихідною точкою для шкідливих атак або витоку даних. Зараження шкідливим кодом є загрозою, яка може призвести до втрати контролю над пристроєм або витоку особистих даних. Крадіжка або втрата пристроїв може призвести до витоку конфіденційної інформації або зловживання даними через фізичний доступ. Неможливість призначити заходи безпеки для кінцевого пристрою може зробити пристрої більш уразливими перед різними загрозами. Гарантії своєчасного оновлення програмного забезпечення безпеки є ключовим для забезпечення безпеки пристроїв. Ці дані свідчать про важливість ретельного управління безпекою мобільних пристроїв у корпоративному середовищі та наголошують на потребі вдосконалення заходів безпеки та освіти користувачів щодо правильного використання мобільних технологій.

2.1. Програмні загрози

Програмні загрози – це небезпеки, що виникають внаслідок дій шкідливих програм або недоліків у програмному забезпеченні, які можуть призвести до порушення безпеки, конфіденційності або доступності даних на мобільних пристроях.

До програмних загроз можна віднести:

1. Віруси – це шкідливі програми, які можуть вкрадатися в систему та поширюватися між пристроями, завдавати шкоди шляхом видалення, модифікації або крадіжки даних.

– Adware і клікери. Іноді для даного виду загроз використовується термін «Madware» (Mobile Adware). Основна мета цього класу шкідливого програмного забезпечення (ШПЗ) – показ користувачеві нерелевантної реклами і генерування штучних переходів на сайти рекламодавців. За допомогою Madware зловмисники заробляють «кліки» і демонструють оплачують їх компаніям ілюзію інтересу користувачів;

– Spyware – ПЗ, що здійснює крадіжку персональних даних або стеження за своїм носієм. Фактично, мобільний пристрій може перетворитися на повноцінний «жучок», передаючи зловмисникам дані про мережеву активність, геолокацію, історію переміщень, а також фото і відеоінформацію, дані про покупки, кредитні картки та ін.;

– дроппер – ШПЗ, метою якого є скачування іншого шкідливого ПЗ;

– бот-агент бот-мереж, ШПЗ, яке за командою C&C-сервера здійснює необхідну зловмисникові мережеву активність.

2. Шпигунське програмне забезпечення (Spyware) – це тип шкідливого програмного забезпечення, яке призначене для таємного відстеження дій користувача на його мобільному пристрої та збирання різних видів особистих даних без його згоди або знання. Загальна характеристика включає:

– таємність дій. Одна з ключових характеристик шпигунського ПЗ – це його здатність до таємного функціонування. Користувач, який інсталює програму, може навіть не підозрювати про її наявність, оскільки вона може приховуватися під іншими назвами або процесами;

– відстеження дій користувача. Шпигунське ПЗ відстежує різні дії користувача, такі як введення паролів, клікання по посиланнях, перегляд веб-сторінок, відправка повідомлень тощо. Всі ці дані можуть бути записані та відправлені зловмиснику;

– збір особистих даних. Цільова інформація, яку збирає шпигунське ПЗ, може включати в себе такі особисті дані, як паролі, історія перегляду веб-сайтів, фінансові дані, особисту інформацію з соціальних мереж, номери кредитних карток та інші конфіденційні дані;

– передача даних зловмиснику. Зібрана інформація передається зловмиснику через інтернет. Це може статися через автоматичні відправлення на зазначені адреси електронної пошти, за допомогою віддалених серверів або інших методів зв'язку;

– порушення приватності та безпеки. Використання шпигунського ПЗ може призвести до серйозних порушень приватності та безпеки, оскільки користувач не контролює, яка саме інформація збирається та що з нею відбувається;

– шляхи поширення. Шпигунське ПЗ може бути поширене через недовірені додатки, фішингові веб-сайти, електронну пошту зі шкідливими вкладеннями та інші шляхи [15].

3. Рекламне програмне забезпечення (Malvertising) представляє собою форму шкідливого програмного коду, який вбудовується у рекламні матеріали, що розміщуються на веб-сайтах або в мобільних додатках. Шкідливий код може відкривати шлях для різних видів атак, включаючи встановлення шкідливих програм або викрадення інформації:

– схема функціонування. Рекламне ПЗ працює шляхом вбудовування шкідливого коду в рекламні банери або відеоролики, які зазвичай розміщуються на веб-сайтах або в мобільних додатках;

– використання уразливостей. Може використовувати вразливості у веб-браузерах або в операційних системах мобільних пристроїв для виконання свого шкідливого коду без уведення користувача в обман;

– підміна легітимної реклами, Часто рекламне ПЗ може підмінювати легітимні рекламні банери або відеоролики на веб-сайтах своїми власними шкідливими рекламними матеріалами, що може спричинити виникнення атаки навіть на довіреному ресурсі;

– шляхи атаки. Після того, як шкідливий код активується, він може виконувати різні дії, включаючи встановлення шкідливих програм, перенаправлення користувача на сайти зі зловмисним вмістом або навіть викрадення особистої інформації, такої як логіни та паролі [16].

Таким чином, програмні загрози для мобільних пристроїв поширені та діють

у різних формах, зазвичай шляхом використання недоліків у програмному забезпеченні або вразливостей в операційних системах. Програмні загрози можуть використовувати різні методи та вектори атаки, такі як електронна пошта, веб-сайти, недоліки програмного забезпечення та соціальна інженерія.

2.2. Web-загрози

Оскільки мобільні пристрої часто підключені до Інтернету і використовуються для доступу до веб-сервісів, веб-загрози створюють проблеми для мобільних пристроїв.

Web-загрози – це різні види небезпек, які можуть виникати під час використання Інтернету та перебування на веб-сайтах. Ці загрози можуть стати причиною порушень безпеки, втрати конфіденційності даних, а також викликати інші негативні наслідки. До них можна віднести:

Фішингові атаки. Використовують веб-сторінки або інші інтерфейси користувача, призначені для того, щоб змусити користувача надати зловмиснику інформацію, таку як дані для входу в обліковий запис.

Сторона, що видає себе за легальний сервіс. Зловмисники часто використовують електронну пошту, текстові повідомлення, Facebook та Twitter для надсилання посилань на фішинг-сайти.

Швидке завантаження. Завантаження програми починається автоматично, коли користувач заходить на веб-сторінку.

Використання браузера. Браузерні подвиги призначені для використання вразливостей у веб-браузері або програмному забезпеченні, яке можна запустити через веб-браузер, наприклад, Flash-програвач, зчитувач PDF або переглядач зображень.

2.3. Мережеві загрози

Мережеві загрози безпеці – це загрози, де потенційним джерелом є

використання вразливостей через мережу оператора зв'язку на прикладному рівні або всередині додатків, файлів або даних (в плані дані/ послуга), також, як і в плані контролю, що відповідає за конфігурацію і управління пристроєм. Мережеві загрози безпеці здійснюються через мережу оператора або мережеві протоколи, а також пристрої, програми та дані, які постійно використовують мережу. Пристрої, що використовують для зв'язку мережі Wi-Fi і стільникові, більш доступні і вразливі, ніж пристрої, що використовують тільки дротові мережі. Ці загрози мають високий рівень ризику і специфічні виключно для мобільних пристроїв.

Wi-Fi. Мобільні пристрої використовують вбудовані модеми Wi – Fi – бездротовий спосіб взаємодії на основі сімейства стандартів IEEE 802.11 a/b/g/n. такі пристрої можуть підключатися до будь-якої мобільної, персональної або корпоративної точки доступу або іншого подібного пристрою для взаємодії «точка - точка». Пристрої, що використовують Wi-Fi, уразливі для перехоплення іншим Wi-Fi-пристроєм, бездротовим програмним інструментарієм, а також аналізатором сигналів. Неконтрольовані точки доступу (несанкціонована точка всередині адміністративно контрольованого домену)-також потенційна загроза, що піддає мобільний пристрій, зокрема, небезпеки «глушіння» (блокування) мобільного пристрою, атаки посередника або «людина посередині» (man-in-the-middle).

Стільниковий зв'язок. Мобільні пристрої можуть взаємодіяти з використанням стільникових мереж різних технологій (GSM, EDGE, LTE та ін.). Деякі оператори зв'язку можуть надавати криптографічні способи захисту. Дані та голос у мережах стільникового зв'язку можуть бути перехоплені, а конфігурація та ключові компоненти пристрою можуть бути скомпрометовані через канали управління.

Bluetooth. Bluetooth – це малопотужна бездротова технологія короткої дії, що забезпечує взаємодію мобільних пристроїв на основі стандартів серії IEEE 802.15.1. Bluetooth використовується для передачі даних між пристроями всередині персональної мережі (personal area network, PAN), а також для передачі команд і голосової взаємодії між пристроєм і гарнітурою. Bluetooth має вбудовані механізми шифрування і аутентифікації (E1, E21, E22 на базі алгоритму SAFER+, у версії 4.0

– aes), проте відомі уразливості і «проломи» цієї технології, такі, як перехоплення ключів при ініціалізації сеансу [17].

Інфрачервона взаємодія. Інфрачервона взаємодія – це малопотужна бездротова технологія ближньої дії в інфрачервоному діапазоні, що забезпечує взаємодію мобільних пристроїв по протоколах Phillips RC-5, Sony SIRC і деяких інших. Інфрачервона взаємодія, як і Bluetooth, використовується для передачіданих між пристроями всередині персональної мережі (personal area network, PAN),а також для односторонньої передачі команд. Інфрачервона взаємодія не має механізмів шифрування і аутентифікації, і тому вразлива. Більшість вразливостей є специфічними та залежать від виробника, наприклад, переповнення буфера при отриманні інфрачервоного коду взаємодії.

Near Field Communication. Near Field Communication (NFC) – це набір стандартів для малопотужного, надближчого бездротового способу взаємодії «точка – точка». Ця технологія використовується для ідентифікаційних карт і транзакцій з банківськими картами спочатку 2012 р реалізації NFC в першу чергу є об'єктами атак фізичного рівня, таких, як перехоплення і нав'язування сигналу [18, с.43].

Маніпуляції з даними при передачі. Дані і голос при передачі можуть бути змінені або вибірково блоковані з метою компрометації з'єднання. Однією з відмінних особливостей мобільних пристроїв є те, що вони часто перемикаються між засобами та операторами, перескакуючи з однієї базової станції стільникового зв'язку на іншу або перемикаючись із стільникового зв'язку на Wi-Fi. Також мобільні пристрої мають порівняно малі обчислювальні потужності і обсяги пам'яті в порівнянні з ПК і серверами. Ці особливості призводять до того, що багато мобільних додатків отримують доступ до віддалених сховищ даних (не розміщених на мобільному пристрої), тим самим вивантажуючи обчислювальні потужності мобільного пристрою для підвищення функціональності. Таким чином, мобільні пристрої збільшують обсяги даних, що передаються через недовірені механізми засобів зв'язку. Крім того, хмарні сервіси від виробника пристрою або третьої сторони пропонують послуги зберігання файлів, обробки додатків і даних, а також

функції управління в розподіленому середовищі, що знижує обмеження на внутрішню пам'ять пристрою при збільшенні обсягу даних, що передаються між хмарою і мобільним пристроєм. Збільшення потоку обмінних даних надає противнику більше поле для нападу, метою якого є передані дані. В результаті критичні дані можуть бути ненавмисно розкриті або скомпрометовані через слабкості архітектури Хмари, некоректної реалізації або зловмисних дій, що може привести до значного збитку. Ця загроза пов'язана з високим ризиком і специфічна для бездротових і хмарних технологій.

2.4. З’єднання з недовіреним сервісом

З'єднання з недовіреним сервісом є однією з типових загроз для мобільних пристроїв, оскільки може призвести до різних негативних наслідків для їх безпеки та приватності. Це загроза полягає в підключенні мобільного пристрою до веб-сайтів, платформ або сервісів, якими користувач не довіряє або які можуть бути потенційно шкідливими. Такий вид загрози може включати [19, с.43]:

– ризик інфікування шкідливим програмним забезпеченням. Підключення до недовіреного сервісу може сприяти введенню шкідливого програмного забезпечення на мобільний пристрій, такого як віруси, троянці або шпигунське ПЗ;

– порушення конфіденційності даних. Ненадійний сервіс може використовувати збирання особистих даних користувачів без їх згоди або неправомірно використовувати ці дані;

– поширення шахрайських схем. Деякі недовірені сервіси можуть бути складовою частиною шахрайських схем або шахрайства, що може призвести до втрати грошей або інших фінансових втрат;

– порушення безпеки мережі. Підключення до ненадійних сервісів може також викликати загрози для безпеки самої мобільної мережі, а не лише самого пристрою.

Тому, з'єднання з недовіреним сервісом може становити серйозну загрозу для

безпеки та приватності мобільних пристроїв, і вимагає обережного підходу з боку користувача при взаємодії з такими сервісами.

2.5. GPS/Місцезнаходження

Майже всі мобільні пристрої забезпечують для своїх додатків той чи інший рівень служби геолокації. Такі програми можуть використовувати цю службу для відображення поточного місцезнаходження пристрою на карті, знаходити ресурси поблизу, відстежувати маршрут користувача та навіть виконувати популярну у користувачів функцію навігації маршрутом руху. Разом з тим ця служба має потенційну можливість розкриття місцезнаходження пристрою або виводити некоректну інформацію про місцезнаходження Користувача за рахунок зовнішніх перешкод або маніпуляцій. Ця загроза характерна виключно для мобільних пристроїв.

Джерела даних геолокації. Збір даних позиціонування від різних джерел-це пасивний процес: джерела періодично розсилають інформацію про місцезнаходження в широкомовному режимі. Оскільки процес збору є пасивним, двостороння автентифікація відсутня і, таким чином, цілісність даних позиціонування не гарантована. При цьому використовуються різні джерела даних позиціонування (сигнатури стільники 2/3/4G мобільного пристрою, сигнатури Wi-Fi, внутрішній приймач A-GPS).

Тріангуляція. Шляхом комбінування двох і більше джерел даних позиціонування і, використовуючи техніку тріангуляції, додатки мобільного пристрою можуть значно підвищити точність визначення свого місцезнаходження, забезпечуючи даними залежні служби, якщо один і більше їх власних джерел недоступний.

Відстеження (Tracking) Відстеження з використанням служби геолокації мобільного пристрою корисна для вирішення багатьох штатних завдань, таких як виявлення загубленого пристрою [20, с.37].

Однак ця ж служба може використовуватися для збору інформації та

створення позаштатних ситуацій для організації або користувача. Незаконне відстеження може бути виконано шляхом вилучення даних (data mining) і перегляду «гео-маркованих» (geotagged) записів, зображень або інших даних.

«Гео-маркування» (Geotagging). Гео-маркування-це процес додавання географічних ідентифікаційних метаданих до фото, Відео та інших даних. Витяг даних з «гео-маркованих» зображень та інших даних, записаних мобільним пристроєм – це метод, що дозволяє відстежувати місце розташування пристрою, як в легальних, так і в незаконних цілях

Підміна місцезнаходження (Location Spoofing). Для передачі некоректної інформації місцезнаходження може використовуватися ретрансляція прихованих сигналів GPS, а також неправдива інформація Місцезнаходження від веж стільникового зв'язку і «гарячих точок» Wi-Fi. Такі атаки можуть привести до того, що мобільний пристрій буде оперувати помилковою інформацією місцезнаходження, що може привести до некоректного функціонування додатків, яким необхідні точні дані місцезнаходження.

2.6. Небезпечне зберігання даних

Уразливості небезпечного сховища даних виникають, коли команди розробників припускають, що користувачі або шкідливе програмне забезпечення не матимуть доступу до файлової системи мобільного пристрою та подальшої конфіденційної інформації в сховищах даних на пристрої. Файлові системи легко доступні. Слід уникати використання неякісних бібліотек шифрування. Рутинг або джейлбрейк мобільного пристрою дозволяє обійти будь-які засоби захисту від шифрування. Якщо дані не захищені належним чином, для перегляду даних програми достатньо спеціалізованих інструментів.

Мобільні додатки, які зберігають дані користувачів у небезпечних умовах, можуть бути вразливими до злому, порушення даних або несанкціонованого доступу. Це може призвести до компрометації конфіденційної інформації

користувача, крадіжки особистих даних, фінансового шахрайства або інших форм кіберзлочинності.

У Java приклад вразливого коду для небезпечного зберігання даних у мобільних додатках може виглядати наступним чином:

```
private void saveCredentials(String username, String password) {
    try {
        FileOutputStream fos = openFileOutput("credentials.txt", Context.MODE_PRIVATE);
        fos.write(username.getBytes());
        fos.write(password.getBytes());
        fos.close();
    } catch (Exception e) {
        e.printStackTrace();
    }
```

У наведеному вище коді метод saveCredentials використовується для збереження облікових даних користувача у файлі під назвою «credentials.txt» в каталозі особистих даних програми. Однак цей код не використовує жодних методів шифрування або хешування для захисту даних користувача. Таким чином, якщо зловмисник отримає доступ до пристрою, він може легко отримати ім'я користувача та пароль.

У Swift приклад вразливого коду для небезпечного зберігання даних у мобільних додатках може виглядати наступним чином:

```
func saveCreditCardInfo(cardNumber: String, expirationDate: String, cvv: String) {
    let filePath = getDocumentsDirectory().appendingPathComponent("creditcard.txt")
    do {
        try "\(cardNumber),\(expirationDate),\(cvv)".write(to: filePath, atomically: true, encoding: .utf8)
    } catch {
```

```
        print("Error saving credit card info")
    }
}
```

Метод saveCreditCardInfo використовується для збереження інформації про кредитну картку Користувача у файлі під назвою «creditcard.txt « у каталозі документів програми. Якщо зловмисник отримає доступ до пристрою, він може легко отримати дані кредитної картки Користувача.

У Python коду може виглядати наступним чином:

```
def savePersonalInfo(name, email, phone):
with open('personalinfo.txt', 'w') as file:
    file.write(name + ',' + email + ',' + phone)
```

Функція savePersonalInfo використовується для збереження особистої інформації користувача у файлі під назвою “personalinfo.txt " у поточному каталозі програми. Якщо зловмисник отримає доступ до пристрою, він може легко отримати особисту інформацію Користувача.

До прикладів використання небезпечного сховища даних у мобільних додатках входять:

Крадіжка облікових даних. Зловмисник може скористатися незахищеним сховищем даних в Мобільних додатках для крадіжки облікових даних Користувача для входу в систему. Наприклад, якщо програма зберігає ім'я користувача та пароль у відкритому тексті, зловмисник, який отримав доступ до пристрою, може легко отримати облікові дані користувача та використовувати їх для входу в обліковий запис Користувача. Це може призвести до крадіжки особистих даних, фінансових шахрайств або інших форм кіберзлочинності.

Маніпулювання даними – якщо програма зберігає фінансові дані Користувача без належного шифрування, зловмисник, який отримав доступ до пристрою, може змінити Дані для переказу грошей або здійснення несанкціонованих транзакцій, що може призвести до фінансових втрат і погіршення кредитного рейтингу користувача.

Несанкціонований доступ. Зловмисник використовує незахищене сховище

даних у мобільних додатках для незаконного доступу до інформації користувача. Наприклад, якщо програма зберігає особисту інформацію без належного шифрування, зловмисник, який отримав доступ до пристрою, може переглянути або скопіювати ці дані [21, с.129].

Установка шкідливого ПЗ. Шахрай може скористатися незахищеним сховищем даних у мобільних додатках для встановлення шкідливого ПЗ на пристрій. Якщо програма зберігає дані Користувача без належного шифрування, зловмисник, який отримав доступ до пристрою, може ввести шкідливий код у Дані для виконання довільних команд або завантаження та встановлення шкідливого програмного забезпечення. Це призводить до повної компрометації пристрою та даних користувача.

2.7. Ненавмисний витік даних

Ненавмисний витік даних відбувається, коли розробник ненавмисно розміщує конфіденційну інформацію або дані в місці на мобільному пристрої, яке легко доступне для інших програм на пристрої. По-перше, код розробника обробляє конфіденційну інформацію, надану користувачем або серверною частиною. Під час цієї обробки побічний ефект (невідомий розробнику) призводить до того, що ця інформація розміщується в небезпечному місці на мобільному пристрої, до якого інші програми на пристрої можуть мати відкритий доступ. Як правило, ці побічні ефекти виникають через операційну систему (OS), що використовується на мобільному пристрої. Це буде дуже поширеною вразливістю для коду, створеного розробником, який не має глибоких знань про те, як ця інформація може зберігатися або оброблятися базовою операційною системою. Порушення даних легко виявити, перевіривши всі місця розташування мобільних пристроїв, доступні для всіх програм, на наявність конфіденційної інформації в додатку.

Порушення даних відбувається, коли конфіденційні дані ненавмисно стають загальнодоступними під час транспортування, у стані спокою або під час

використання:

– дані, виявлені при передачі – дані, що передаються по електронній пошті, за допомогою викликів API, чатів та інших засобів зв'язку;

– незахищені дані – це може статися через неправильно налаштоване хмарне сховище, небезпечні бази даних та залишені без нагляду або втрачені пристрої;

– незахищені дані в процесі використання, такі як дані на принтерах, скріншотах, буферах обміну та USB-накопичувачах.

До способів витоку даних в мобільних додатках можна віднести:

1) Електронне спілкування. Співробітники часто отримують доступ до Інтернету, електронної пошти та облікових даних для обміну миттєвими повідомленнями в рамках своїх службових обов'язків. Проблема полягає в тому, що хакери розглядають усі ці засоби масової інформації як свої основні цілі, що є проблематичним. З метою проникнення в систему використовуються різні стратегії, включаючи фішинг, підміну і атаку цільових жертв шкідливим ПЗ, що призводить до витоку даних.

2) Випадковий витік. Ненавмисний або навмисно навмисний витік даних може статися в будь-який час. Такі незаконні дії часто трапляються нерегулярно та за незвичних обставин. Більшість порушень даних є результатом людської помилки і є ненавмисними. Одного разу працівник помилково надіслав електронний лист не тій особі, ненавмисно надавши цій особі доступ до особистих даних.

Такі ненавмисні порушення даних мають серйозні наслідки, включаючи штрафи та шкоду репутації.

3) Незадоволені співробітники. Саме ті співробітники, які незадоволені своєю роботою, або планують, або беруть участь у витоку даних. Більшість компаній вважають, що витік електронної пошти та втрачені або вкрадені ноутбуки є основними джерелами втрати даних. З іншого боку, найчастіше витік даних відбувається з таких пристроїв, як принтери, фотоапарати, копіювальні апарати та портативні USB-накопичувачі. Незважаючи на підписання суворого трудового

договору, ніщо не завадить незадоволеному співробітнику розкрити дані, якщо він незадоволений або хакери пообіцяли йому значні виплати.

Причини витоку даних наступні [22]:

1) Застарілі методи та інструменти. Хоча існує багато нових загроз для даних, все ще важливо мати справу зі старими стратегіями атак, які використовують переваги застарілих систем та інструментів. Сучасні організації часто використовують не тільки хмарні Інструменти та сторонні пропозиції SaaS, але й фізичні пристрої, такі як настільні комп'ютери, USB-накопичувачі та принтери.

Інструменти можуть знадобитися для здійснення юридичних дій (наприклад, для того, щоб співробітники могли роздруковувати презентації вдома), вони також становлять значний ризик. Наприклад, співробітники можуть втратити USB-накопичувач або зовнішній пристрій, що містить конфіденційну інформацію. Пристрій може бути вкрадений зловмисником, який хоче обійти систему безпеки компанії.

2) Проблеми з неправильним налаштуванням. Складність зростає, коли в конфігурації мережевої інформаційної системи використовуються прикладне програмне забезпечення, хмарні сервіси та засоби машинного навчання. Щоб алгоритми ML мали доступ до необхідних даних і при цьому запобігали непотрібному доступу до них, процеси налаштування даних мають вирішальне значення. Помилки конфігурації є загальними, оскільки система ускладнюється.

3) Атаки соціальної інженерії. Зловмисники систематично використовують методи соціальної інженерії для обману привілейованих користувачів, таких як співробітники, з метою отримання конфіденційної інформації. Ці кіберзлочинці регулярно намагаються втягнути свої жертви в обман, виступаючи, наприклад, як колеги або члени IT-відділу, і придумуючи виглядні виправдання для запиту облікових даних для отримання доступу.

Спроби соціальної інженерії часто спрямовані на отримання телефонних номерів, реєстраційних даних або імен осіб, які мають привілейований доступ. Щоб запобігти доступу співробітників та зловмисників до даних, до яких вони не мають

доступу, користувачі повинні уникати розголошення конфіденційної інформації авторизованим користувачам.

4) Уразливості нульового дня. Уразливості «нульового дня» можуть призвести до постійних загроз, які призводять до прихованої витоку даних протягом декількох місяців або навіть років, перш ніж вони будуть виявлені. Коли новини повідомляють про серйозне порушення, багато організацій дізнаються про ці загрози лише після їх виявлення.

Витік даних у мобільних додатках є серйозною загрозою для безпеки та конфіденційності інформації. Причини витоку даних можуть бути різноманітні, включаючи помилки користувачів, атаки хакерів, ненавмисні витоки та проблеми з налаштуванням систем. Зловмисники використовують різні методи, такі як соціальна інженерія, фішинг та використання застарілих інструментів, для отримання доступу до конфіденційної інформації. Щоб запобігти витокам даних, необхідно посилення заходів безпеки, постійне оновлення систем та програмного забезпечення, а також освіта користувачів щодо безпечного використання мобільних технологій.

2.8. Проблеми авторизації та аутентифікації

Мобільні пристрої широко поширені та зручні, але вони також створюють серйозні проблеми для мережевої безпеки. Аутентифікація, процес підтвердження особи користувача або пристрою, має важливе значення для захисту даних і ресурсів від несанкціонованого доступу. Однак мобільна аутентифікація несе ризики та вразливості, які можуть поставити під загрозу безпеку та конфіденційність користувачів та організацій [23, с.52].

1) Ненадійні або вкрадені облікові дані. Одним з найбільш основних і поширених ризиків мобільної аутентифікації є використання ненадійних або вкрадених облікових даних, таких як паролі, PIN-коди або біометричні дані. Ці облікові дані можуть бути легко вгадані, зламані або перехоплені зловмисниками за допомогою різних методів, таких як фішинг, брутфорс, кейлоггінг або підміна.

Отримавши облікові дані, зловмисник може видати себе за законного користувача і отримати доступ до його облікових записів, даних або служб.

2) Небезпечні канали зв'язку. Ще одним поширеним ризиком для мобільної аутентифікації є використання небезпечних каналів зв'язку, таких як загальнодоступні мережі Wi-Fi, Bluetooth-з'єднання або SMS-повідомлення. Ці канали можуть бути перехоплені, змінені або перенаправлені зловмисниками, які можуть перехоплювати дані для автентифікації або виконувати атаки «людина посередині». Зловмисник може перехопити SMS-повідомлення, що містить одноразовий пароль, і використовувати його для автентифікації як користувача.

3) Шкідливі або скомпрометовані додатки. Третім поширеним фактором ризику для перевірки автентичності мобільних пристроїв є наявність шкідливих або скомпрометованих додатків на пристрої. Ці програми можуть виконувати різні шкідливі дії, такі як крадіжка або зміна автентифікаційних даних, введення шкідливого коду або використання вразливостей. Наприклад, програма може отримати доступ до камери або мікрофона пристрою та отримати біометричні дані користувача, такі як розпізнавання обличчя або голосу.

4) Втрата або крадіжка пристрою. Четвертим поширеним ризиком для мобільної аутентифікації є можливість втрати або крадіжки пристрою. Якщо пристрій потрапить у неправильні руки, зловмисник може отримати доступ до даних та ресурсів пристрою або обійти механізми автентифікації. Наприклад, зловмисник може використовувати сканер відбитків пальців пристрою або систему розпізнавання обличчя, щоб розблокувати пристрій і отримати доступ до облікових записів користувача.

Технічні наслідки поганої автентифікації полягають у тому, що рішення не може ідентифікувати користувача, який виконує запит на виконання дії. Відразу ж рішення не зможе реєструвати або перевіряти дії користувача, оскільки неможливо встановити особу користувача. Це призведе до неможливості виявити джерело атаки, природу будь-яких вразливостей, що лежать в її основі, або способи запобігання майбутнім атакам. Збої аутентифікації можуть також призвести до збоїв в авторизації. При збої елементів управління аутентифікацією рішення не

зможе підтвердити особу користувача. Це посвідчення пов'язане з роллю користувача і відповідними дозволами. Якщо зловмисник може анонімно виконувати конфіденційні функції, це вказує на те, що базовий код не перевіряє дозволи користувача, який надсилає запит на виконання дії. Отже, анонімне виконання коду виявляє збої як в елементах керування автентифікацією, так і в авторизації [24].

Технічні наслідки неправильної авторизації аналогічні технічним наслідкам неправильної аутентифікації. Технічні наслідки можуть бути найрізноманітнішими і залежати від характеру виконуваних функцій з надмірними привілеями. Наприклад, виконання функцій віддаленого або локального адміністрування з надмірними привілеями може призвести до руйнування систем або доступу до конфіденційної інформації.

Висновки за розділом 2

Загрози для мобільних пристроїв включають різноманітні аспекти, які варіюються від програмних до мережевих проблем безпеки. Програмні загрози включають в себе шпигунське програмне забезпечення, рекламне ПЗ та інші віруси , які можуть шкодити пристрою та даним користувача. Web-загрози виникають через несприятливі веб-сайти або шкідливі веб-додатки, які можуть заражати пристрої шкідливим кодом. Мережеві загрози включають в себе атаки типу «перехоплення даних», які можуть стежити за активністю користувача та отримувати конфіденційну інформацію. З'єднання з ненадійними сервісами може призвести до витоку даних або компрометації пристрою.

GPS/Місцезнаходження може бути використане для стеження за користувачем або витоку особистої інформації. Небезпечне зберігання даних може призвести до неправомірного доступу до конфіденційної інформації, тоді як ненавмисний витік даних може стати результатом людських помилок або вразливостей програмного забезпечення. Проблеми з авторизацією та аутентифікацією можуть призвести до несанкціонованого доступу до пристрою або інформації.

Загальною тенденцією є те, що мобільні пристрої стають все більш уразливими перед різноманітними загрозами, і важливо приділяти належну увагу заходам безпеки для їх захисту.

РОЗДІЛ 3
ЗАСОБИ ЗАХИСТУ МОБІЛЬНИХ ПРОСТРОЇВ

3.1. Антивірусне програмне забезпечення

В даний час смартфони є найкращим пристроєм для перегляду веб-сторінок, надсилання електронної пошти, використання соціальних мереж та здійснення покупок. Завдяки своїм розмірам Смартфони легко носити в кишенях, гаманцях або портфелях. На жаль, популярність смартфонів є живильним середовищем для кібератак. Операційні системи смартфонів не містять програмного забезпечення для захисту даних. Наприклад, традиційне програмне забезпечення для захисту персональних комп'ютерів (ПК), таке як брандмауери, антивіруси та засоби шифрування, наразі недоступне у смартфонах (Ruggiero, 2011). Крім того, операційні системи мобільних телефонів оновлюються не так часто, як їх аналоги на ПК. Зловмисники можуть використовувати цю прогалину в безпеці на свою користь. Прикладом такого розриву в безпеці є напад на День Святого Валентина 2011 року.

Зловмисники розповсюдили мобільний додаток для обміну фотографіями, який таємно надсилав преміум-текстові повідомлення з мобільного телефону Користувача. Таким чином, цей приклад ілюструє важливість наявності політики безпеки для мобільних телефонів.

Одним із найефективніших засобів захисту мобільних пристроїв є антивірусне програмне забезпечення. Воно виконує функції виявлення та нейтралізації шкідливих програм, захисту даних та приватності користувачів. Антивірусне програмне забезпечення для мобільних пристроїв забезпечує комплексний захист від різноманітних кіберзагроз, що дозволяє користувачам безпечно використовувати свої гаджети у повсякденному житті.

Android – одна з найпопулярніших операційних систем для смартфонів на сьогоднішній день. У 2015 році її частка на ринку становила понад 80%, згідно з даними Worldwide Quarterly Mobile Phone Tracker. Така популярність в значній мірі

обумовлена великою екосистемою, що пропонує безліч додатків на будь-який смак. Лише в офіційному магазині Google Play у 2015 році було доступно понад 1,6 мільйона додатків. Однак не всі з цих додатків є безпечними. Деякі програми створюються зі злим наміром вкрасти конфіденційну інформацію Користувача або отримати доступ до преміум-сервісів за його рахунок. Оскільки багато користувачів виконують конфіденційні завдання, такі як онлайн-банкінг, на своїх телефонах, і багато пристроїв оснащені датчиками, що порушують конфіденційність, такими як GPS, це становить високий ризик. Крім того, деякі програми не є відверто шкідливими, але мають серйозні уразливості в системі безпеки. Ці вразливості дозволяють шкідливим програмам, встановленим на тому ж пристрої, або навіть віддаленим зловмисникам красти конфіденційні дані або маніпулювати пристроєм [25, с.129].

Щоб захистити свої пристрої та дані від атак, будь то за допомогою шкідливих програм або використання вразливостей безпеки, багато користувачів покладаються на програми безпеки від відомих виробників. Як і їхні настільні аналоги, ці програми пропонують послуги, що виходять за рамки традиційного антивірусного сканування. Крім перевірки списку встановлених додатків на наявність відомих небажаних програм, ці програми блокують відображення браузером фішингових або інших шкідливих веб-сайтів і пропонують заблокувати або стерти дані з пристрою в разі його втрати або крадіжки. Хоча всі ці функції корисні і призначені для підвищення безпеки пристрою, вони, знову ж таки, розробляються людьми-розробниками додатків, які можуть допускати помилки. Попередні дослідження показали [22, 7, 8], що багато розробників Android або не пройшли належного навчання з безпеки, або, принаймні, не проводять ретельного тестування безпеки та аудиту своїх програм.

Сучасні антивірусні програми або програми безпеки для Android не тільки захищають користувача від відомих шкідливих програм за допомогою механізму перевірки на наявність шкідливих програм, але й оснащені додатковими функціями безпеки, які захищають користувача від шкідливих або небажаних дій. Кожен додаток безпеки містить різні функції безпеки. Однак усі ці функції можуть

працювати лише в тому випадку, якщо ними не можна маніпулювати, деактивувати або навіть використовувати для зловмисних цілей.

2.1 Механізм виявлення шкідливих програм

Кожне антивірусне додаток поставляється з механізмом перевірки на віруси, який на основі бази сигнатур визначає, чи є додаток шкідливим чи ні. Додаток часто завантажує оновлення для цієї бази даних із сервера оновлень відповідного виробника. Цей механізм оновлення працює без будь-якої взаємодії з користувачем і автоматично завантажує не тільки файли підписів, але й оновлення ядра сканування у вигляді виконуваних файлів коду або бібліотечного коду.

Вимоги: CAM модуль сканування повинен відповідати концепції доступності для забезпечення постійного захисту. Файли, завантажені за допомогою модуля оновлення, повинні відповідати концепції цілісності та автентичності, щоб виключити можливість встановлення несанкціонованих або підроблених вірусних баз або файлів коду. Більшість файлів підписів антивірусів також зашифровані для забезпечення конфіденційності з міркувань захисту інтелектуальної власності. Крім того, необхідно гарантувати доступність сервера оновлень, щоб користувачі завжди могли оновлювати свої сканери.

2.2 Захист від небажаної пошти

Функція захисту від небажаної пошти блокує небажані SMS-повідомлення або телефонні дзвінки.

Вимоги: заблоковані рядки SMS-повідомлень або телефонних номерів повинні відповідати принципам доступності та цілісності для захисту від маніпуляцій. Не повинно бути можливості обійти чорний або білий списки системи захисту. Крім того, ці списки повинні зберігатися в таємниці, оскільки особливо білі списки можуть містити конфіденційні дані користувача, наприклад, номери телефонів, що представляють інтерес для користувача [26, с.124].

2.3 Безпечний перегляд

Модуль безпечного перегляду відстежує роботу браузера, щоб запобігти доступу до шкідливих веб-сайтів, які користувач міг би випадково відвідати в іншому випадку. Фільтр зазвичай реалізується за допомогою локального проксі-

сервера, який працює в контексті антивірусної програми. Потім веб-браузер налаштовується на маршрутизацію всього трафіку через цей проксі-сервер. Для кожного доступу програма перевіряє запитувану URL-адресу на серверну службу, запущену постачальником послуг AV. Альтернативний метод, який не вимагає локального проксі-сервера, постійно переглядає історію браузера.

Коли користувач переходить на веб-сайт у своєму браузері, відповідна URL-адреса відображається у верхній частині його історії відвідувань. Додаток безпеки зчитує його звідти і відправляє на сервер постачальника мультимедійних послуг. Незалежно від того, як відстежується робота браузера, AV-програма повинна відображати попереджувальне повідомлення та запобігати завантаженню веб-сторінки, якщо відповідна URL-адреса була виявлена у чорному списку та вважається шкідливою. Для цього кроку блокування av-програми зазвичай містять спеціальні веб-сторінки або всередині програми, або на задній панелі Постачальника av-додатків, на які браузер перенаправляється замість того, щоб переходити за оригінальною шкідливою URL-адресою.

Вимоги: конфіденційність і цілісність URL-адреси, введеного користувачем, повинні бути захищені, поки він передається в серверну частину антивіруса. Модуль безпечного перегляду повинен відповідати концепції доступності, щоб усі запитувані URL-адреси дійсно могли бути перевірені. Крім того, захист не повинен впливати на поведінку користувача під час відвідування безпечних веб-сайтів. Функція блокування модуля безпечного перегляду також повинна бути надійною, шкідливий веб-сайт не повинен мати можливості обійти її.

2.4 Радник з налаштування пристрою

ОС Android пропонує різні настройки безпеки, такі як «дозволити установку додатків з невідомих джерел», «тип блокування екрану (pin-код, пароль, шаблон і т.д.)», «шифрування пристрою» і т. д. для забезпечення максимальної безпеки пристрою користувач повинен правильно налаштувати ці параметри. Тому багато програм безпеки містять модуль, який сканує телефон на наявність небезпечних налаштувань і дає рекомендації щодо покращення конфігурації пристрою.

Вимоги: справжність і цілісність цього модуля або його бази даних з

правилами Налаштування повинні бути гарантовані, щоб зловмисник не зміг впровадити слабкі конфігурації, які потім будуть запропоновані користувачеві.

2.5 Радник і захисник конфіденційності

Модуль privacy advisor захищає користувача від проблем, пов'язаних з конфіденційністю, таких як витік даних. Якщо телефон користувача загублений або вкрадений, він може, наприклад, відправити на телефон спеціальне SMS-повідомлення, що містить секретний токен або пароль. Після отримання такого спеціального SMS - повідомлення програма безпеки блокує або стирає дані з пристроїв, щоб запобігти витоку даних або просто зробити пристрій непридатним для використання злодієм. Інші програми можуть бути запитані віддалено за допомогою аналогічних SMS-команд для визначення місця розташування пристрою по GPS в спробі полегшити відновлення пристрою або ідентифікацію злодія.

Вимоги: Модуль захисту конфіденційності активно запускає механізми захисту, які можуть мати побічні ефекти, такі як втрата даних або блокування телефону. Тому механізм повинен бути автентифікований таким чином, щоб його могли запускати лише авторизовані користувачі. Крім того, після активації зловмисник не зможе обійти блокування пристрою або відновити дані звіддаленого пристрою.

2.6 Преміум-оновлення

Багато виробників антивірусів пропонують безкоштовну базову версію своїх інструментів. Якщо користувачеві потрібно більше функцій, він може заплатити та розблокувати преміум-функції. Поширені преміум-функції включають додаткові модулі захисту або частіші оновлення бази підписів.

Вимога: зловмисник не повинен мати можливості оновити додаток без будь-якої оплати. Ця вимога відрізняється від попередніх, оскільки захищає постачальника, а не користувача.

До прикладів популярного антивірусного програмного забезпечення для мобільних пристроїв входить:

1. Avast Mobile Security – це безкоштовне антивірусне програмне

забезпечення, яке пропонує широкий спектр функцій для захисту мобільних пристроїв. Основні функції включають сканування в реальному часі, яке виявляє та видаляє шкідливі програми, віруси та інші загрози в момент їх появи. Програма також забезпечує захист від крадіжок, пропонуючи функції віддаленого блокування та відстеження місцезнаходження пристрою, а також можливість видалення даних. Додатково Avast Mobile Security забезпечує безпеку веб-браузера, попереджаючи про небезпечні веб-сайти та фішингові атаки. Модуль антиспаму блокує небажані дзвінки та повідомлення, зменшуючи кількість спаму. Для підвищення продуктивності пристрою, програма містить інструменти для очищення пам'яті та видалення непотрібних файлів.

2. Bitdefender Mobile Security – це антивірусне програмне забезпечення, відоме своїм низьким впливом на продуктивність пристрою та високим рівнем захисту. Основні функції включають автопілот, який надає інтелектуальні рекомендації щодо покращення безпеки вашого пристрою. Програма забезпечує сканування на вимогу та в реальному часі для виявлення та видалення шкідливих програм. Антифішинг захищає від спроб крадіжки особистих даних через фальшиві веб-сайти. Захист приватності включає функцію App Lock, що дозволяє блокувати додатки за допомогою PIN-коду або відбитка пальця. Додатково, вбудований VPN забезпечує захист ваших даних під час користування незахищеними мережами Wi-Fi.

3. Kaspersky Mobile Security – потужне рішення з розширеними функціями захисту приватності та антивірусними можливостями. Основні функції включають сканування на вимогу та в реальному часі, яке виявляє та нейтралізує віруси та шкідливі програми. Програма також забезпечує захист веб-браузера, виявляючи фішингові сайти та блокуючи небезпечні URL. Захист від крадіжки включає можливість віддаленого блокування, очищення даних та відстеження пристрою. Антифішинг блокує спроби крадіжки особистих даних через підроблені веб-сайти. Функція App Lock дозволяє блокувати додатки за допомогою PIN-коду, відбитка пальця або розпізнавання обличчя.

4. Norton Mobile Security – це надійне антивірусне програмне забезпечення,

яке забезпечує захист від вірусів, фішингових атак та шкідливих додатків. Основні функції включають сканування в реальному часі, яке виявляє та видаляє шкідливі програми. Захист веб-браузера попереджає про небезпечні веб-сайти та блокує фішингові атаки. Антифішинг забезпечує захист від крадіжки особистих даних через підроблені веб-сайти. Захист від крадіжки включає віддалене блокування пристрою, видалення даних та відстеження місцезнаходження. Додатково, програма має функцію сигналу тривоги, яка дозволяє включити гучний сигнал для пошуку втраченого пристрою.

5. McAfee Mobile Security – це антивірусне програмне забезпечення, яке пропонує захист від вірусів, захист від крадіжок та функції збереження приватності. Основні функції включають сканування на вимогу та в реальному часі, яке виявляє та видаляє шкідливі програми. Захист від крадіжки включає віддалене блокування та очищення даних, відстеження місцезнаходження пристрою. Програма також забезпечує безпеку веб-браузера, захищаючи від фішингових сайтів та небезпечних URL. Антифішинг блокує спроби крадіжки особистих даних через фальшиві веб-сайти. Функція App Lock дозволяє блокувати додатки за допомогою PIN-коду або відбитка пальця. Додатково, програма має функцію безпеки Wi-Fi, яка аналізує безпеку мереж Wi-Fi та попереджає про небезпечні мережі [28].

Таки чином, антивірусне програмне забезпечення для мобільних пристроїв відіграє критичну роль у забезпеченні безпеки особистих даних та конфіденційності користувачів. Використання таких програм дозволяє ефективно захищати мобільні пристрої від численних кіберзагроз, таких як віруси, фішингові атаки, шкідливе програмне забезпечення та викрадення даних.

3.2. Браузери з підтримкою захищеного з’єднання (SSL/TLS)

Захищене з'єднання за допомогою протоколів SSL (Secure Sockets Layer) та TLS (Transport Layer Security) стало стандартом для забезпечення безпеки в Інтернеті. Ці протоколи використовуються для шифрування даних, що

передаються між браузером та сервером, забезпечуючи конфіденційність та цілісність інформації. Майже всі сучасні веб-браузери підтримують SSL/TLS, що робить їх важливим інструментом для безпечного серфінгу в Інтернеті. Найбільші популярні браузери, які підтримують захищені з'єднання:

Google Chrome – один з найпопулярніших браузерів, який підтримує SSL/TLS. Він автоматично використовує захищене з'єднання, коли це можливо, та попереджає користувача, якщо з'єднання не є безпечним. Chrome регулярно оновлює свої функції безпеки, включаючи підтримку новітніх версій TLS (рис. 3.1).

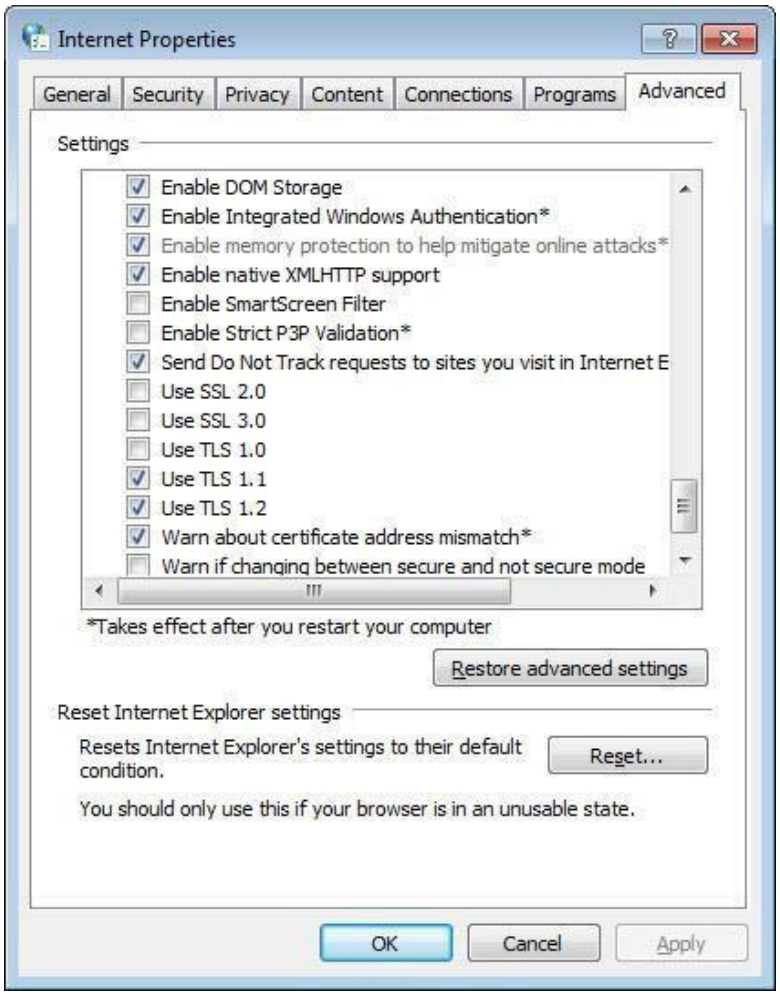

Рисунок 3.1 – TLS 1.1 і TLS 1.2 Google Chrome

Mozilla Firefox також підтримує SSL/TLS і надає користувачам потужні інструменти для забезпечення безпеки. Firefox автоматично використовує HTTPS, коли це можливо, і пропонує розширення HTTPS Everywhere, яке автоматично

встановлює з'єднання через HTTPS на сайтах, що підтримують цей протокол. Крім того, браузер надає детальну інформацію про безпеку з'єднання для кожного веб-сайту (рис. 3.2).

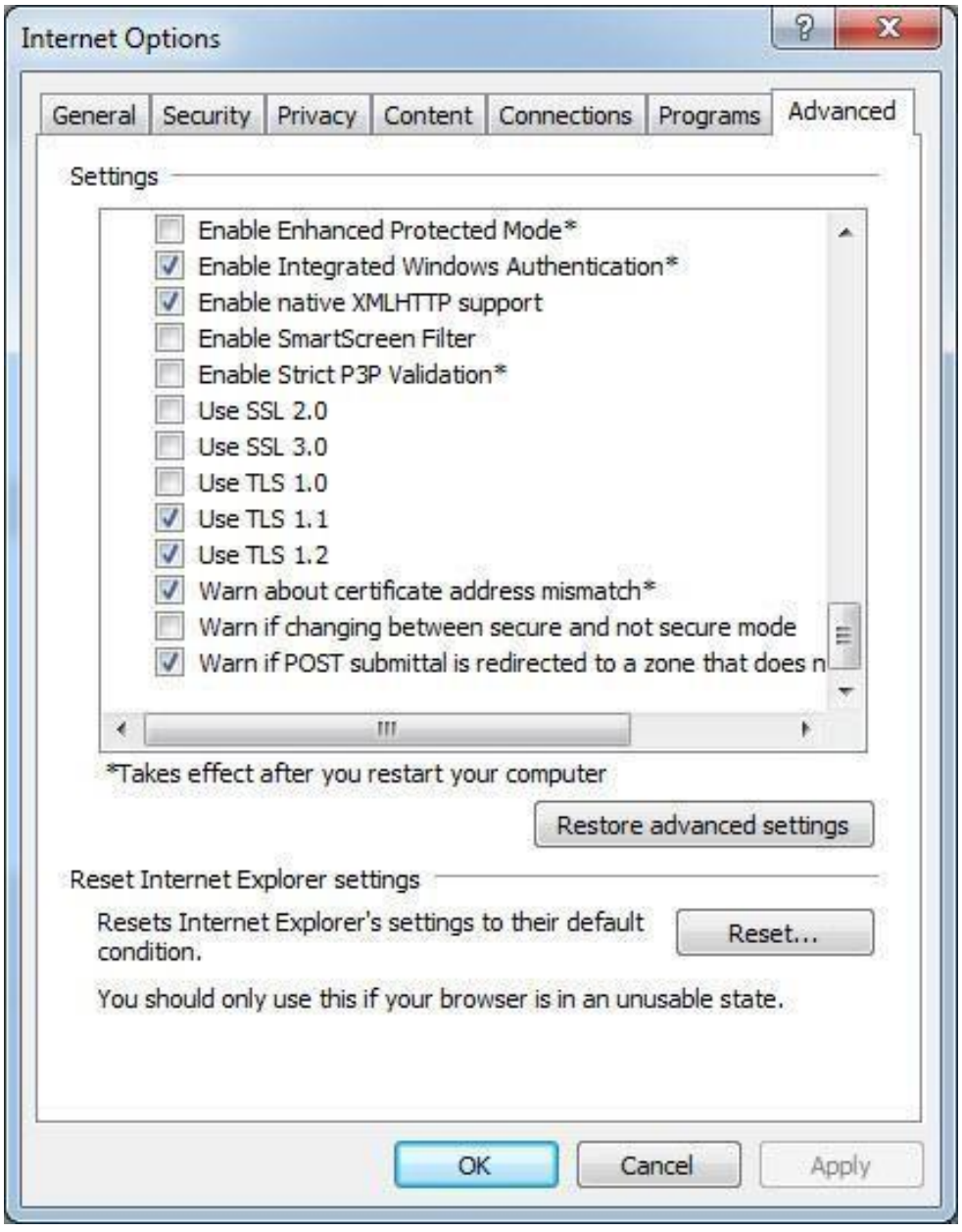

Рисунок 3.2 – TLS 1.1 та TLS 1.2 Mozilla Firefo

Microsoft Edge підтримує SSL/TLS та забезпечує високий рівень безпеки. Edge автоматично встановлює захищене з'єднання та попереджає користувача про можливі загрози. Браузер також підтримує функцію SmartScreen, яка блокує доступ до небезпечних веб-сайтів та фішингових сторінок (рис. 3.3).

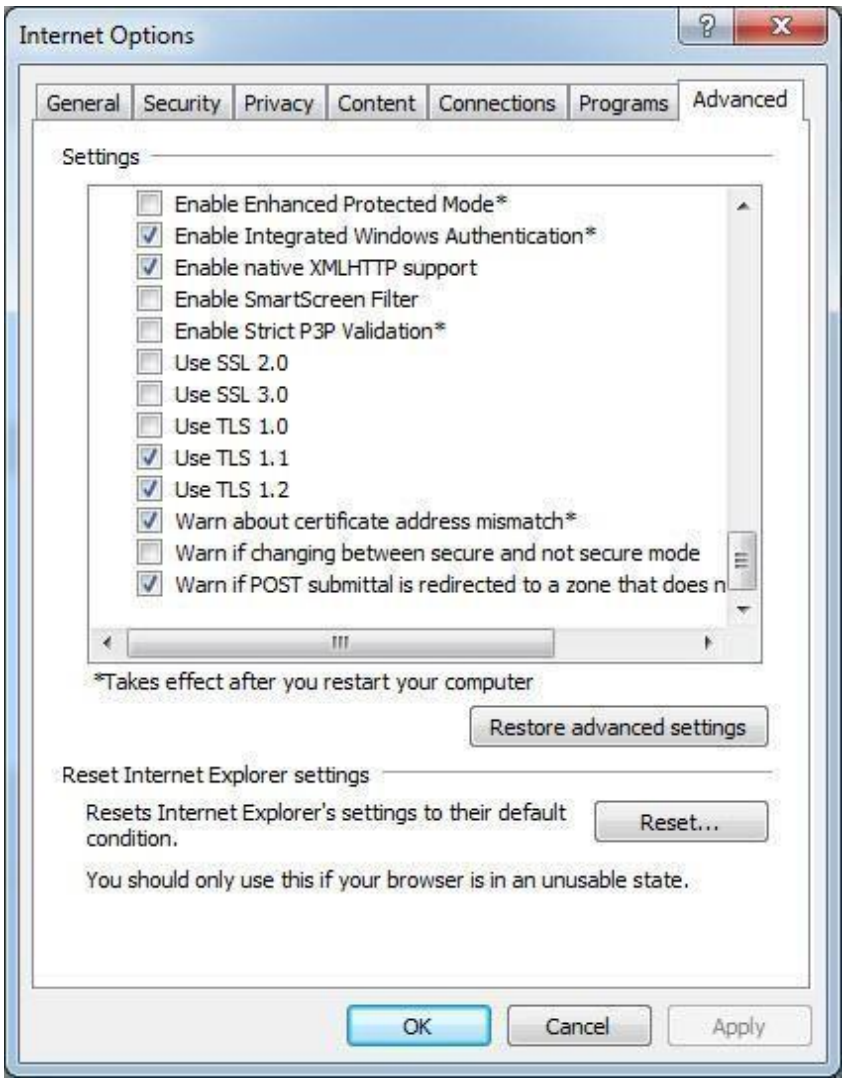

Рисунок 3.3 – TLS 1.1 та TLS 1.2 Microsoft Edge

Apple Safari автоматично використовує захищене з'єднання на всіх веб-сайтах, що підтримують HTTPS. Safari надає користувачам можливість переглядати детальну інформацію про сертифікат безпеки для кожного веб-сайту, а також має вбудовані функції для захисту від фішингу та інших загроз. Параметри для включення протоколів SSL відсутні. Якщо ви використовуєте Safari версії 7 або новішої, TLS 1.1 і TLS 1.2 вмикаються автоматично [29, с.75].

Opera також підтримує SSL/TLS і забезпечує захищене з'єднання. Браузер автоматично використовує HTTPS, коли це можливо, і має вбудований VPN для додаткового рівня захисту. Opera також включає функції блокування реклами та трекерів, що підвищує загальний рівень безпеки та конфіденційності (рис. 3.4).

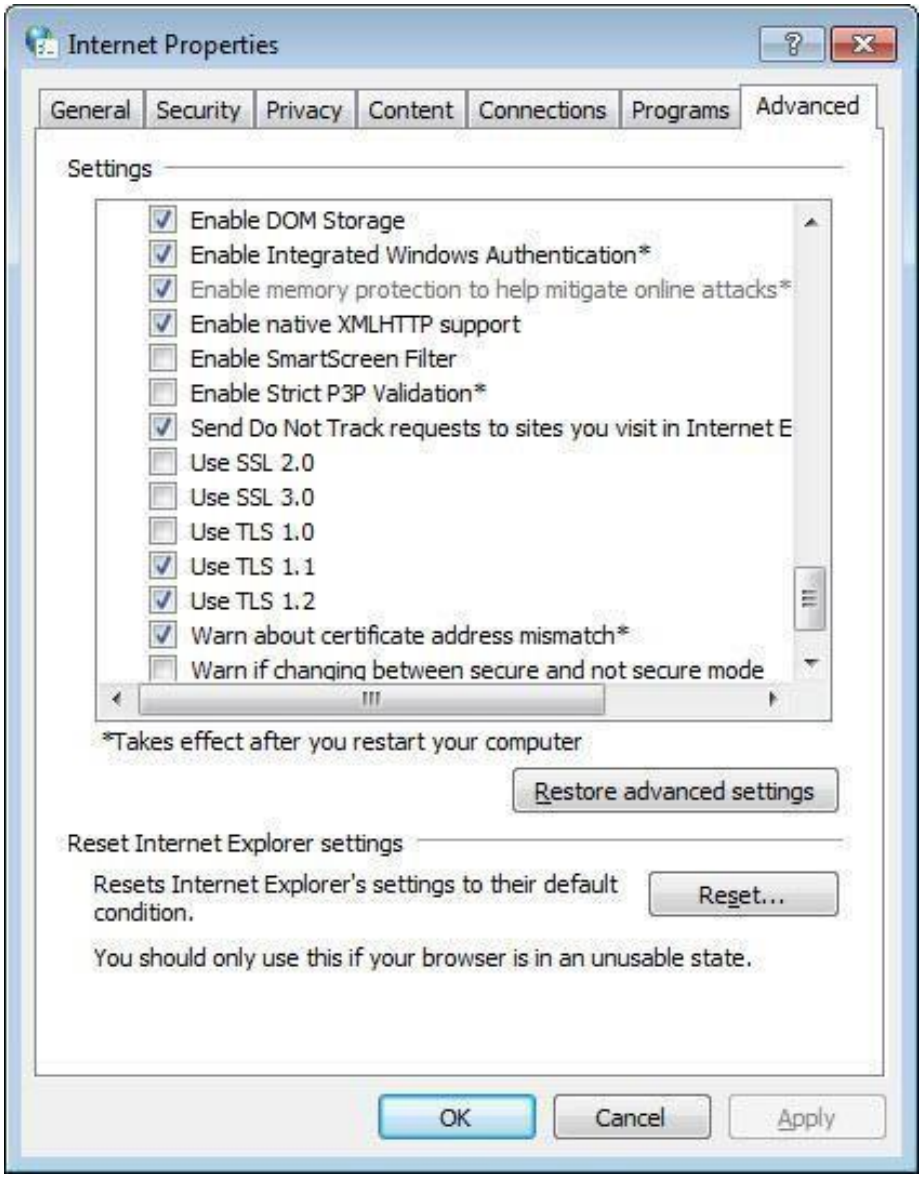

Рисунок 3.4 – TLS 1.1 та TLS 1.2 Opera

Vivaldi – це браузер, орієнтований на користувачів, які цінують приватність та безпеку. Він підтримує SSL/TLS і автоматично встановлює захищене з'єднання. Vivaldi також надає інструменти для блокування трекерів і реклами, що допомагає захистити конфіденційність користувачів.

Brave – браузер, який зосереджується на безпеці та конфіденційності користувачів. Він підтримує SSL/TLS та автоматично встановлює HTTPS-з'єднання на всіх можливих сайтах за допомогою вбудованої функції HTTPS Everywhere. Brave також блокує трекери та рекламу, що робить його одним із найбільш безпечних браузерів.

Тому, використання браузерів з підтримкою SSL/TLS є критично важливим

для забезпечення безпеки в Інтернеті. Ці браузери не тільки забезпечують шифрування даних, але й надають додаткові інструменти для захисту від фішингових атак, шкідливих сайтів та трекерів. Вибір надійного браузера допоможе користувачам зберегти свої дані в безпеці та забезпечити конфіденційність під час серфінгу в Інтернеті.

3.3. Віртуальна приватна мережа

Віртуальна приватна мережа (VPN) – це технологія, яка забезпечує безпечне і приватне з'єднання до Інтернету шляхом створення захищеного тунелю між вашим пристроєм і сервером VPN. Це дозволяє приховувати вашу IP-адресу, шифрувати ваші дані та захищати ваше інтернет-з'єднання від стороннього втручання. Використання VPN має багато переваг, особливо в сучасному цифровому світі, де приватність і безпека стали нагальними питаннями.

Основні функції VPN включають:

1. Шифрування даних. VPN використовує потужні методи шифрування, щоб захистити ваші дані від перехоплення третіми сторонами. Це особливо важливо при використанні публічних Wi-Fi мереж, де ризик втрати даних значно вищий.

2. Приховування IP-адреси. VPN дозволяє приховати вашу реальну IP-адресу, замінюючи її на IP-адресу сервера VPN. Це допомагає зберегти анонімність в Інтернеті і ускладнює відстеження вашої онлайн-активності.

3. Доступ до заблокованого контенту. VPN може обходити географічні обмеження і отримувати доступ до контенту, який може бути заблокований у вашому регіоні. Це особливо корисно для доступу до стрімінгових сервісів, соціальних мереж та інших веб-ресурсів.

4. Захист від цензури. У країнах з жорсткою інтернет-цензурою VPN може допомогти обійти обмеження та отримати доступ до вільного Інтернету.

5. Безпечне обмін даними. VPN забезпечує безпеку даних під час передачі між різними офісами компанії або між віддаленими співробітниками, що робить його важливим інструментом для бізнесу.

Популярні VPN-сервіси включають:

1. ExpressVPN – це один з найпопулярніших VPN-сервісів, відомий своєю високою швидкістю, надійністю та безпекою. Він має більше 3000 серверів у 94 країнах, що забезпечує широкий вибір для користувачів. ExpressVPN використовує 256-бітове шифрування і підтримує протоколи OpenVPN, IKEv2 та L2TP/IPsec. Додаткові функції включають захист від витоків DNS, розділене тунелювання та функцію автоматичного відключення (kill switch).

2. NordVPN відомий своїм високим рівнем безпеки і великою кількістю серверів (понад 5400 у 59 країнах). Він використовує подвійне шифрування для додаткового захисту даних і підтримує протоколи OpenVPN та IKEv2/IPsec. NordVPN також пропонує функції, такі як CyberSec для блокування шкідливих сайтів і рекламних оголошень, і функцію Onion over VPN для додаткової анонімності.

3. CyberGhost пропонує простий у використанні інтерфейс і високий рівень безпеки. Він має більше 7000 серверів у 90 країнах і використовує 256-бітове шифрування. CyberGhost підтримує протоколи OpenVPN, IKEv2 та WireGuard. Додаткові функції включають блокування реклами, захист від трекерів і автоматичне перемикання на HTTPS [30, с.32].

Тому, VPN є важливим інструментом для забезпечення безпеки та конфіденційності в Інтернеті. Вони захищають ваші дані від перехоплення, приховують вашу IP-адресу та дозволяють обійти географічні обмеження. Вибір надійного VPN-сервісу залежить від ваших потреб та вимог щодо безпеки, швидкості та функціональності. Використовуючи VPN, ви можете бути впевнені, що ваші онлайн-дії залишаться приватними та захищеними.

3.4. Перевірка рейтингів та відгуків про сервіси

Перевірка рейтингів та відгуків про сервіси є критично важливою для ефективного вибору засобів захисту мобільних пристроїв. Цей процес сприяє виявленню надійних програмних рішень, які допоможуть мінімізувати ризики

вразливості та атак на пристрої. Оцінка рейтингів і відгуків дозволяє користувачам отримати об'єктивну інформацію про якість та ефективність захисних програм.

Високий рейтинг та позитивні відгуки свідчать про ефективність та надійність засобу захисту. Вони підтверджують, що програма здатна ефективно виявляти та блокувати загрози, забезпечуючи високий рівень безпеки для мобільного пристрою. Перевірка відгуків також допомагає виявити можливі недоліки чи недоліки програми, що дозволяє користувачам уникнути встановлення недостатньо ефективного захисту.

Оцінка функціональності та продуктивності засобу захисту також є важливим аспектом. Користувачам важливо мати засіб, який не лише забезпечує безпеку, але й має мінімальний вплив на продуктивність пристрою та не викликає перешкод у роботі з іншими програмами.

Оновлення та актуальність програмного забезпечення є також важливими. Регулярні виправлення помилок та оновлення баз даних загроз допомагають підтримувати високий рівень захисту пристрою від нових та еволюціонуючих загроз. Співпраця з підтримкою є ще одним аспектом, який варто враховувати при виборі засобу захисту. Якісна підтримка допоможе швидко та ефективно вирішувати будь-які проблеми, що виникають у процесі використання програми.

Отже, перевірка рейтингів та відгуків про сервіси є необхідним етапом у процесі вибору засобу захисту мобільних пристроїв, що дозволяє користувачам забезпечити ефективний та надійний рівень безпеки своїх даних та пристроїв.

3.5. Функція «псевдонімізації» для приховування точного місцезнаходження

Функція «псевдонімізації» є ефективним засобом для забезпечення приватності та конфіденційності мобільних пристроїв, призначеним для приховування точного місцезнаходження користувача. Функція працює шляхом заміни реальних географічних даних на випадкові або загальні дані, що утруднює визначення точного місця знаходження користувача третіми особами.

Застосування функції «псевдонімізації» дозволяє користувачам залишати сліди своєї активності в інтернеті чи в мобільних додатках, не розкриваючи свою реальну географічну прив'язку. Особливо корисно в сферах, де приватність є важливою, таких як мобільний маркетинг, аналітика розташування та інші додатки, які використовують геолокаційні дані.

Тим не менш, важливо враховувати, що функція «псевдонімізації» може зменшити точність та корисність деяких мобільних додатків, які використовують геолокаційні дані для надання персоналізованих послуг. Також, вона не завжди може забезпечити абсолютну анонімність, особливо при комплексному аналізі додаткових даних.

Простий код на мові Python для генерації псевдонімів для приховування точного місцезнаходження виглядає наступним чином:

```
def generate_pseudonym(latitude, longitude):
    # Генеруємо випадкові зміщення для координат
    offset_lat = random.uniform(-0.5, 0.5) # Випадкове зміщення для широти
    offset_long = random.uniform(-0.5, 0.5)  # Випадкове зміщення для довготи
    # Застосовуємо зміщення до вхідних координат
    pseudonym_lat = latitude + offset_lat
    pseudonym_long = longitude + offset_long
    return pseudonym_lat, pseudonym_long
# Приклад використання
latitude = 48.858844
longitude = 2.294351
pseudonym_lat, pseudonym_long = generate_pseudonym(latitude, longitude)
print("Псевдонім широти:", pseudonym_lat)
print("Псевдонім довготи:", pseudonym_long)
```

Отже, функція «псевдонімізації» становить важливий елемент у забезпеченні приватності та безпеки користувачів мобільних пристроїв, проте вона потребує уважного розгляду в контексті конкретного застосування з урахуванням його потреб та ризиків.

3.6. Шифрування для захисту конфіденційної інформації на пристрої

Шифрування для захисту конфіденційної інформації на пристрої – це процес перетворення звичайного тексту або даних у нечитабельний формат за допомогою спеціальних алгоритмів шифрування. Основна мета полягає в тому, щоб зробити інформацію недоступною для несанкціонованих осіб, які можуть намагатися отримати доступ до неї. Шифрування забезпечує безпеку даних на пристрої шляхом перетворення їх у формат, який може бути розшифрований лише з допомогою правильного ключа або пароля.

Сьогодні широко використовуються два типи шифрування: симетричне та асиметричне шифрування.

Симетричне шифрування. При симетричному шифруванні для шифрування і дешифрування використовується один і той же ключ. Тому вкрай важливо, щоб для передачі ключа між відправником і одержувачем використовувався безпечний метод.

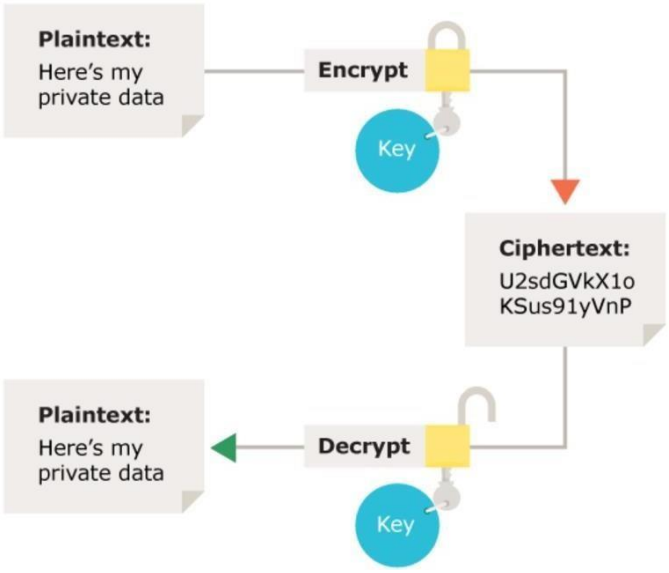

Рисунок 3.5 – Симетричне шифрування – використання одного і того ж ключа для шифрування та дешифрування

В асиметричному шифруванні використовується поняття пари ключів: для процесу шифрування і дешифрування використовується інший ключ. Один із

ключів зазвичай називають приватним, а інший – відкритим.

Власник зберігає приватний ключ у таємниці, а відкритий ключ або передається авторизованим одержувачам, або стає загальнодоступним. Дані, зашифровані за допомогою відкритого ключа одержувача, можуть бути розшифровані тільки за допомогою відповідного закритого ключа. Таким чином, передача даних може здійснюватися без ризику несанкціонованого або незаконного доступу до них.

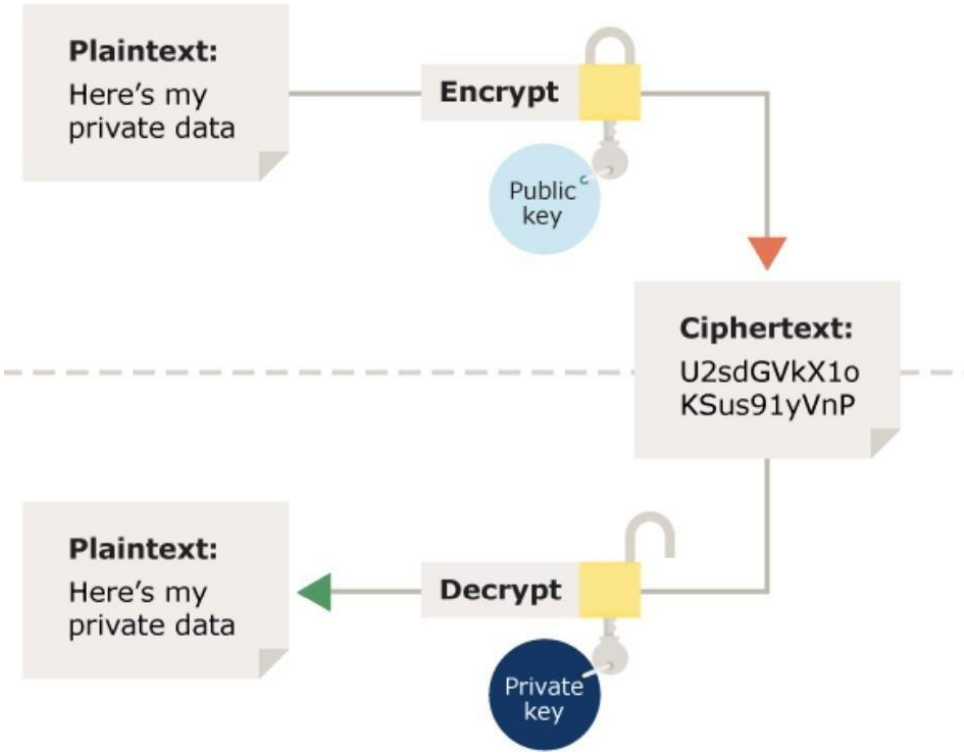

Рисунок 3.6 – Асиметричне шифрування – використання іншого ключа для процесу шифрування та дешифрування

Таке використання також може гарантувати ідентифікацію відправника або одержувача повідомлення. Для цього використовується процес, який називається цифровим підписом. Повідомлення, підписане приватним ключем відправника, може бути перевірено одержувачем за допомогою відповідного відкритого ключа. Сертифікати для підпису повідомлень також можуть видаватися довіреними третіми сторонами (наприклад, центрами сертифікації), які можуть забезпечити

додаткову впевненість в тому, що власник певної пари ключів є тим, за кого себе видає.

До прикладів використання шифрування можна віднести:

– шифрування дисків. Інструменти, такі як BitLocker (Windows) або FileVault (macOS), шифрують весь диск, забезпечуючи захист всіх даних на ньому;

– шифрування файлів і папок. Програми, такі як VeraCrypt або AxCrypt, дозволяють шифрувати окремі файли або папки;

– шифрування даних в мережі. Використання протоколів HTTPS, TLS/SSL для забезпечення безпеки даних, що передаються через інтернет [31, с.43].

Шифрування є ключовим заходом для захисту конфіденційної інформації на пристроях. Воно забезпечує безпеку даних, захищаючи їх від несанкціонованого доступу навіть у разі фізичної втрати пристрою або кібератаки. Впровадження шифрування є необхідним для виконання стандартів безпеки та збереження конфіденційності даних у сучасному цифровому світі.

3.7. Моніторінг активності додатків

Моніторинг активності додатків є важливим компонентом для забезпечення безпеки та оптимальної роботи мобільних пристроїв і комп'ютерів. Цей процес передбачає постійне відстеження та аналіз поведінки програмного забезпечення з метою виявлення потенційних загроз та аномалій. Ось ключові аспекти моніторингу активності додатків:

1. Виявлення шкідливого програмного забезпечення. Моніторинг допомагає виявляти та блокувати шкідливі додатки, які можуть становити загрозу для безпеки пристрою чи особистої інформації користувача. Це включає виявлення вірусів, троянів, шпигунських програм та інших видів зловмисного ПЗ.

2. Спостереження за системними ресурсами. Моніторинг дозволяє відслідковувати використання системних ресурсів, таких як процесор, пам'ять, дисковий простір та мережевий трафік. Це допомагає виявити додатки, які споживають надмірно багато ресурсів, що може свідчити про їх неефективність або

потенційну небезпеку.

3. Аналіз мережевої активності. Моніторинг мережевої активності дозволяє виявляти додатки, які здійснюють підозрілу мережеву активність, наприклад, надсилають або отримують великі обсяги даних без відома користувача. Це може бути ознакою витоку інформації або зловмисних дій.

4. Оновлення та вразливості. Моніторинг активності додатків включає виявлення програм, які потребують оновлення. Своєчасне оновлення додатків важливе для закриття виявлених вразливостей, що можуть бути використані для атак.

5. Аудит дозволів. Моніторинг дозволів, які надаються додаткам, допомагає впевнитись, що програми не мають надмірних прав доступу, які можуть бути зловживані. Це включає перевірку доступу до мікрофона, камери, контактів та інших конфіденційних даних.

До програм моніторингу активності додатків зараховано:

1. Antivirus та антималварні програми. Такі як Avast, Bitdefender, Kaspersky, які мають вбудовані функції моніторингу активності.

2. Системні монітори. Програми типу Activity Monitor (macOS) або Task Manager (Windows) дозволяють відслідковувати використання ресурсів та активність додатків.

3. Спеціалізовані інструменти. Програми на зразок Little Snitch (macOS) для моніторингу мережевої активності або GlassWire (Windows) для відслідковування мережевого трафіку.

Моніторинг активності додатків є необхідним для забезпечення безпеки та ефективної роботи мобільних і комп'ютерних пристроїв. Він допомагає вчасно виявляти потенційні загрози, контролювати використання ресурсів та захищати конфіденційну інформацію. Використання сучасних інструментів для моніторингу забезпечує надійний захист від різноманітних загроз та підтримує оптимальну роботу пристроїв.

3.8. Використання двофакторної аутентифікації для забезпечення додаткового рівня захисту

Двофакторна аутентифікація (2FA) – це функція, яка вимагає від користувача представити два різні типи ідентифікаційних даних, перш ніж йому буде дозволено доступ до облікового запису. Це ключовий підхід для підвищення безпеки ваших облікових записів. Цей метод захисту включає те, що відомо користувачеві, і те, до чого він має доступ. Двофакторна аутентифікація забезпечує другий рівень захисту онлайн-акаунтів користувача, крім пароля користувача. За допомогою 2FA користувач входить в онлайн-акаунт, але замість того, щоб отримати негайний доступ, він повинен надати додаткову інформацію, таку як особистий ідентифікаційний номер (PIN-код), одноразовий код підтвердження, відповіді на запитання, відомі лише користувачеві тощо. У деяких випадках 2FA надсилає текстове повідомлення на мобільний телефон користувача.

Основні типи двофакторної аутентифікації:

– токени на основі SMS. Після введення паролю користувач отримує одноразовий код через SMS, який необхідно ввести для підтвердження своєї особи. Хоча цей метод широко використовується, він має вразливості, зокрема можливість атак на мобільні мережі;

– аутентифікаційні додатки. Додатки, такі як Google Authenticator, Authy або Microsoft Authenticator, генерують одноразові коди на пристрої користувача, які оновлюються кожні 30 секунд і не потребують підключення до Інтернету для їх генерації;

– апаратні токени. Спеціалізовані пристрої, такі як YubiKey, генерують одноразові коди або підключаються до комп'ютера через USB для аутентифікації. Вони забезпечують високий рівень безпеки, хоча можуть бути менш зручними для деяких користувачів через необхідність постійного носіння пристрою;

– біометричні методи. Використання біометричних даних, таких як відбитки пальців або розпізнавання обличчя, для додаткової аутентифікації забезпечує зручність і високий рівень безпеки.

Незважаючи на певну незручність, пов'язану з подовженням процесу автентифікації, експерти з безпеки настійно рекомендують впроваджувати двофакторну аутентифікацію (2FA) скрізь, де це можливо, і використовувати її для захисту облікових записів електронної пошти, менеджерів паролів, додатків соціальних мереж, хмарних сховищ даних та фінансових сервісів. Тому варто враховувати ці рекомендації під час створення нових облікових записів або удосконалення заходів безпеки для вже існуючих.

Двофакторна аутентифікація стала невід'ємною складовою для захисту різноманітних цифрових ресурсів, включаючи інтернет-банкінг, хмарні служби зберігання даних, роботу та бізнес і навіть крипто-гаманці. У сфері інтернет-банкінгу, 2FA використовується для захисту фінансових транзакцій та особистих облікових записів, а методи аутентифікації можуть включати SMS-коди, аутентифікаційні додатки або біометричні дані. Хмарні служби зберігання даних також вимагають додаткових заходів безпеки, і 2FA використовується для забезпечення захисту від несанкціонованого доступу до конфіденційних інформаційних ресурсів. У сфері роботи та бізнесу, 2FA забезпечує додатковий рівень захисту для корпоративних систем, електронної пошти та конфіденційних даних, і методи включають аппаратні токени, аутентифікаційні додатки та біометричні дані. Нарешті, у сфері крипто-гаманців, 2FA є критично важливим для захисту від кібератак та втрати цифрових активів, і методи включають аутентифікаційні додатки, аппаратні гаманці та SMS-коди. Загалом, впровадження 2FA є кроком у забезпеченні безпеки в онлайн-світі та захисту конфіденційних даних користувачів.

Популярні програми для 2FA включають Google Authenticator, Authy, Microsoft Authenticator та LastPass Authenticator. Вони надійно захищають онлайн-акаунти користувачів, забезпечуючи додатковий шар безпеки і запобігаючи несанкціонованому доступу до особистої інформації.

Приклад коду на мові Python для реалізації двофакторної аутентифікації за допомогою генерації одноразових кодів з використанням бібліотеки PyOTP:

```
import pyotp
```

```
# Генеруємо секретний ключ для користувача
secret_key = pyotp.random_base32()
# Створюємо об'єкт для генерації TOTP (Time-based One-Time Password)
totp = pyotp.TOTP(secret_key)
# Виводимо секретний ключ для користувача
print("Секретний ключ для 2FA:", secret_key)
# Генеруємо та виводимо перший одноразовий код
first_code = totp.now()
print("Перший одноразовий код:", first_code)
# Перевіряємо введений користувачем код
user_code = input("Введіть одноразовий код для перевірки: ")
if totp.verify(user_code):
    print("Код правильний. Доступ надано.")
else:
print("Код неправильний. Доступ заборонено.")
```

Код створює новий секретний ключ для користувача, генерує і виводить перший одноразовий код, а потім перевіряє, чи відповідає введений користувачем код встановленому ключу.

В цілому, використання двофакторної аутентифікації є важливим елементом забезпечення безпеки в онлайн-середовищі і допомагає ефективно захищати конфіденційні дані користувачів від потенційних загроз. Використання двофакторної аутентифікації ускладнює завдання для потенційних зловмисників, які намагаються отримати доступ до облікових записів користувачів шляхом перехоплення паролів.

Висновки по розділу 3

Антивірусне програмне забезпечення є основою безпеки мобільних пристроїв, забезпечуючи захист від шкідливих програм і загроз в Інтернеті. Браузери, які підтримують захищене з’єднання за допомогою протоколів SSL/TLS,

забезпечують безпечніше переглядання веб-сторінок і передачу даних. Віртуальна приватна мережа (VPN) додає додатковий рівень конфіденційності, шифруючи з’єднання і приховуючи реальну IP-адресу користувача. Перевірка рейтингів та відгуків про сервіси допомагає користувачам обирати надійні програми та послуги для своїх пристроїв. Функція «псевдонімізації» для приховування точного місцезнаходження забезпечує більшу приватність при використанні мобільних додатків та послуг, залишаючи користувача в безпеці від стеження. Шифрування даних на пристрої захищає конфіденційну інформацію від несанкціонованого доступу. Моніторинг активності додатків допомагає виявляти та запобігати небажаним діям програм, які можуть загрожувати безпеці пристрою. Використання двофакторної аутентифікації забезпечує додатковий рівень захисту, вимагаючи від користувачів підтвердження своєї ідентичності двома різними методами. Разом ці заходи створюють комплексний підхід до захисту мобільних пристроїв і забезпечують безпеку даних та конфіденційність користувачів в онлайн-середовищі.

ВИСНОВКИ

Операційні системи мобільних пристроїв представляють собою спеціалізовані платформи, призначені для управління смартфонами, планшетами та іншими мобільними пристроями. Вони поєднують у собі функції та властивості операційних систем для ПК з можливостями, специфічними для мобільних і кишенькових пристроїв. Серед основних характеристик мобільних операційних систем можна виділити підтримку сенсорного екрану, стільникового зв'язку, Bluetooth, Wi-Fi, GPS-навігації, камер, розпізнавання мови, диктофону, музичного плеєра, NFC та інфрачервоного дистанційного керування. Сьогодні на ринку представлено декілька популярних мобільних операційних систем, серед яких Android, iOS та Windows Mobile займають провідні позиції. Ці операційні системи визначають функціональні можливості та продуктивність мобільних пристроїв, забезпечуючи користувачам широкий спектр послуг та інструментів для виконання різноманітних завдань.

Залежно від ролі для власника, мобільні застосунки можуть бути корпоративними або комерційними. Корпоративні застосунки автоматизують бізнес-процеси підприємств, надаючи доступ до оперативної інформації, здійснюючи господарські операції та управління підприємством. Комерційні застосунки виступають як товар і призначені для реалізації на ринку за допомогою різних моделей монетизації.

З точки зору функціональності, мобільні застосунки поділяються на такі категорії: розваги, подорожі, бізнес, соціальні додатки, їжа, спорт, освіта та новини. Кожна категорія забезпечує певні специфічні функції для користувачів, такі як замовлення квитків, фінансове планування, соціальні мережі, замовлення їжі, спортивні новини та навчальні програми.

За технологією розробки, мобільні застосунки поділяються на нативні, кросплатформні та гібридні. Нативні застосунки створюються під конкретну операційну систему і встановлюються безпосередньо на пристрій користувача. Кросплатформні застосунки розробляються як веб-додатки, що не потребують

встановлення на пристрій. Гібридні застосунки комбінують елементи нативних і кросплатформних застосунків.

Апаратна частина мобільних пристроїв складається з ключових компонентів, кожен з яких виконує важливі функції для забезпечення продуктивності та функціональності пристрою. Центральний процесор (ЦП) є серцем пристрою, виконуючи основні обчислювальні завдання. Оперативна пам'ять (ОЗП або RAM) забезпечує швидкий доступ до даних та програм під час їх роботи. Внутрішня пам'ять служить для зберігання операційної системи, додатків та користувацьких даних. Дисплей є основним засобом взаємодії користувача з пристроєм, а батарея забезпечує автономну роботу пристрою. Камери дозволяють знімати фото та відео, що є важливою функцією для багатьох користувачів. Система підтримки мереж забезпечує підключення до мобільних мереж для здійснення дзвінків і передачі даних. Датчики, такі як акселерометри та гіроскопи, покращують функціональність та взаємодію з користувачем, дозволяючи визначати положення пристрою в просторі. Роз'єми, такі як USB-порти, забезпечують підключення до інших пристроїв та зарядку. Бездротові інтерфейси, такі як Wi-Fi, Bluetooth та NFC, дозволяють обмін даними та підключення до інших пристроїв без використання кабелів.

Серед основних інструментів, які забезпечують високу якість та ефективність розробки мобільних додатків, виділяються Android Studio, Xcode, Visual Studio, Flutter, React Native та AppCode.

Типи загроз для мобільних пристроїв охоплюють широкий спектр ризиків, які можуть вплинути на безпеку та конфіденційність користувацьких даних. Програмні загрози включають шкідливе програмне забезпечення, віруси та трояни, які можуть проникати в систему через різні канали. Web-загрози пов'язані з небезпечними вебсайтами та фішинговими атаками, що намагаються отримати конфіденційну інформацію. Мережеві загрози стосуються атак на мережеву інфраструктуру, таких як перехоплення даних через незахищені Wi-Fi з’єднання.

З’єднання з недовіреним сервісом може призвести до витоку даних або компрометації пристрою. Використання GPS та функцій місцезнаходження несе

ризики відстеження та небажаного доступу до даних про місцезнаходження. Небезпечне зберігання даних пов'язане з недостатньо захищеними файлами та базами даних на пристрої, що може призвести до їх втрати або крадіжки. Ненавмисний витік даних може статися через недбале поводження з пристроєм або недостатньо захищені програми.

Проблеми авторизації та аутентифікації включають слабкі паролі та недостатні методи аутентифікації, що робить пристрої вразливими до несанкціонованого доступу. Таким чином, розуміння та управління цими загрозами є критично важливими для забезпечення безпеки мобільних пристроїв та захисту особистих даних користувачів.

Засоби захисту мобільних пристроїв охоплюють широкий спектр інструментів та методів, які спрямовані на забезпечення безпеки користувацьких даних та захист від різноманітних загроз. Антивірусне програмне забезпечення є основним засобом боротьби зі шкідливими програмами, забезпечуючи постійний захист від вірусів та інших шкідливих кодів. Браузери з підтримкою захищеного з’єднання (SSL/TLS) гарантують безпечну передачу даних через Інтернет, запобігаючи перехопленню конфіденційної інформації.

Віртуальна приватна мережа (VPN) забезпечує анонімність та безпеку під час доступу до мережі, приховуючи справжнє місцезнаходження користувача та захищаючи дані від стороннього втручання. Перевірка рейтингів та відгуків про сервіси допомагає користувачам обирати надійні додатки та сервіси, зменшуючи ризик встановлення шкідливого або низькоякісного програмного забезпечення. Функція «псевдонімізації» дозволяє приховувати точне місцезнаходження користувача, забезпечуючи додатковий рівень конфіденційності.

Шифрування для захисту конфіденційної інформації на пристрої є ефективним засобом запобігання несанкціонованому доступу до даних, навіть у випадку втрати або крадіжки пристрою. Моніторінг активності додатків дозволяє виявляти підозрілу активність та своєчасно реагувати на потенційні загрози. Використання двофакторної аутентифікації додає ще один рівень захисту, роблячи доступ до пристрою або облікових записів значно складнішим для зловмисників.

Отже, комплексне використання цих засобів захисту дозволяє ефективно захищати мобільні пристрої від широкого спектра загроз, забезпечуючи безпеку та конфіденційність користувацьких даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mobile Phone Market Forecast – 2019 [Електронний ресурс] – Режим доступу: https://stats.areppim.com/stats/stats_mobilex2019.htm

2. Аналіз безпеки мобільних пристроїв: підсумки першого півріччя 2019 [Електронний ресурс] – Режим доступу: https://eset.ua/ua/news/ view/ 717/analiz-bezopasnosti-mobilnykh-ustroystv-itogi-pervogo-polugodiya2019

3. Захист корпоративної інформації від витоку через мобільні пристрої [Електронний ресурс] – Режим доступу: https://licenziya-fsb.com/ utechka-mobilnye-ustroistva

4. Афонін О. Android і шифрування даних. Про те як все погано, і навряд чи стане краще [Електронний ресурс] – Режим доступу: https:// xakep.ru/2016/05/02/android-encryption/

5. What is Mobile Device Management (MDM)? [Електронний ресурс] – Режим доступу: https://www.continuum.net/resources/mspedia/ everything-to-know-about-mobile-device-management-mdm

6. Bader S. What Is Data Loss Prevention and How Does It Work? [Електронний ресурс] / Sarah Bader // Rewind. 2022. Режим доступу: https://rewind.com/blog/data-loss-prevention/.

7. How Antivirus Works? [Електронний ресурс] // COMODO CYBERSECURITY. 2020. Режим доступу: https://antivirus.comodo.com/how-antivirus-software-works.php.

8. Нечволод К.В. Аналіз безпеки даних в ЕММ системах. Системи управління, навігації та зв'язку. Полтава: ПНТУ. 2019. Вип. 3(55). С. 131-134

9. Нечволод К.В. Аналіз безпеки даних на основі платформи Samsung Knox. Комп'ютерні та інформаційні системи і технології. Третя міжнародна науково-технічна конференція. Збірник наукових праць. Х: ХНУРЕ, 2019. С. 80-81.

10. Аносов А. О. Модель перехоплення та захисту інформації в бездротових мережах. Сучасний захист інформації. 2017. № 2(30). С. 90-94.

11. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту. Сучасний захист інформації. 2017. №1. С. 128–132.

12. Benjamin L.M. Privacy, computers and personal information: Towards equality and equity in an information age. Communications and the Law. 2017. 13 (2). P. 3-16.

13. Froehlich T.J. Re-thinking ethical issues in an online environment. / T.J. Froehlich // Online Information '17, edited by D.I. Raitt & B. Jeapes. Oxford: Learned Information. 2017. P. 415-422.

14. Neuburg M. iOS 13 Programming Fundamentals with Swift: Swift, Xcode, and Cocoa Basics. Matt Neuburg. O'Reilly Media, 2019. 680 с.

15. Weichbroth Paweł, Łysik Łukasz. Mobile Security: Threats and Best Practices. Mobile Information Systems. 2020. DOI: 10.1155/2020/8828078.

16. Luis Castro Silva, Samyr Vale. A Methodology for Network Security Infrastructure according to the New Brazilian General Law for Personal Data Protection. International Journal of Computer Applications. 2021. Vol 183. DOI: 10.5120/ijca2021921520

17. Ali Balapour, Hamid Reza Nikkhah, Rajiv Sabherwal. Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management. 2020. Vol. 52. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.102063

18. Бондар Г. Л. Інформаційна політика та інформаційна безпека. Публічне управління та митне адміністрування. 2019. Вип. 4. С. 42–49

19. Жилін А. В., Шаповал О. М., Успенський О. А.. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с

20. Komar M., Sachenko A., Bezobrazov S., Golovko V. Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques. Communications in Computer and Information Science. 2017. Vol. 783. Pp. 36-55.

21. Платоненко А. В. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. Сучасний захист інформації. Київ, 2017. No

1. С. 128–132.

22. Мобільна безпека: Захист мобільних пристроїв в корпоративній мережі. URL: https://xakep.ru/2011/10/13/57058

23. Куперштейн Л.М. Базно-орієнтований підхід до захисту даних в операційній системі Android. Науковий журналі «Вісник Хмельницького національного університету». Київ, 2018. С.51-62.

24. Axel Buecker, Per Andreas, Scott Paisley. Understanding IT Perimeter Security. https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf

25. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту. Сучасний захист інформації. 2017. № 1. С. 128-132.

26. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої. Інформаційна безпека таІнформаційні технології: збірник тез доповідей IV Всеукраїнської науково- практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД. 2020. С.121-124).

27. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

28. How to: Android file encryption. [Electronic resource]. Access to resources: https://www.sookasa.com/resources/Android-file-encryption/ – name from screen.

29. Оксенюк В.Ю. Використання програмних засобів для оцінки та управління ризиками інформаційної безпеки. Інформаційні моделі, системи та технології: Праці VII наук.-техн. конф. (Тернопіль, 11-12 грудня 2019 р.) Тернопіль, 2019. С. 75.

30. Sheppard D. Beginning Progressive Web App Development. – United States of America: Apress, 2017. 286 c.

31. Rob W. Developing Inclusive Mobile Apps: Building AccessibleApps for iOS and Android.–United States of America: Apress, 2020. 359c.

UNICHECK
by Turnitin

Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки...

ID перевірки:
1016357007

Дата перевірки:
13.06.2024 15:11:36 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.06.2024 16:55:55 EEST

ID користувача:
100005746

Назва документа: Диплом_Маргушко

Кількість сторінок: 75 Кількість слів: 16174 Кількість символів: 127033 Розмір файлу: 537.54 KB ID файлу: 1016161268

5.94%
Схожість

Найбільша схожість: 0.48% з Інтернет-джерелом (https://cqr.company/web-vulnerabilities/insecure-data-storage-in-mo...

3.86% Джерела з Інтернету 108 ..... Сторінка 77

3.92% Джерела з Бібліотеки 348 ..... Сторінка 79

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел