Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Засоби та механізми захисту інформаційних ресурсів та додатків мобільних пристроїв»

Виконавець: студент IV курсу, групи КБ-42

_____ **Кіт Ілля Сергійович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Пархоменко І.І.	

Нормоконтроль	Зюбіна Р.В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** (група) **Кіту Іллі Сергійовичу** (прізвище ім'я по-батькові)

Тема дипломної роботи Засоби та механізми захисту інформаційних ресурсів та додатків мобільних пристроїв

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Структури, архітектури, засоби функціонування мобільних додатків, стек інструментів для розробки мобільних додатків та алгоритми їх захисту

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Апаратна частина мобільних пристроїв, основні ОС мобільних пристроїв, інструменти розробки додатків, нормативно-правова база ,персональні данні в мобільних додатках, загрози мобільному банкінгу, соціальний фактор як вразливість, захист в ОС Android/IOS, рекомендації розробникам додатків

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Поєднання механізмів захисту мобільних пристроїв та формування рекомендацій щодо їх впровадження.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав		І.І. Пархоменко
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання		І.С. Кіт
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 27.01.2021	*виконано*
2	Аналіз літератури	28.01.2021 – 11.02.2021	*виконано*
3	Дослідження ОС мобільних пристроїв та засобів розробки додатків	12.02.2021 – 24.02.2021	*виконано*
4	Дослідження нормативно-правової бази	25.02.2021 – 24.03.2021	*виконано*
5	Дослідження вразливостей та загроз	25.03.2021 – 07.04.2021	*виконано*
6	Дослідження методів та механізмів захисту	08.04.2021 – 20.04.2021	*виконано*
7	Формування рекомендацій щодо захисту мобільних пристроїв та додатків	21.04.2021 – 05.05.2021	*виконано*
8	Формування рекомендацій щодо використання антивірусного забезпечення	05.05.2021 – 04.06.2021	*виконано*
9	Оформлення пояснювальної записки	05.06.2021 – 08.06.2021	*виконано*
10	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Завдання видав		І.І. Пархоменко
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання		І.С. Кіт
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, 4 розділів, загальних висновків, списку використаних джерел, додатків, має 62 сторінки основного тексту та 1 таблиці. Список використаних джерел містить 23 найменування і займає 2 сторінки.

Метою даної роботи є дослідження засобів та механізмів захисту інформаційних ресурсів та додатків мобільних пристроїв.

У роботі проаналізована існуюча література з захисту мобільних пристроїв, розроблено рекомендації з захисту персональних даних при використані мобільних пристроїв.

Розроблені рекомендації призначені для користувачів, що хочуть забезпечити безпеку своїх персональних даних в мобільних пристроях.

Ключові слова: захист персональних даних, мобільні пристрої, безпека в мобільних додатках, мобільний банкінг, операційна система, політика BYOD, соціальний фактор, антивірусне програмне забезпечення.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard
API	–	Application Programming Interface
BYOD	–	Bring Your Own Device
CVE	–	Common Vulnerabilities and Exposures
ENISA	–	The European Union Agency for Cybersecurity
IPS	–	Intrusion Prevention System
HTTP	–	HyperText Transfer Protocol
HTTPS	–	HyperText Transfer Protocol Secure
IaAM	–	Identity and access management
IT	–	Information Technology
IP	–	Internet Protocol
IPS	–	Intrusion Prevention system
SSL	–	Security information and event management
SOC	–	Security Operations Center
SSH	–	Secure Shell
TLS	–	Transport Layer Security
VPN	–	Virtual Private Network
ІБ	–	Інформаційна безпека
ІКТ	–	Інформаційно-комунікаційні технології
ПЗ	–	Програмне забезпечення
СУБД	–	Система управління базами даних
ОС	–	Операційна система
ЦОД	–	Центр обробки даних

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що на даний момент практично кожен використовує мобільні пристрої.

В даний час інформація є важливою складовою життя кожної людини. Користувачі цінять мобільні пристрої за швидкість використання та доступу до різноманітного контенту. При такій популярності використання пристрою збільшується його цінність для зловмисників, так як кількість персональних даних у пристрої збільшується з геометричною прогресією.

Тому *метою роботи* є дослідження засобів та механізмів захисту інформаційних ресурсів та додатків мобільних пристроїв.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

- дослідити апаратну частину, нормативно правову базу та операційні системи мобільних пристроїв;
- здійснити опис характеристичних особливостей вразливостей та загроз для мобільних пристроїв;
- розглянути інструменти, які використовуються при захисті мобільних пристроїв, а також надати рекомендації користувачам та розробникам для безпечної роботи з мобільними пристроями;
- провести тестування популярного антивірусного ПЗ та надати рекомендації користувачам щодо вибору програмного забезпечення.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1
ОС ТА ІНСТРУМЕНТИ РОЗРОБКИ ДОДАТКІВ

1.1 Апаратна частина мобільних пристроїв

Для мобільного телефону, який працює на базовій смузі мережі GSM (рівень 1), і стек протоколів, що працює на центральному процесорі, відрізняється, що базуватиметься на стандарті GSM. Для мобільних телефонів CDMA той самий рівень 1 і стек протоколів базуватимуться на стандарті CDMA і так далі для мобільних телефонів на базі LTE, HSPA. Мобільний телефон забезпечує зв'язок з ноутбуком / іншими пристроями за допомогою WLAN, Bluetooth та GPS. Усі ці функції базуються на спеціальних стандартних специфікаціях. Мобільний телефон GSM раніше використовувався лише для голосових програм. У наш час він став більш популярним для SMS / MMS та Інтернет-додатків завдяки функції GPRS. Після впровадження смартфона в телефон вбудовано багато додатків, таких як Facebook, Orkut, Twitter, різні ігри. Зараз мобільний телефон повільно зайняв місце ноутбука для багатьох програм.

На наступному малюнку зображені компоненти загального мобільного телефону незалежно від технології, на якій вони повинні працювати, такі як GSM, CDMA, LTE тощо. Тут ми розберемося з мобільними телефонами стосовно стандарту GSM.

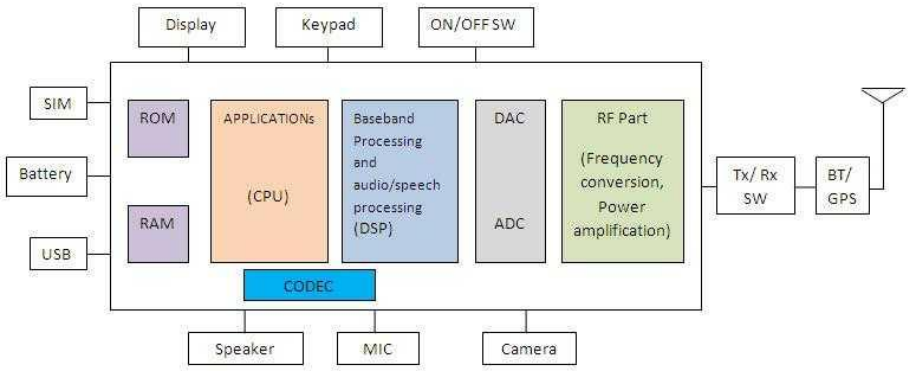

Рисунок 1.1 – Компоненти загального мобільного телефону незалежно від технології

На малюнку зображена блок-схема мобільного телефону gsm. Зазвичай апаратні компоненти мобільного телефону включають дисплей (РК-дисплей, сенсорний екран), клавіатуру, мікрофон, динамік, SIM-карту, акумулятор, USB-порт, антену, блок пам'яті (оперативна пам'ять, ПЗУ), камеру, CODEC, радіочастотну частину, ЦАП / АЦП , частина базової смуги (L1 / Layer1 / фізичний рівень), що працює на DSP, рівні додатків / протоколів, що працюють на центральному процесорі, перемикач ON / OFF та функції Bluetooth / GPS.

Радіочастотний приймач мобільного телефону:

Як показано на малюнку, кожен мобільний телефон матиме радіочастотну частину, яка складається з перетворювача частоти підвищення частоти та перетворювача частоти зниження частоти. Для системи GSM перетворювач вгору перетворює модульований сигнал базової смуги (I і Q) або з нульовою частотою ПЧ (проміжна частота), або якоюсь частотою ПЧ, в частоту РЧ (890-915 МГц). РЧ-перетворювач перетворює РЧ-сигнал (від 935 до 960 МГц) в сигнал смуги частот (I і Q). Для GSM використовується модуляція GMSK. У приймачі мобільних телефонів GSM застосовуються два підходи, тобто гетеродин або гомодин. Основним компонентом, що використовується для перетворення частоти, є радіочастотний змішувач. Щоб дізнатися більше, прочитайте нашу сторінку про гетеродин проти гомодину. Щоб дізнатись більше про конструкцію РЧ-перетворювача, можна ознайомитись на нашій сторінці в розділі статей. Зверніться до таблиці RF проти IF, де згадуються загальні проміжні частоти, що використовуються для різних додатків.

Антена мобільного телефону та комутатор Tx / Rx:

Антена - це металевий предмет, який перетворює електромагнітний сигнал в електричний сигнал і навпаки. Антени, що часто використовуються в мобільному телефоні, мають різні типи, такі як гвинтовий тип, площинний інвертований тип F, батіг або патч. Патч-антени на основі мікросмужки популярні серед мобільних телефонів завдяки своїм розмірам, простоті інтеграції на друкованій платі та багаточастотному діапазону роботи. Сучасні мобільні телефони підтримують різні діапазони GSM, а також різні технології, такі як CDMA, LTE, WiMAX, а також

WLAN, Bluetooth тощо. У цьому випадку цей тип патч-антен виконує свою роботу. Щоб дізнатись більше про антену, зверніться до підручника з антени.

Перемикач Tx / Rx:

Оскільки існує лише одна антена, яка використовується як для передачі, так і для прийому в різний час, перемикач Tx / Rx використовується для з'єднання як тракту Tx, так і шляху Rx з антеною в різний час. Перемикач Tx / Rx управляється автоматично DSP на основі структури кадру GSM щодо фізичного слоту, виділеного для цього конкретного мобільного телефону GSM як в низхідній, так і в висхідній лінії зв'язку. Для систем FDD замість комутатора використовується диплексер, який виконує роль фільтра для розділення різних діапазонів частот. Щоб знати основи ВЧ-перемикачів та виробників, прочитайте сторінку про ВЧ-перемикачі в розділі термінології.

Частина базової смуги мобільного телефону

Ця частина в основному перетворює голос / дані, що передаються через повітряний інтерфейс GSM, в сигнал базової смуги I / Q. Це основна частина, яка змінює модем на модем для різних стандартів повітряного інтерфейсу, а саме: CDMA, Wimax, LTE, HSPA та інших. Його часто називають фізичним рівнем або шаром 1 або L1. Зазвичай він переноситься на DSP (цифровий процесор сигналів), щоб задовольнити вимоги до затримки та потужності мобільного телефону. Для мовлення / аудіо кодек використовується для стиснення та декомпресії сигналу відповідно до швидкості передачі даних відповідному кадру. CODEC перетворює мовлення із частотою дискретизації 8 КГц до швидкості 13 кбіт / с для каналу мовного трафіку з повною швидкістю. Для цього використовується мовний кодер RELP (Residiously Excited Linear Predictive coder), який пакує 260 бітів за 20 мс для досягнення швидкості 13 кбіт / с. Базова смуга або фізичний рівень додасть надлишкові біти, щоб дозволити виявлення помилок, а також виправлення помилок. Виявлення помилок отримується за допомогою CRC та виправлення помилок за допомогою таких методів виправлення помилок, як згортковий кодер (використовується у передавальній частині) та декодер viterbi (використовується у приймальній частині). Окрім цього чергування виконується для даних одного

пакету, що допомагає розповсюджувати помилку протягом часу, отже, допомагає приймачеві де-чергувати та правильно декодувати кадр (послідовний пакет даних).

АЦП та ЦАП:

АЦП (аналого-цифровий перетворювач) та ЦАП (цифро-аналоговий перетворювач) використовуються для перетворення аналогового мовного сигналу в цифровий сигнал і навпаки у мобільній слухавці. На шляху передачі цифровий сигнал, перетворений АЦП, передається кодеру мови. Доступні різні АЦП, серед них популярним є тип дельта сигма. AGC (автоматичне регулювання підсилення) та AFC (автоматичне регулювання частоти) використовуються в тракті приймача для управління підсиленням та частотою. AGC допомагає підтримувати роботу ЦАП задовільно, оскільки він утримує сигнал в динамічному діапазоні ЦАП. AFC підтримує похибку частоти в межах, щоб досягти кращих характеристик приймача.

Програмне забезпечення для мобільних телефонів :

Окрім фізичного рівня, в мобільному телефоні GSM задіяні й інші рівні, щоб він працював із мережею GSM / базовою станцією. Щоб дізнатись більше про стек протоколів, що використовується в мобільному телефоні, зверніться до стеку протоколів GSM. Весь стек протоколів переноситься на процесор ARM або на будь-який інший тип процесорів.

Шар додатків:

Він також працює на процесорі. різні програми працюють у мобільному телефоні GSM. Він включає аудіо, відео та графічні / графічні програми. Він підтримує різні аудіо формати, такі як MP3, MP4, WAV, rm. Зазвичай доступні формати зображень JPEG. Він підтримує відеоформати, наприклад, MPEG-1 до MPEG-5. Мобільний телефон підтримує стандартні роздільні здатності відео CIF, QCIF.

ОС мобільного телефону (операційна система):

У мобільних телефонах підтримуються різні операційні системи, такі як Symbian, java, android, RT-Linux, Palm. Вони працюють на процесорі різних виробників. Для критично важливих для часу програм застосовується RTOS (операційна система реального часу).

Аккумулятор:

Це єдине основне джерело енергії, яке робить / підтримує функціонування мобільного телефону. Існують різні типи акумуляторів, виготовлені з нікель-кадмієвого (NiCd), нікелево-металевого гідриду (NiMH) на основі літію, літій-іонного тощо. Основними факторами для дизайнерів є зменшення розміру батареї, тривалість роботи в режимі розмови, збільшення часу автономної роботи. Зазвичай акумулятор постачається з напругою 3,6 або 3,7 та потужністю 600 мАг або 960 мАг. Зарядний пристрій зазвичай постачається з мобільним телефоном для заряджання акумулятора мобільного телефону. Зарядний пристрій - перетворювач змінного та постійного струму.

Підключення (WLAN, Bluetooth, USB, GPS):

Щоб зробити передачу даних досить швидкою між мобільним телефоном та іншими обчислювальними пристроями (ноутбук, настільний ПК, планшет) або між мобільним та мобільним пристроями, розроблені різні технології, що включають WLAN, Bluetooth, USB. GPS (глобальна система позиціонування) використовується для допомоги в розташуванні та дозволить карті Google ефективно працювати.

Мікрофон і динамік:

Мікрофон: Мікрофон або мікрофон перетворює зміни тиску повітря (результат нашої мови) в електричний сигнал для з'єднання на друкованій платі для подальшої обробки. Зазвичай у мобільному телефоні використовується мікрофон типу конденсаторний, динамічний, вуглецевий або стрічковий.

Динамік: Він перетворює електричний сигнал у звуковий сигнал (коливання тиску), щоб людина могла почути. Це часто поєднується з підсилювачем звуку, щоб отримати необхідне посилення звукового сигналу. Він також пов'язаний зі схемою регулювання гучності для зміни (збільшення або зменшення) амплітуди звукового сигналу.

Камера: Зараз доступні майже всі функції камери мобільного телефону для того, щоб натискати фотографії в різних випадках. Це основні характеристики збільшення вартості мобільного телефону. Існують різні мегапіксельні камери для мобільних телефонів, такі як 12-мегапіксельні, 14-мегапіксельні і навіть 41-

мегапіксельні, доступні в смартфонах. Це стало очевидним завдяки прогресу в сенсорній технології. Якщо ви хочете придбати недорогий мобільний телефон, вони зазвичай використовують мобільний телефон, що не є камерою.

Дисплей і клавіатура:

Дисплей: У мобільних телефонах використовуються різні пристрої відображення, такі як РК-дисплей (рідкокристалічний дисплей), TFT (тонкоплівковий транзисторний) екран, OLED (органічний світлодіод), TFD (тонкоплівковий діод), ємнісний та резистивний сенсорний екран тип тощо

Клавіатура: Раніше клавіатура була простою клавіатурою матричного типу, яка містить цифрові цифри (від 0 до 9), алфавіти (від a до z), спеціальні символи та спеціальні функціональні клавіші. Вони були розроблені для різних програм, таких як прийняття дзвінка, відхилення дзвінка, переміщення курсору (ліворуч, праворуч, зверху, вниз) набору номера, введення імені / sms / mms тощо. Клавіатура "Зараз на добу" була вилучена з дизайну телефону і стала частиною програмного забезпечення для мобільних телефонів. Він з'являється на самому екрані дисплея, яким користувач може керувати, натискаючи кінчик пальця.

1.2 Основні операційні системи мобільних пристроїв

iOS

iOS - це власна операційна система, якою керує Apple, і працює виключно на власних пристроях Apple. Це виграє на користь iOS порівняно з операційною системою Android, яка працює на декількох пристроях виробника (Samsung, HTC, Google), кожен зі своїми стандартами та підходом до безпеки. Apple також суворо вимагає включити додаток до свого магазину. Вони перевіряють, чи є ви законним бізнесом, плата набагато вища, ніж Android або Windows, і люди перевіряють кожну заявку до її подання.

Плюси:

Удосконалення MDM (управління мобільними пристроями), що дозволяє компаніям “вкладати” свої політики на пристрої, які раніше не були можливі в iOS.

Це дозволяє компаніям створювати облікові записи з самого початку (через провайдерів MDM чи Інтернет-провайдерів) та керувати ними, навіть якщо особа мала залишити компанію.

Удосконалюючи вже безпечний процес подання програм, Apple вимагає, щоб програми підписувалися сертифікатами, які перевіряються на серверах Apple. Це дозволяє відкликати, якщо виявлено шкідливий вміст. Програми також потрібно оновлювати / подавати за зашифрованими каналами.

Мінуси:

З моменту випуску iOS 10 у вересні вже був виявлений недолік безпеки. Apple додала альтернативну перевірку пароля до iOS 10, що послабило безпеку локальних резервних копій в iTunes. Цей компроміс локальних резервних копій відкрив можливість для розшифровки брелока (менеджера паролів Apple).

Як і Android, велика кількість мобільних користувачів також володіє пристроями Apple. Одне лише це створює ризик, оскільки воно більш сприйнятливе до того, щоб стати мішенню для нападників.

З виходом iOS 10 з'явилися кращі інструменти управління для IT-команд. Адміністратори можуть запропонувати користувачам оновити будь-який пристрій, зареєстрований у Програмі реєстрації пристроїв, ініціюючи завантаження та встановлення оновлень програмного забезпечення окремо. IT-команди можуть встановлювати та оновлювати керовані програми, обмежуючи загальний доступ до магазину програм та керувати програмами навіть після того, як користувачі встановлюють їх, не перевстановлюючи програму або втрачаючи будь-які дані користувача. Також до iOS 9 включені нові мережеві політики. Адміністратори можуть вказати, як керовані програми використовують мережі, обмежуючи можливість додатка підключатися через стільниковий зв'язок під час роумінгу в інших мережах.

Можливість подальшого управління пристроями, що випускаються компанією, надає IT-командам можливість встановлювати параметри та застосовувати оновлення, що включають важливі випуски безпеки для кращого захисту корпоративних даних. VPN для кожного додатка забезпечує окремі

мережеві шляхи для особистих та корпоративних даних, тоді як керований відкритий захищає корпоративні вкладення від збереження в особистих програмах або хмарних службах. Нарешті, сенсорні ідентифікатори та паролі пристрою ще більше сприяють підвищенню безпеки системи, програм та даних організації.

Android:

Android працює з відкритим вихідним кодом, тобто зловмисне програмне забезпечення набагато частіше. Порівняно з Apple та Windows, набагато простіше подати та отримати ваш додаток до магазину Google Play. Існує нижча плата за подання, не перевіряє ваш додаток людина і не перевіряє, чи є ви законним бізнесом. Google розробив Google Bouncer, сканер зловмисного програмного забезпечення, для контролю та сканування програм, доступних у Google Play Store, але компанії все ще втомилися від ОС Android.

Плюси:

Пряме завантаження / шифрування на основі файлів - Пряме завантаження є новим для Android і дозволяє програмам запускатись у фоновому режимі перед тим, як ви розблокуєте пристрій, і не відкриває жодної особистої інформації. Шифрування тепер відбувається на більш детальному рівні (на основі файлів),

Після того, як влітку минулого року з’явилася атака на вантажні перевезення, Google / Android наростила поліпшення безпеки та витіснила їх набагато швидше, ніж у минулі роки. Магазин Google Play також спостерігав за деякими оновленнями та набагато пильніше відстежував програми та зупиняв шкідливу активність до її початку.

Мінуси:

Android підтримує більшість користувачів смартфонів, що робить їх більш сприйнятливими до зловмисних атак порівняно з іншими мобільними ОС

Оскільки Android працює на багатьох різних пристроях, не всі з них підтримують новітні ОС. Це проблематично через виправлення / оновлення безпеки, які підтримуються в найновішій ОС, і зрештою пристрої більше не отримуватимуть цих критичних оновлень.

Android_4Work

Для боротьби з цими зловмисними атаками для організацій, Android представила Android for Work у вересні 2015 року, що дозволило користувачам розділяти роботу та грати. Подвійні персони використовуються для відокремлення робочих та особистих програм та захисту корпоративних даних. Важливо зазначити, що не всі пристрої мають право на подвійні персони, пристрої деяких виробників не підтримують шифрування, необхідне для запуску персональних персон. Розглядаючи пристрої, що підтримують Android, ознайомтесь із чотирма основними порадами Android щодо кращої мобільної безпеки в блозі Search Mobile Computing.

Windows

Мобільна ОС Windows схожа на iOS тим, що людина переглядає та схвалює всі програми, що надходять у магазин, допомагаючи запобігти отриманню зловмисних програм

Плюси:

З випуском Windows 10 для настільних комп'ютерів / ноутбуків компанія Microsoft розумно оновила свою мобільну ОС, щоб наслідувати її приклад. Найбільші досягнення були пов'язані з безпекою.

Зараз існує шифрування пристрою для локального вмісту, вдосконалене на мобільних пристроях Windows 8, які працювали лише за допомогою якогось рішення MDM.

З невеликою часткою ринку Windows Mobile 10 має меншу ймовірність нападу. Це одне не робить його безпечним, але інтеграція з його флагманською архітектурою настільних / серверних ОС однозначно робить.

Підприємства можуть забезпечити безпечний доступ до ресурсів набагато простіше, ніж до використання Microsoft Passport. Це дозволяє надійно проводити автентифікацію за допомогою багатофакторних облікових даних, що використовуються в службі Active Directory, Azure та Microsoft Account для єдиного входу.

За допомогою нової функції Device Guard на пристрої можуть працювати лише підписані та надійні програми, які блокують будь-які потенційно шкідливі програми.

Мінуси:

Багато недоліків Windows Mobile 10 пов'язані з відсутністю функцій, а не з точки зору безпеки.

Microsoft Enterprise Mobility

ОС Windows для організацій підтримується Microsoft Enterprise Mobility. Microsoft Enterprise Mobility захищає електронну пошту, файли та програми Microsoft Office, заявляючи на своєму веб-сайті, що це єдине рішення, розроблене для цього. Рішення Microsoft допомагає звести до мінімуму складність BYOD, пропонуючи управління мобільними пристроями (MDM) та управління мобільними додатками (MAM) як локально, так і в хмарі, з однієї консолі. Настільна віртуалізація дозволяє користувачам запускати настільні комп'ютери та програми Windows де завгодно та задовольняти мінливі потреби бізнесу, одночасно захищаючи чутливі корпоративні ресурси.

Безпека є основним напрямком Microsoft Enterprise Mobility. Advanced Threat Analytics (ATA) допомагає ідентифікувати порушення та загрози за допомогою поведінкового аналізу та забезпечує чіткий, дієвий звіт про простий графік атак. ATA постійно вчиться на поведінці організаційних структур та пристосовується до відображення змін на швидко розвиваються підприємствах. У міру вдосконалення тактики зловмисників ATA допомагає компаніям адаптуватися до мінливого характеру атак кібербезпеки за допомогою постійної навчальної поведінкової аналітики.

Слід зазначити, що в даний час Windows є найменш використовуваною мобільною ОС з трьох, що, безумовно, грає на її користь, оскільки вона менш цільова. Платформа Windows Phone від Microsoft є найбезпечнішою мобільною операційною системою, доступною для бізнесу, тоді як Android залишається притулком для кіберзлочинців.

Завдяки своїй вдосконаленій аналітиці загроз, яка постійно вивчає моделі та звички організацій, система лише покращується з часом.

Спочатку Microsoft розробили інфраструктуру Windows 8, яка вже була безпечною, і внесли вдосконалення, які стали популярними завдяки настільній ОС

Windows 10 у мобільному середовищі. Apple випустила кілька покращень безпеки своєї ОС, випустивши iOS 10, а Android покращила недоліки безпеки, які переслідували їх у минулому. Оскільки Apple і Android є головною мішенню для зловмисників, зараз безпечніше зробити ставку на мобільну платформу ОС, яка становить близько 2% частки ринку.

Підвищена вразливість Android сприяє політиці Google, що дозволяє стороннім магазинам працювати на ОС - популярній системі для злочинців у всьому світі, щоб обдурити користувачів встановленням шкідливих програм. У 2012 році F-Square зафіксував 10-кратне збільшення кількості шкідливих інсталяційних файлів Android, перескочивши з 5000 шкідливих інсталяційних файлів у другому кварталі до 51 000 інсталяційних файлів у третьому кварталі.

Перевагу має магазин Windows порівняно з магазином Google Play та Apple App Store. Windows все ще перевіряє безпеку додатків реальними людьми, які її тестують, на відміну від Android, але це набагато швидший процес порівняно з процесом Apple, на оновлення якого може зайняти до двох тижнів. Це може стати проблематичним, при видачі нові оновлення безпеки та виправлення помилок. Windows також проводить випадкові перевірки контролю якості всіх програм, що працюють у магазині.

Незважаючи на те, що всі три ОС пропонують IT-командам можливість контролювати додатки та стирати інформацію при втраті пристрою або припиненні роботи працівника, Windows та її всеосяжна платформа Microsoft Enterprise Mobility є найбезпечнішим варіантом. Завдяки можливості захищати та керувати програмами iOS, Android, Windows та Windows 10, це також найпривабливіша платформа для компаній, що впроваджують політики BYOD.

Таблиця 1.1

Статистика використання ОС

Android	72.2%
iOS	26.99%
Samsung	0.39%
KaiOS	0.17%

Unknown	0.14%
Windows	0.02%

1.3 Інструменти розробки додатків

Програми можна використовувати для такого широкого кола потенційних випадків використання.

Компанії можуть використовувати програмне забезпечення для розробки додатків, щоб покращити мобільний досвід для своїх клієнтів. Великі організації зазвичай використовують ці інструменти для створення додатків для внутрішніх цілей, таких як HR, віддалене спілкування співробітників та управління бізнес-процесами.

Навіть підприємці та приватні користувачі можуть інвестувати в інструмент розробки мобільних додатків, якщо у них є нова ідея або вони хочуть розпочати бізнес з нуля.

Найпопулярнішими інструментами є:

1. Appery.io:

Appery - це хмарний конструктор мобільних додатків, який ви можете використовувати для створення додатків для Android або iOS, і включає Apache Cordova (Телефонний розрив), Ionic та jQuery Mobile з доступом до вбудованих компонентів.

Оскільки конструктор працює в хмарі, нема чого встановлювати або завантажувати, і швидко швидко розпочати роботу. Конструктор додатків Appery включає візуальний редактор за допомогою компонентів перетягування для побудови інтерфейсу. Appery автоматично генерує код для будь-яких компонентів, до яких ви потрапляєте. Є можливість підключитися до будь-якого REST API і використовувати його у своєму додатку, і миттєво додавати хмарну базу даних та серверну інформацію до свого додатка, якщо вам потрібно зберігати дані.
Можливо додати потужну функціональність за допомогою каталогу плагінів Appery або створити власні власні приватні плагіни для використання у своїх програмах.

2. Mobile Roadie:

Mobile Roadie - це програма, яка дозволяє будь-кому створювати та керувати власною програмою для iOS або Android. Ще краще, будівля відбувається дуже візуально. Платформа підтримує всі типи медіа, з автоматичним імпортом ключових слів RSS, Twitter або Google News та автоматичним оновленням стіни вентилятора для спілкування в режимі реального часу з користувачами.

Є можливість точно переглянути свій додаток через задню панель Mobile Roadie, як це роблять користувачі на своїх пристроях. Mobile Roadie перевірить якість та доцільність вмісту.

Цей конструктор додатків також надає можливість надсилати push-сповіщення. Це може бути вміст із власного сайту або через саму платформу. Платформа в цілому є мовно агностичною, тому підтримується отримання даних у різних форматах, включаючи XML, JSON, PHP, CSV та HTML. На початку йде отримання кілька варіантів макету, але також є можливість налаштувати будь-який із них на свій смак

3. TheAppBuilder

TheAppBuilder надає набір програм, що підходять для працівників, клієнтів, подій та брошур, з двома різними підходами. Це може бути платформа, з якою слід працювати, якщо ви розробляєте додаток як інтрамережу для компанії. Можливо створити додаток за допомогою онлайн-набору інструментів, і наданий тренінг або сам TheAppBuilder допоможуть визначити та побудувати структуру програми та заповнити її початковим вмістом.

Розробник може захистити як загальнодоступні, так і приватні програми іменами користувачів та паролями та розповсюджувати їх через магазин програм, використовуючи інтеграцію Active Directory від TheAppBuilder, щоб увімкнути вхід із наявними обліковими даними та групами користувачів.

Оновити структуру та вміст програм легко, навіть після того, як вони вийдуть в ефір, тому що є можливість робити необмежені оновлення та публікувати на декількох мобільних платформах одним кліком. Платформа підтримує власні iPhone, iPad та Android, причому оновлення оновлюються протягом 60 секунд після

подання змін. Час оновлення, як видається, не відповідає іншим службам. Ціна: ціна доступна за запитом

1.4 Нормативно-правова база захисту мобільних пристроїв

В Україні розроблено і впроваджено наступні законодавчі та нормативні документи щодо захисту інформації, технічного захисту інформації, захисту персональних даних, електронного цифрового підпису, технічного захисту інформації:

- Закон України «Про захист персональних даних»;
- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;
- Закон України “Про захист інформації в інформаційно телекомунікаційних системах”;
- Закон України “Про телекомунікації”;
- Закон України «Про ліцензування видів господарської діяльності»;
- Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 No1126;
- Постанова Кабінету Міністрів України від 25.05.2011 No616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення»;
- Постанова Кабінету Міністрів України від29.10.00 No1755 «Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу».
- Постанова Кабінету Міністрів України від 16.11.2016 No821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації
- Постанова Кабінету Міністрів України від 21.06.17 No437 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження

господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації».

- Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 No1229.
- Постанова Кабінету Міністрів України від13.03.02 No281 «Про деякі питання захисту інформації, охорона якої забезпечується державою»
- Постанова Кабінету Міністрів України від29.03.06 No373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».
- Постанова Кабінету Міністрів України від12.04.02 No522 «Порядок підключення до глобальних мереж передачі даних».
- Положення про порядок надання відомостей з Єдиного державного реєстру юридичних осіб та фізичних осіб –підприємців, затверджено Наказом Державного комітету України з питань регуляторної політики та підприємництва 20.10.2005 No97, Зареєстровано в Міністерстві Юстиції України 28 жовтня 2005 р. за No1294/11574.
- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 No93, зареєстровано в Міністерстві юстиції України 16.07.07 за No820/14087.

Висновки за розділом 1

Було проаналізовано апаратну частину, нормативно правову базу та операційні системи мобільних пристроїв.

Мобільний телефон GSM раніше використовувався лише для голосових програм. У наш час він став більш популярним для SMS / MMS та Інтернет-додатків завдяки функції GPRS. Після впровадження смартфона в телефон вбудовано багато додатків, таких як Facebook, Orkut, Twitter, різні ігри. Зараз мобільний телефон повільно зайняв місце ноутбука для багатьох програм.

Windows та її всеосяжна платформа Microsoft Enterprise Mobility є найбезпечнішим варіантом. Завдяки можливості захищати та керувати програмами iOS, Android, Windows та Windows 10, це також найпривабливіша платформа для компаній, що впроваджують політики BYOD.

Основою нормативно правової бази є:

- Закон України «Про захист персональних даних»;
- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;

РОЗДІЛ 2
ЗАГРОЗИ ПЕРСОНАЛЬНИМ ДАНИМ В МОБІЛЬНИХ ПРИСТРОЯХ

2.1 Персональні данні в мобільних додатках

Застосування європейської системи захисту даних починається з питання про те, чи відбувається якась обробка „персональних даних". Визначення персональних даних є широким, тобто „Будь-яка інформація, що стосується ідентифікованої або ідентифікуваної фізичної особи („ суб'єкта даних ")" .

Питання про те, чи визначений тип даних кваліфікується як особиста інформація, може вимагати детального аналізу, включаючи юридичний, на який можна отримати адекватну відповідь лише при розгляді конкретного контексту, в якому відбувається обробка інформації.

У середовищі мобільних додатків, коли дані збираються про мобільний пристрій або з нього, особистий характер використання мобільних пристроїв передбачає, що такі дані повинні розглядатися як особисті дані, як у значенні GDPR.

Таким чином, не лише дані на пристрої, що є особистими та приватними за своєю природою, такі як зображення, повідомлення, електронні листи, пункти порядку денного тощо, кваліфікуються як особисті дані, але й дані, що стосуються пристрою, такі як ідентифікатори пристрою, екологічне середовище такі аспекти, як розташування пристрою та дані, пов'язані з його використанням, включаючи журнали, що містять дані про використання, пов'язані з конкретними програмами.

Після того, як розробник додатків збирає (та обробляє) дані на пристрої та його користувачі та з нього, включаючи метадані, пов'язані з пристроєм та поведінкою користувача, усі ключові вимоги щодо захисту даних у GDPRaretriggered. Якщо персональні дані повністю анонімізовані, система захисту даних не застосовується, оскільки анонімні персональні дані неможливо відрізнити від будь-якого іншого типу даних.

Псевдонімні дані - це нова підгрупа персональних даних, введена в юридичному сенсі до GDPR. Відповідно до GDPR, "псевдонімізація" означає обробку персональних даних таким чином, що персональні дані більше не можуть бути віднесені до конкретного суб'єкта даних без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо і підлягає технічні та організаційні заходи, спрямовані на те, щоб персональні дані не приписувались ідентифікованій або ідентифікованій фізичній особі ".

Зокрема, псевдонімічні дані все ще залишаються особистими даними, а процес псевдонімізації - це просто міра, яку GDPR стимулює завдяки своїм вигодам для конфіденційності даних При доступі до конфіденційних (спеціальних категорій) даних застосовуються більш суворі вимоги на підставі статті 9 GDPR.

Відповідні спеціальні категорії даних включають дані, що стосуються расового чи етнічного походження, політичних поглядів, релігійних чи філософських переконань, генетичних біометричних даних та даних про здоров'я, або дані, що стосуються статевого життя або сексуальної орієнтації фізичної особи.

Під час обробки таких конфіденційних даних, наприклад, у додатках для охорони здоров’я чи знайомств, зазвичай контролер повинен забезпечити наявність явної згоди користувача на обробку цих даних для конкретних визначених цілей.

Цілком можливо, що певна інформація, що обробляється в мобільному контексті, наприклад, зображення, повідомлення, введені користувачем дані, містять дані, які мають бути кваліфіковані як конфіденційні відповідно до статті 9 GDPR.

Зображення зазвичай не вважаються конфіденційними даними, але зображення людей можуть виявляти їх расове чи етнічне походження, приватні повідомлення людей можуть розкривати вірування та настрої людей та стан здоров'я.

Те саме може бути справедливим для метаданих, які зібрані з часом можуть надати унікальний інвазивний профіль користувачів. Хоча дані про місцезнаходження не включені до списку спеціальних категорій даних, обробка даних про місцезнаходження, як правило, вимагає особливої уваги до питання

необхідності та пропорційності, а основні мобільні ОС запровадили спеціальні механізми для прозорості даних про місцезнаходження та згоди користувачів.

У випадку надмірних постачальників послуг міжособистісних послуг зв'язку, пропозиція щодо регулювання ePrivacy містить нові правила щодо законності обробки вмісту та метаданих, які суворіші за загальні правила GDPR щодо персональних даних. Точний обсяг нових правил досі незрозумілий, включаючи питання про те, чи застосовуватимуться правила лише до комунікацій у дорозі або також до комунікацій у збереженому форматі.

2.2 Атаки спрямованні на ОС Андроїд та додатки на її основі

На даний час у світі не існує повністю безпечної системи, і Android зовсім не є виключенням. Перше місце серед шкідливих програм для операційної системи (ОС) Android займають SMS-троянці (сімейство Android.SmsSend). Їх головною метою являється відправка високо тарифних повідомлень на спеціальні короткі номери. Доля зібраних таким чином коштів збагачує зловмисників. Подібні програми відрізняються одна від одної лише незначними змінами в інтерфейсі та номерами, на які відправляються повідомлення. Зазвичай їх поширюють під виглядом розповсюджених додатків та ігор, використовуючи відповідні іконки. Наступними йдуть більш серйозні троянські програми. До таких відносяться: Android.DreamExploid, Android.Gongfu, Android.Wukong, Android.Geinimi, Android.Spy то-що. Ці програми, залежно від сімейства, займаються збором конфіденційної інформації користувача, до-даванням закладок в браузер, виконанням команд, які дають зловмисники, відправкою SMS-повідомлень, а також визначенням додатків і т.п. Особливу увагу слід приділити комерційним програмам-шпигунам. Залежно від класу, ціни та виробника, вони перехоплюють вхідні та вихідні SMS-повідомлення і дзвінки, роблять аудіозапис середовища, відстежують координати, збирають статистичні дані браузера (закладки, історію відвідувань) і т.п.

Відкритість системи Android полягає в декількох поняттях. По-перше, код ОС Android доступний і може використовуватися, модифікуватися і покращуватися розробниками відповідно до їх ідей та потреб. З одного боку, це плюс для розробників пристроїв та виробників, з іншого – це дає змогу зловмисникам знаходити вразливості та помилки. По-друге, можна встановити додатки як з офіційного каталогу додатків Google Play, так і з будь-якого іншого доступного сайту. По-третє, розробка додатків є практично розповсюдженою та доступною справою, оскільки для розміщення своїх продуктів в офіційному каталозі необхідно заплатити всього $25, а поширення програм поза його межами взагалі безкоштовне. По-четверте, програми, що розміщуються в Google Play до недавнього часу не піддавалися попередній перевірці або тестуванню з боку Google. Нещодавно з'явилася система Bouncer, яка перевіряє додатки, розміщені в каталозі Play, на наявність небезпечних функцій; облікові записи розробників також піддаються перевірці.

Досить велика кількість розробників мобільних пристроїв використовує систему Android, через це перед споживачами відкривається широкий вибір пристроїв з різноманітним функціоналом. З іншого боку розробка додатків с великим охопленням пристроїв – надзвичайно складна і трудомістка задача для кожного Android-розробника. Коли виходить чергове оновлення операційної системи, розробники додають не лише нові функції, а й усувають раніше виявлені вразливості. Існують випадки, коли пристрій стає об'єктом хакерських атак через несвоєчасне оновлення ОС або, взагалі, відсутність оновлення програмного забезпечення. Причиною можуть бути як технічні, так і економічні фактори.

2.3 Загрози мобільному банкінгу

Вразливості на стороні клієнта:

Найнебезпечніші уразливості є в додатках Android і включають небезпечну обробку глибоких посилань. Глибоке зв'язування по-різному використовується на iOS та Android: розробники на Android мають більшу свободу реалізації. Це пояснює

більшу кількість вразливостей у програмах Android порівняно з iOS. Однак це не означає, що розробники iOS мають імунітет. Безпека мобільного банкінгу залежить перш за все від безпечного життєвого циклу розробки програмного забезпечення (SSDL).

100% клієнтів мобільного банкінгу містять вразливості у своєму коді. Наприклад:

- код не заплутаний;
- захист від введення та переупаковки коду відсутній;
- код містить назви класів і методів.

Дослідження демонструє, що недостатній захист коду робить банки вразливими до аналізу вихідного коду. Для використання вразливостей у коді всім зловмисникам потрібно завантажити програму з Google Play або App Store, а потім декомпілювати її.

Відсутність заплутаності дозволяє зловмисникам аналізувати код і знаходити важливі дані, такі як:

- імена користувачів та паролі, пов’язані з тестуванням;
- ключі шифрування та параметри, з яких можна отримати ключі;
- солі для перемішування та шифрування.

Потім зловмисники можуть використовувати цю інформацію для отримання облікових даних та доступу до веб-серверів. Більше того, хакери можуть аналізувати алгоритм програми та використовувати недоліки бізнес-логіки. Конкуренти можуть також захотіти знати, як розроблена програма для копіювання нових функцій для власних продуктів.

Щоб використати деякі вразливості на стороні клієнта, зловмисникові потрібно лише переконати жертву встановити шкідливий додаток, можливо, за допомогою фішингу.

Небезпечна обробка глибоких посилань є критичною вразливістю, яка може спричинити фінансові збитки для банків. Наприклад, одній банківській програмі не вдалося відфільтрувати URL-адреси з глибоким посиланням. Проблема полягає в

тому, що вбудовані компоненти WebView можуть завантажувати довільні посилання. Тож зловмисники могли скористатися цим, завантаживши посилання на веб-сторінку, що містить шкідливий код, і взаємодіяти з інтерфейсами JavaScript, доступними в цих компонентах WebView. Експерти Positive Technologies розробили тестові сценарії та продемонстрували перехоплення SMS. Вони змогли отримати номери карток, маніпулюючи здатністю сканувати банківські картки за допомогою бортової камери або через NFC. Зловмисники можуть відображати шкідливу сторінку в інтерфейсі програми та пропонувати сканувати карту. Для користувача все виглядає як звичайна банківська операція, за винятком того, що дані отримуватимуть злочинці (а не банк).

Глибоке зв'язування - це технологія, яка дозволяє користувачам переходити між програмами (або розділами в додатку) до певного місця за допомогою спеціальних посилань, подібних до гіперпосилань у веб-додатках.

11 з 14 мобільних банків дозволяють автоматично знімати знімки екрана - функцію, яка допомагає швидко переглядати нещодавно використані програми. Але скріншоти можуть містити конфіденційні дані, такі як інформація про картки та залишки на рахунках.

Клієнтська файлова система майже половини програм містить незашифровану конфіденційну інформацію. Для доступу до цих даних зловмисникам потрібні права root або джейлбрейк. Вкорінення або джейлбрейк пристрою можна здійснити з фізичним доступом або віддалено за допомогою шкідливого програмного забезпечення. В одному додатку для мобільного банкінгу наші експерти знайшли виписки з балансу карт, що зберігаються в телефоні. Ще одна програма зайшла так далеко, що зберегла PIN-код користувача, що дозволило зловмисникам отримати доступ до облікового запису користувача.

Лише один із перевірених мобільних банків не містив уразливостей, що дозволяють зловмисникам отримувати доступ до даних користувачів. 13 із 14 додатків були вразливі до атак man-in-the-middle через відсутність закріплення сертифікатів для перевірки сертифікатів SSL, проблем із реалізацією з'єднання та використання незахищених посилань на зовнішні об'єкти. У разі успіху зловмисники

можуть отримати доступ до конфіденційних даних користувача, а також читати та підробляти дані, передані між сервером та клієнтською програмою.

Вразливості додатків на стороні сервера

Більше половини мобільних банків містять вразливості на стороні сервера. Загалом, жодна сторона сервера не мала рівня безпеки, кращого за "середній". Три мали рівень безпеки, який був "низьким", а один "надзвичайно низьким".

Більшість уразливостей bruteforce спричинені недоліками механізму одноразового пароля (OTP). Найпоширеніша проблема полягає в тому, що пароль залишається дійсним, навіть якщо кількість спроб введення пароля перевищена. Зловмисники можуть отримати доступ до облікового запису користувача та скористатися недоліками OTP, щоб видати себе за користувача під час різних операцій, включаючи переказ коштів.

Три із семи мобільних банків містять вразливості бізнес-логіки на стороні сервера. У більшості випадків ці вразливості впливають на функціональність, безпосередньо корисну для спроб шахрайства. Помилки бізнес-логіки можуть спричинити значні збитки для банків і навіть призвести до юридичних ускладнень.

П'ять із семи мобільних банків мають вразливості на стороні сервера, які хакери можуть використати проти користувачів. Наприклад, недостатня перевірка розширення завантажених файлів в одному мобільному додатку дозволяє зловмисникам завантажувати шкідливі виконувані файли на сервер. Якщо працівник банку запускав такий файл, шкідливий скрипт міг запускати і викрадати дані із сервера, наприклад.

Несанкціонований доступ до програм зазвичай виникає внаслідок недоліків автентифікації та авторизації. Наприклад, зловмисники можуть грубо примусити пароль користувача під час автентифікації та отримати доступ до облікового запису жертви. Далі, якщо зловмисникам вдасться обійти одноразовий захист паролем, використовуючи недоліки OTP, вони можуть видавати себе за жертву.

Облікові дані користувачів виявилися найбільш вразливою здобиччю: імена користувачів та паролі мобільного банкінгу загрожують серверній стороні п’яти мобільних банків. Особисті дані можуть потрапити в руки зловмисників у більш ніж

половині мобільних додатків. Ця інформація може включати імена користувачів, залишки на рахунках, підтвердження переказу, ліміти карток та номер телефону, пов'язаний з карткою жертви.

Що повинні знати користувачі:

Усі програми мобільного банкінгу мають недоліки безпеки. Наші дослідження показують, що програми для Android є більш вразливими, ніж програми для iOS. Вразливі місця, які хакери використовують для шахрайства та крадіжок, як правило, є наслідком помилок кодування. Уникнення таких вад має бути головним пріоритетом для розробників. Однак багато вразливостей неможливо використати без взаємодії з користувачем. Деякі атаки вимагають фізичного доступу до пристрою.

Вкорінення (Android) або джейлбрейк (iOS) пристрою, або не встановлення PIN-коду для розблокування телефону, надає зловмисникам більше можливостей для здійснення зловмисних дій.

Деякі атаки вимагають взаємодії користувача у формі натискання посилання, встановлення шкідливого програмного забезпечення або введення даних на підроблену веб-сторінку.

Вразливості можуть міститися і в самій мобільній ОС. Але Google і Apple постійно оновлюють своє програмне забезпечення та випускають виправлення безпеки. Користувачі повинні пам’ятати, що вразливості стають загальнодоступними після випуску виправлень. Хакери можуть використовувати це для атаки пристроїв, на яких не встановлено останні оновлення.

Поради користувачам

- не відкривайте посилання, надіслані незнайомцями за допомогою SMS або чату. Ніколи не завантажуйте додатки з неофіційних джерел. Завантажуйте програми лише з офіційних магазинів, таких як Google Play та App Store. Вирішуючи, що завантажувати, зверніть увагу на інформацію про розробника програми та кількість завантажень;

- не робіть джейлбрейки та не викорінюйте пристрій. Це відкриває доступ до файлової системи пристрою та відключає механізми захисту даних. Встановіть PIN-код, щоб розблокувати пристрій. Це обмежує можливості зловмисників, навіть якщо вони мають фізичний доступ до вашого телефону;
- завжди встановлюйте останні оновлення для своєї ОС та мобільних додатків.

2.4 Соціальний фактор як вразливість

Людський фактор відіграє не останню роль в її безпеці. При здійсненні нападу на мобільну систему зловмисники зазвичай використовують компоненти соціальної інженерії. Соціальний інжиніринг відноситься до психологічної маніпуляції людьми в інформаційній мережі. Наприклад, поширення шкідливих програм через рекламу в додатках за допомогою використання гучних фраз («Терміново оновити систему», «Версія браузера застаріла», «Встановіть оновлення Skype» і т.п.). Аналогічна ситуація і з розповсюдженням шкідливих програм шляхом розсилки спама по SMS. Іншим компонентом соціальної інженерії являється хибна безкоштовність програми («Нова версія Need for Speed», «Оновлення Dr Web безкоштовно!»), а також залучення тематики «для дорослих». Захистом від цих загроз є уважність з боку самих користувачів. Зазвичай зловмисники підробляють популярні сайти, повторюючи їх оформлення, структуру, або створюють точну копію. Також можуть підробляються і додатки, і, з великою ймовірністю, неуважний користувач надасть зловмиснику доступ до своєї конфіденційної інформації.

Дослідження Enisa вказує на те, що всі мобільні програми вразливі. У кількох випадках для використання вразливостей може знадобитися фізичний доступ до пристрою, але зазвичай це можна зробити віддалено через Інтернет. Кожен тестований мобільний додаток містив принаймні одну вразливість, яку можна було використати віддалено за допомогою шкідливого програмного забезпечення.

Іноді хакеру потрібен повний доступ до файлової системи: джейлбрейк на iOS або root права на Android. Але навіть це не завжди є проблемою. Багато власників мобільних пристроїв нарощують свої привілеї в ОС навмисно, намагаючись обійти різні обмеження, завантажити програмне забезпечення або налаштувати користувальницький інтерфейс. За даними дослідників, 8 відсотків користувачів iOS зламали свої пристрої, а 27 відсотків пристроїв Android працюють із правами root. Пристрої з такими привілеями піддаються більшому ризику, оскільки цими привілеями може зловживати шкідливе програмне забезпечення. Наприклад, зловмисне програмне забезпечення KeyRaider поширюється через платформи розповсюдження додатків для зламаних пристроїв та викрадає облікові дані, сертифікати та ключі шифрування у 225 000 користувачів iOS.

Через масштаби проблеми з шкідливим програмним забезпеченням Google і Apple вживають активних заходів для боротьби з кіберзлочинцями. Для захисту від хакерів Google пропонує Google Play Protect для сканування програм на пристроях Android та самого Google Play. Щоб запобігти розповсюдженню зловмисного програмного забезпечення через Apple App Store, Apple виконує ручний аналіз програм розробників, перш ніж зробити їх доступними для завантаження.

Цей аналіз допомагає зменшити кількість шкідливих програм, але не може охопити всі з них. Шкідливе програмне забезпечення може надходити навіть з офіційних магазинів програм. Хакерам вдалося завантажити 39 шкідливих програм в App Store за допомогою XcodeGhost, підробленої версії законного середовища розробки Xcode, що використовується для створення додатків для пристроїв Apple. Інший приклад - Anubis, банківський троянець, який успішно ухилявся від перевірок безпеки як Google Play, так і системи безпеки Android.

Офіційні магазини програм - це лише один із способів зараження шкідливим програмним забезпеченням пристрою. Навіть абсолютно новий смартфон може містити шкідливий код. Наприклад, атака розробника призвела до попереднього встановлення шпигунського програмного забезпечення на смартфонах Alcatel. Користувацькі пристрої були скомпрометовані ще до того, як їх було запущено

вперше. Інший приклад - бекдор "TimpDoor", який хакери розповсюджували, надсилаючи посилання жертвам за допомогою SMS.

Щоб запобігти атакам, iOS забороняє завантажувати програмне забезпечення з інших джерел, окрім App Store. Але є способи обійти це обмеження. Сюди входить використання власних сертифікатів користувача та управління мобільними пристроями (MDM). Для цього користувач повинен вручну підтвердити, що сертифікат розробника програми є надійним, і дозволити завантажувати та встановлювати програму з ненадійного джерела. Під час фішингової атаки хакери можуть переконати користувача виконати ці дії.

Apple забороняє додаткам App Store використовувати приватні API. Ці API містять методи, які можна використовувати для завантаження інших програм та виконання інших дій. Троянець може використовувати приватні API для встановлення іншого програмного забезпечення, що не є App Store, на пристрій жертви, таким чином, обходячи будь-які перевірки безпеки з боку Apple. Однак самі перевірки Apple не є досконалими, судячи з розповсюдження шкідливих програм, таких як YiSpecter. Техніка, яку використовували зловмисники YiSpecter, була дуже простою. Користувач відкрив заражене посилання, підтвердив встановлення програмного забезпечення поза межами App Store, і пристрій заразився. Опинившись на пристрої жертви, YiSpecter використовував приватні API та автоматично завантажував інші програми для викрадення персональних даних.

Одним із альтернативних способів встановлення шкідливого програмного забезпечення на пристрої Apple є завантаження файлів програм (.ipa) на комп’ютер жертви та їх установка за допомогою ідентифікатора Apple жертви (обліковий запис iCloud) та інсталятора програми (наприклад, Cydia Impactor) через USB з'єднання. Це шкідливе програмне забезпечення може поширюватися в неофіційних магазинах як безкоштовна ("зламана") версія програмного забезпечення App Store. Це те, як пристрої заражалися WireLurker.

Висновки за розділом 2

Було проведенно опис характеристичних особливостей вразливостей та загроз для мобільних пристроїв.

Застосування європейської системи захисту даних починається з питання про те, чи відбувається якась обробка „персональних даних”. Визначення персональних даних є широким, тобто „Будь-яка інформація, що стосується ідентифікованої або ідентифікуваної фізичної особи („ суб’єкта даних ”)” .

Питання про те, чи визначений тип даних кваліфікується як особиста інформація, може вимагати детального аналізу, включаючи юридичний, на який можна отримати адекватну відповідь лише при розгляді конкретного контексту, в якому відбувається обробка інформації.

Досить велика кількість розробників мобільних пристроїв використовує систему Android, через це перед споживачами відкривається широкий вибір пристроїв з різноманітним функціоналом. З іншого боку розробка додатків с великим охопленням пристроїв – надзвичайно складна і трудомістка задача для кожного Android-розробника.

Людський фактор відіграє не останню роль в її безпеці. При здійсненні нападу на мобільну систему зловмисники зазвичай використовують компоненти соціальної інженерії. Соціальний інжиніринг відноситься до психологічної маніпуляції людьми в інформаційній мережі. Наприклад, поширення шкідливих програм через рекламу в додатках за допомогою використання гучних фраз

РОЗДІЛ 3
ЗАСОБИ ТА МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1 Захист в ОС Android

Частка світового ринку мобільних пристроїв під управлінням системи Android величезна. Android, або Android Open Source Project (AOSP), - це набір програмного забезпечення з відкритим вихідним кодом, розробленого Open Handset Alliance під заступництвом Google.

Мобільні сервіси Google (GMS), що включають в себе пропрієтарні API і програмні сервіси, значно розширюють і ускладнюють екосистему Android. Будучи заснованої на базі Linux, Android має всі переваги і недоліки безпеки даної операційної системи. Уразливості мобільних пристроїв під управлінням Android завжди гостро відчуваються в усьому світі в силу великої популярності і поширеності.

Далі було розглянуто, як саме організована захист призначених для користувача даних в Android, але спочатку, був проведенний огляд еволюції захисту.

Огляд еволюції захисту Android:

Ізольована середа додатків.

З перших версій файлове сховище Android розділене на внутрішнє (вбудоване в пристрій) і зовнішнє (SD Card). Саме внутрішнє сховище знаходиться під особливим контролем операційної системи; там додаток ізолюється в пісочниці, отримуючи доступ тільки до своєї власної частини сховища.

В Android 4.3 було додано SELinux (Security Enhanced Linux), який був активний для критичних системних функцій, а починаючи з Android 5.0 механізми безпеки SELinux застосовувалися вже до всієї системи. Подальший розвиток призвело до того, що в Android 9.0 кожен додаток працює в окремій «пісочниці»

SELinux. Треба відзначити, що починаючи з Android 7.0 суворіші обмеження вводяться і на зовнішнє сховище даних (SD Card).

Шифрування даних.

Перші версії не застосовували ніяких методів шифрування для захисту даних користувача. В Android 4.4 введена опція шифрування всього диска, а з Android 5.0 шифрування диска стало стандартом за замовчуванням.

Подальша еволюція Android оптимізувала роботу з шифруванням, домігшись комбінації з шифрування метаданих (інтегрована в Android 9.0) і шифрування на основі файлів (Android 7.0), що дозволяє пристрою безпечно виконувати критично важливі системні функції без розблокування телефону.

Контроль цілісності.

Відбувається за допомогою перевірки завантажувального коду і файлів APK (Android Package). Перевірка завантажувального коду в розділі здійснювалася модулем «dm-verity» і була введена в Android 4.4. Якщо цілісність даних була порушена, користувач отримує попередження, але завантаження ОС триває.

В Android 8.0 представлена нова версія завантажувача Android Verified Boot (AVB). Перевірка установки APK-файлів з джерел відмінних від довірених (Google Play) додана в Android 2.1. В Android 7.0 введена система підпису додатка, специфічна для APK. В 2021 році Google вимагає, щоб програми при публікації в Google Play використовували App Bundles.

Остаточну зборку і підписування APK перед публікацією в Google Play здійснює безпосередньо Google, що викликає протести і невдоволення багатьох розробників.

Надійність апаратного забезпечення.

Android не вимагає використання спеціального обладнання відповідно до специфікації від Open Handset Alliance. Android 4.1 вводить механізм Keymaster Hardware Abstraction Layer (HAL) для зберігання ключів на рівні апаратної абстракції. Keymaster TA виконує операції підпису і перевірки додатків. В Android 6.0 додані AES і HMAC, а також контроль за використанням ключів шифрування. Введення додаткового апаратного модуля безпеки (secure element), аналогічного SEP

в iOS, стало звичайним явищем в останні роки. Це - криптографічний модуль, що існує окремо від основного процесора і призначений для роботи виключно з секретними даними користувача. В Android 9 додана функціональність StrongBox Keymaster, яка розширює можливості Keymaster TA з метою здійснення криптографічних операцій на головному процесорі пристрою.

Сучасний захист даних користувача Android:

Аутентифікація

Цифровий код, буквено-цифрова фраза або патерн (графічний ключ-візерунок). За деякими дослідженнями, патерн-аутентифікація еквівалентна по силі цифровому паролю з двох або трьох цифр. Також підтримується біометрична аутентифікація по відбитку пальця або особі користувача, що застосовується виробниками пристроїв за бажанням, тому що не потрібно для Android в обов'язковому порядку.

Підтримується опція Smart Lock, коли система використовує інформацію про оточення для розблокування (наприклад, коли телефон перебуває вдома або в кишені).

Пісочниця для додатків

Використовується дискреційний контроль доступу (DAC) і SELinux. Файли додатки в системі мають дозволу засновані на ідентифікаторах користувачів Linux, тому спроба доступу програми не до своїх файлів викликає помилку. Додатковий рівень ізоляції забезпечує SELinux.

Політики SELinux дозволяють здійснювати контроль привілеїв додатків більш строго. Обов'язковий контроль доступу (MAC) гарантує, що якщо процес запущений з правами суперкористувача (root), це не призведе до повної компрометації системи.

Шифрування

Розділяється в Android на два види: повне шифрування диска і файлове шифрування. Повне шифрування диска (з'явилося в Android 4.4) базується на модулі «dm-crypt» ядра Linux. Застосовується алгоритм AES-128 в режимі CBC з ESSIV. Майстер-ключ шифрується ключем, який створюється з пароля користувача (цифровий код, фраза, патерн).

Майстер-ключ повинен бути доступний при завантаженні ОС, щоб була можливість активувати основні функції системи. Після аутентифікації користувача майстер-ключ зберігається в пам'яті пристрою завжди, так як він необхідний для всіх операцій блокування доступу до розділу з даними.

Файлове шифрування забезпечує більш гранульований контроль. Модуль «fscrypt» ядра Linux використовує алгоритм AES-256 в режимі XTS для файлів і CBC для метаданих файлів.

Зашифровані файли в свою чергу поділяються на дві категорії: Credential Encrypted (CE) і Device Encrypted (DE). Дані CE зашифровані з використанням ключа, отриманого з призначеного для користувача пароля, тому доступ до них відкривається тільки після розблокування пристрою.

Дані DE базуються на секретах безпосередньо устрою і доступні як при завантаженні, так і після розблокування. За замовчуванням для всіх додатків застосовується CE, а DE зарезервований для певних системних додатків (виклики, годинник, клавіатура і т. Д.).

Поєднання шифрування на основі файлів з шифруванням метаданих дозволяє Android здійснити захист весь вміст у пристрої. Однак зловмисник, якому вдалося отримати доступ до пам'яті пристрою (наприклад, застосувавши експлойт для компрометації ядра системи), може отримати прямий доступ до майстер-ключу і зашифрованих даних.

Знімний носій даних (SD-карта)

Зручна функція розширення пам'яті пристрою забезпечується підтримкою SD-карт. В Android 6 представлена опція адаптируемого сховища, коли система може інтегрувати SD-карту як частина свого внутрішнього сховища, застосовувати там шифрування і управляти доступом. З іншого боку, ця опція прив'язує SD-карту до одного пристрою, так як ключі шифрування зберігаються безпосередньо на останньому.

Апаратні елементи безпеки

Безпека в сучасних пристроях під управлінням Android реалізується і апаратними методами. Пристрої з архітектурою ARM застосовують механізм ARM

TrustZone. На відміну від Apple SEP, TrustZone використовує один процесор, а не окремий співпроцесор, що ніяк не позначається на рівні захисту.

Деякі виробники встановлюють додатковий процесор безпеки: наприклад, у Samsung він є в лінійці Galaxy S, а Google вставляє чіп Titan M в пристрої лінійки Pixel. Ці модулі (secure elements) є по суті аналогами Apple SEP для операцій тільки з секретними даними. Ключі Keymaster передаються в ці захищені апаратні модулі для обробки, що не задіюючи основний процесор. Android Verified Boot (AVB)

Застосовується модуль верифікації «dm-verity» для перевірки цілісності початкового завантаження системи на основі криптографічного хеш-дерева. Якщо у міру завантаження модулів ОС одне зі значень не збігається з очікуваним, то перевірка завершується помилкою і пристрій переводиться в нефункціональне стан.

Підтримується опція відкоту до попередньої безпечної версії Android, яка зберігається в захищеному від несанкціонованого доступу розділі. Розблокований завантажувач дозволяє відключити AVB і виконувати довільний код при завантаженні пристрою, що може бути корисно розробникам або користувачам, що бажають отримати рут-доступ.

3.2 Захист в ОС IOS

У 2020 році корпорація Apple заявила, що кількість активних пристроїв по всьому світу складає більше 1 400 000 000. 48% смартфонів у США і західних країнах - iPhone під управлінням iOS.

Поступове зростання кількості пристроїв Apple на світовому ринку приваблює не тільки зловмисників, а й фахівців з пошуку вразливостей (БагХантер), яким корпорація пропонує програми винагороди до 2 000 000 доларів США. У обмеження ОС і додатків, що працюють на пристроях Apple, корпорація вкладає великі кошти.

Висока цінність експлойтів і централізоване реагування на інциденти створюють класичну боротьбу між щитом і мечем.

Огляд еволюції захисту Apple iOS

Шифрування даних.

Перша версія шифрування даних флеш-пам'яті при відключенні харчування була реалізована в iOS 3 (2009 рік). Ключ шифрування не залежав від коду доступу користувача і не був потрібний для дешифрування. В iOS 8 (2014 рік) Apple значно збільшила кількість зашифрованих даних на пристрої з використанням ключа, який генерувався на основі пароля користувача. З функцією Data Protection видалення даних відбувається разом з ключами без можливості відновлення.

Однак в деяких випадках видалення даних користувачем відбувається за допомогою їх перенесення у відповідний розділ бази даних SQL на пристрої, що зберігає можливість подальшого відновлення.

Від кодів до біометрії.

TouchID з'явився в 2013 році, а в iOS 9 (2015) була збільшена стандартна довжина цифрового пароля - до шести символів. До цього паролі, що складалися з чотирьох символів, могли бути обійдені програмними експлойта. Ємнісний датчик відбитків пальців і подальший FaceID (2017), на думку Apple, підвищили і спростили безпеку, так як частота, з якою обробляються біометричні дані, обмежена SEP (Secure Enclave Processor).

Ефективність даних нововведень піддавалася сумніву в наукових колах. SEP-архітектура і посилення апаратних компонентів пристроїв. З еволюцією iOS змінювалися апаратні компоненти пристроїв Apple. До введення чіпа A4 (власна однокристальна розробка SoC) Apple використовувала компоненти від Samsung, LG та інших виробників (2007-2009 роки).

Безпека будувалася на шифруванні завантажувального пам'яті NOR за допомогою апаратного ключа AES (ключа UID), який управлявся прискорювачем Crypto Engine. Архітектура SEP (Secure Enclave Processor) була вперше реалізована в чіпі A7 (iPhone 5S, 2013) і дозволила виконувати функції безпеки окремо від основного процесора, на якому працюють ОС і додатки.

Активуючи TouchID, SEP використовує власний ключ UID для шифрування. Особливість полягає в тому, що при генерації ключа SEP навіть виробники не знають ключ UID. Починаючи з чіпа A7 відбувається послідовне посилення безпеки і продуктивності, розширення функцій SEP. Наприклад, в чіпі A12 (2020 рік) Apple

встановила захист на режим оновлення прошивки пристрою (DFU mode), як це реалізовано в режимі відновлення (recovery mode).

iCloud Keychain.

З 2016 анонсований iCloud Keychain, а в iOS 11 (2017) представлений CloudKit з подальшим API для сторонніх розробників. Перевага полягає тут в тому, що зберігання контейнера довільних даних в хмарі організовано особливим чином: ніхто крім користувача зі своїм Keychain, навіть сама Apple, не може дешифрувати ці дані.

Сучасний захист даних користувача iOS

Ключові елементи захисту сформовані взаємодіями безпосередньо з пристроєм і з хмарними технологіями.

Аутентифікація

Фізичне взаємодія з пристроєм: цифровий / буквений код або біометрична аутентифікація. 6-символьний пароль активований за замовчуванням. Підтримується вибір довших пральних буквено-цифрових фраз. Можливо повне відключення аутентифікації, що вкрай не рекомендується Apple. Спроби перебору цифрових паролів блокуються часовими інтервалами. TouchID (ємнісний датчик відбитка пальця) і FaceID (розпізнавання особи камерою, чутливої до глибини) застосовуються Apple для організації більш високого рівня безпеки користувачів.

Підписування коду додатків

Цифрові підписи допомагають серйозно обмежувати виконуваний код на iOS. Це досягається за рахунок безпечного завантаження (відбувається перевірка підпису, вбудованої на низькому рівні (Boot ROM), що гарантує довгострокову захист від ініціалізації підозрілого софта) і за рахунок підпису додатка, що представляє собою наступну комбінацію: підпис, яка контролюється Apple, і сертифікати з відкритим ключем для масштабування системи.

Для більш спеціалізованого запуску додатків на iOS в рамках організації необхідно придбати так звані «сертифікати підпису підприємства».

Пісочниця і аналіз коду

Для захисту від підозрілих додатків накладаються обмеження доступу до призначених для користувача даних і API за допомогою ізольованого середовища (пісочниці). Додатком обмежується доступ до файлової системи, простору пам'яті. У підписаному маніфесті позначається дозволений доступ до системних ресурсів і службам, наприклад службі геолокації.

Додатки з App Store проходять автоматичну і ручну перевірку коду. Втім, навіть при цих суворих обмеженнях деякі небажані програми можуть пройти перевірку і порушити конфіденційність користувача.

Шифрування

На той випадок, якщо зловмисникові вдасться обійти механізми безпеки через логічні уразливості або недоліки в обладнанні, Apple підготувала надійну систему шифрування даних пристрою - Data Protection. iOS застосовує криптографічні стандарти AES, ECDH over Curve25519 та інші схвалені Національним інститутом стандартів і технологій США (NIST).

Доступ до даних прив'язаний до пристрою і контролюється користувачем. Ключ для шифрування даних формується на основі комбінації обраного користувачем пароля і UID (унікальний апаратний секретний кріптоключа).

Після перезавантаження пристрою потрібно відновити ключі шифрування шляхом введення встановленого раніше пароля, далі для розблокування ключів досить біометричних даних.

Обхід шифрування присікається двома шляхами: функцією отримання ключа на основі пароля і методом обмеження припущень зі збільшенням тимчасових інтервалів. Apple використовує кілька «класів захисту» (Class key) шифрування, які розробники вільні вибирати при створенні файлів або об'єктів даних:

- повний захист (CP) - через 10 секунд після блокування пристрою ключі шифрування видаляються;
- захищено поки не відкрито (PUO) - зберігається недовговічний відкритий ключ в пам'яті, передача зашифрованих файлів при заблокованому

пристрої. Чи включається повний захист даних (CP) після того, як файл був створений і закритий;

- захищено до першої аутентифікації користувача - першої розблокування (AFU) - при введенні першого пароля ключі шифрування розшифровуються в пам'яті і залишаються там при блокування пристрою;
- немає захисту (NP) - при вимкненому пристрої ключі шифрування зашифровані тільки апаратними ключами UID. Ці ключі постійно доступні в пам'яті, коли пристрій включено.

3.3 Рекомендації розробникам мобільних додатків

Як показують дослідження, однією важливою проблемою в галузі мобільних додатків та конфіденційності є розрив між законодавчими вимогами та перекладом цих вимог у практичні рішення, які розробники програм можуть застосувати. Дійсно, існуючі рекомендації розробникам додатків зазвичай дають уявлення лише про те, що розробники повинні робити, без подальших вказівок щодо того, як вони зможуть виконати ці вимоги. Наприклад, в області дозволів ми спостерігаємо, що вказівки щодо захисту даних зосереджені на тому, як постачальники програм / розробники повинні організовувати згоду щодо особистої інформації, яку вони збиратимуть та оброблятимуть. У певному сенсі вони відповідають на запитання "що": "Що повинен робити постачальник / розробник програми? Він / вона повинен попросити згоди. Тим не менше, рекомендації містять менше або взагалі не містять вказівок щодо "запитання" про згоду, що є основним фактором для забезпечення конфіденційності. "Як, коли, яким чином" - це запитання, які повинні задати розробники додатків, коли йдеться про переведення частини цього у моделі дозволів, що надаються різними ОС. Отже, в ідеалі рекомендації, які можуть бути застосовані для розробників додатків, повинні включати відповіді на деякі основні запитання, такі як:

- коли розробники повинні запитувати дозвіл (наприклад, під час встановлення, виконання, коли програма оновлюється)?
- як часто розробники повинні запитувати користувачів для дозволів і як їм боротися із звиканням користувачів?
- чи є способи переробити функціональність програми (або платформу ОС), щоб кількість необхідних дозволів була зведена до мінімуму?
- скільки поля слід залишити для уподобань користувачів?
- яка допустима межа вибору користувача щодо дозволів та повідомлень?

Чи правильні ці запитання, і як найкраще відповісти на них, щоб вони могли діяти для розробників, є важливими питаннями, які повинні бути невід'ємною частиною будь-якої ініціативи щодо надання рекомендацій розробникам додатків. Ключовою проблемою є надання достатньо загальних рекомендацій, щоб вони не втрачали своєї актуальності завдяки оновленням операційних систем та пов'язаних з ними функціоналам конфіденційності та відповідали сучасним обмеженням для екосистеми. Більше того, деякі інші важливі питання, які необхідно вирішити, щоб такі рекомендації були корисними та ефективними, такі як:

- поінформованість та освіта. У багатьох випадках розробники можуть бути не тими, хто несе відповідальність, і не може розглядатися як той, хто відповідає за захист даних, однак, вони можуть існувати, щоб змінити ситуацію;
- рекомендації повинні поєднуватися з інформаційною кампанією, яка дозволяє розробнику визначити, яку роль вони можуть зіграти у вирішенні вимог щодо захисту даних;
- вони також повинні зробити очевидним терміновість для розробника вирішити ці проблеми, враховуючи численні інші обов'язки, на які вони покладаються. Навчання розробників з питань конфіденційності та безпеки має вирішальне значення для цього;
- специфічно для умов розробників додатків. Існує небагато наукових досліджень, що оцінюють розробників та умови, за яких вони розробляють мобільні

програми із захисту даних з точки зору дизайну. Нещодавно було запущено кілька проектів, які розглядають, як найкраще дати рекомендації окремим розробникам;

- поширення. Потрібно вивчити, чи є один документ PDF, список 10 найкращих, портал чи інші варіанти найкращим способом зробити рекомендації доступними, актуальними та корисними для розробників. Відповідь може також залежати від типу рекомендацій (наприклад, фрагменти коду можуть краще відображатися на StackOverflow, тоді як юридичні вимоги краще пояснити в довшому PDF-файлі) або проблеми, які спонукають розробників до рекомендацій. показує останні статистичні дані щодо ресурсів, до яких розробники Android звертаються, коли вони звертаються за технічною допомогою або мають запитання, пов'язані з безпекою.

Ця статистика випливає з досліджень, які показують, що найпопулярнішим ресурсом може бути не той, який повертає правильні або ефективні результати (тобто книги можуть служити розробникам краще, ніж потрапляння на випадкову сторінку в StackOverflow);

- рекомендації повинні бути легкими для сприйняття і не треба очікувати, що розробники думатимуть як юристи, науковці чи політики. Вони в ідеалі повинні говорити про свої умови праці, а також стосуватися стресу в управлінні або почуття пригніченості, коли вони можуть зіткнутися з такими питаннями, як захист даних та конфіденційність;
- визначити типові проблеми захисту даних: важливо визначати та фіксувати ті моменти, коли розробники помічають, що вони несуть відповідальність за захист даних.

3.5 Рекомендації щодо зниження ризику виникнення загрози

Рекомендації для користувачів:

Не відкривайте посилання, отримані від невідомих відправників, у SMS-повідомленнях та чатах. Навіть якщо ви знаєте особу, яка пропонує заявку, вона

залишається пильною. Ніколи не підтверджуйте запити на встановлення сторонніх програм на ваш смартфон

Регулярно оновлюйте свою ОС та програми. Якщо ви скористалися або зламали свій пристрій, пам'ятайте, що він може не оновлюватися автоматично

Будьте пильні, переглядаючи поштову скриньку. Уважно перевіряйте посилання, перш ніж їх відкривати, навіть якщо ви є клієнтом компанії, яка надіслала електронний лист. Якщо пов'язана адреса містить помилки, правопис електронної пошти не є справжнім. Пам'ятайте, що працівники банку ніколи не запитують повну інформацію про картку

Ваш PIN-код повинен бути справді випадковим. Не використовуйте свою дату народження, номер телефону або ідентифікаційний номер. Використовуйте біометричну автентифікацію (відбитки пальців, голос або обличчя), якщо ваш пристрій це підтримує

Не посилюйте привілеї. Вкорінення або джейлбрейк пристрою відкриває доступ до файлової системи пристрою та відключає механізми захисту

Будьте обережні, коли програми вимагають надто широкого доступу до функціональних можливостей або даних. Якщо запитувані дозволи здаються нерозумними для цілей програми, не надавайте їх.

Рекомендації для розробників:

Android: Використовуйте LocalBroadcastManager для надсилання та отримання трансляційних повідомлень, не призначених для сторонніх програм

IOS: Якщо вам потрібно використовувати посилання для взаємодії між компонентами, використовуйте універсальні посилання

IOS: Щоб вимкнути використання сторонніх клавіатур у програмі, застосуйте метод shouldAllowExtensionPointIdentifier у програмі UIApplicationDelegate

Android: Якщо програма приймає введення конфіденційних даних, таких як фінансова інформація, застосуйте спеціальну клавіатуру. Це захистить додаток від атак, які маніпулюють системою клавіатури

Використовуйте спеціальне фонове зображення, щоб замаскувати конфіденційні дані на екрані програми

Сучасні пристрої, як правило, використовують біометричні дані (Touch ID або Face ID) для автентифікації в додатках. У цьому випадку PIN-код зберігається на пристрої. Локальне зберігання конфіденційних даних допустимо лише в спеціальних каталогах із шифруванням. Android має сховище ключів під назвою Keystore; iOS має брелок

Не потрібно надсилати одноразові паролі двічі як в SMS-повідомленнях, так і в push-сповіщеннях. Натомість використовуйте вибраний користувачем спосіб доставки пароля

TRACE можна використовувати для обходу захисту файлів cookie за допомогою прапора httpOnly. Вимкнути обробку запитів TRACE

Тривалість сеансу повинна бути обмежена. Ідентифікатор сеансу повинен бути видалений як на стороні клієнта, так і на стороні сервера. Сервер повинен створювати новий сеанс для користувача щоразу, коли потрібна автентифікація

Для максимальної безпеки зв'язку клієнт-сервер ми рекомендуємо використовувати закріплення сертифікатів. При такому підході сертифікат вбудовується безпосередньо в код мобільного додатка. В результаті додаток стає незалежним від сховища сертифікатів ОС. Це запобігає атакам MITM

Фільтруйте введені користувачем дані на стороні сервера. Використовуйте HTML-кодування для спеціальних символів

Обмеження спроб автентифікації мають бути впроваджені як на стороні сервера, так і на стороні клієнта

Висновки за розділом 3

Було проведенно огляд інструментів, які використовуються при захисті мобільних пристроїв, а також надання рекомендацій користувачам та розробникам для безпечної роботи з мобільними пристроями.

РОЗДІЛ 4
ТЕСТУВАННЯ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ. ПОВЕДІНКОВИЙ АНАЛІЗ МОБІЛЬНОГО АНТИВІРУСНОГО ПЗ

4.1 Об’єкти тестування

Для тестування було вибрано найпопулярніше антивірусне програмне забезпечення:

1. Avast Premium Security;
2. ESET SMART SECURITY;
3. F-Secure SAFE;
4. Avira Prime;
5. Trend Micro;
6. McAfee AntiVirus Plus;
7. NORTON ANTIVIRUS;
8. KASPERSKY SECURITY CLOUD;
9. Bitdefender.

4.2 Параметри тестування

Тестовані параметри швидкодії

Під час тестування на швидкодію і продуктивність антивірусів, вимірювалися такі параметри:

1. використання ресурсів оперативної пам'яті, процесора і жорсткого диска в стані спокою

Вимірювалося використання оперативної пам'яті,% завантаженості процесора, час читання / запису даних (час зайнятості диска операціями читання / запису - чим менше, тим краще).

весь процес займав 5 хвилин після 3-хвилинного інтервалу від запуску комп'ютера. Монітор ресурсів збирав дані кожні 5 секунд протягом 5 хвилин, після чого враховувалася середня продуктивність - екстремальні значення (мінімум і максимум) не бралися до уваги;

2. використання ресурсів оперативної пам'яті, процесора і жорсткого диска під час сканування:

та ж процедура, що і в пункті 2, з тією різницею, що вимірювання параметрів продуктивності запускалося на початку сканування, і процедури збору даних тривала до кінця сканування;

3. час сканування:

При виконанні кроку 3 вимірювався час операції сканування;

4. температура пристрою при скануванні:

При виконанні кроку 4 вимірювалася температура під час операції сканування;

5. пропускна здатність сканування (швидкість сканування):

це швидкість сканування, виражена в [MB / c]. Чим більше, тим краще - сканування буде завершено швидше.

Тестовані параметри захисту:

1. Перевірка приватності додатків
2. Функція фотографування викрадача
3. Блокування небажаних викликів
4. Перевірка захисту WiFi
5. Оцінка перевірених додатків в офіційному магазині
6. Знаходження загубленного пристрою

4.3 Створення середовища-емуляції для проведення тестування

Тестована система

Був підготовлений спеціальний образ OS Android 9.0 с критичними оновленнями від 5 квітня 2021 року. Після цієї дати поновлення Android були

вимкнені, щоб не вплинути на результати випробувань. Всі інші настройки були за замовчуванням.

Комп'ютер, який використовується для тестування, має наступні параметри:

Процесор: Intel Core i5-7200U 240 2,8 ГГц

RAM: 2x4GB DDR3 1333 МГц

Жорсткий диск: Seagate 500 Гб SATA II 7200 RPM 32MB Cache

Також було створенно спеціально для тестування та доступу до ПЗ обліковий запис Google.

Рисунок 4.1 – Створення образу для ПЗ BlueStacks

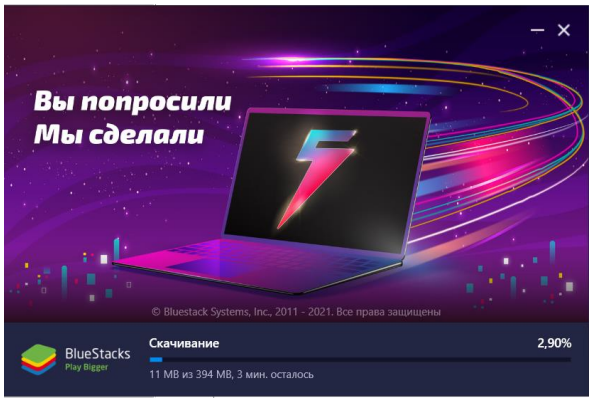

Рисунок 4.2 – Встановлення програми

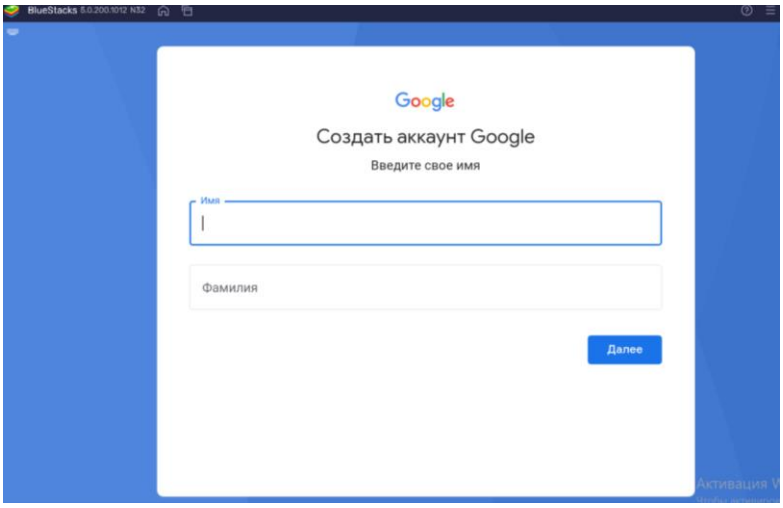

Рисунок 4.3 – Створення аккаунту

4.4 Проведення тестування мобільного антивірусного ПЗ

1. Збільшенно кількість об’єктів сканування. Спільна кількість файлів зайняла 8,72 гігабайти пам’ять на пристрої. Також бли встановлено шкідливе пз.

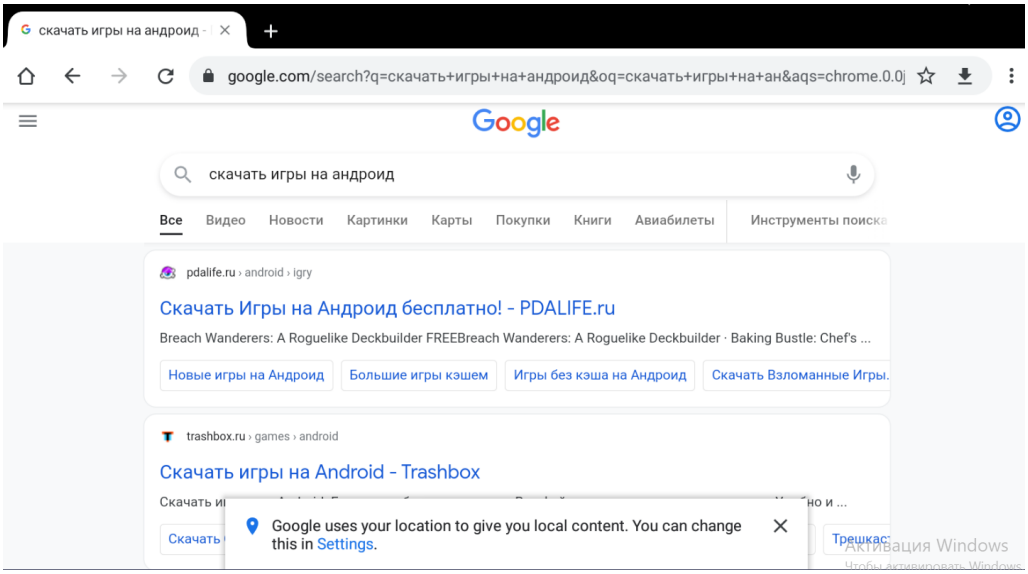

Рисунок 4.4 – Встановлення додаткових файлів

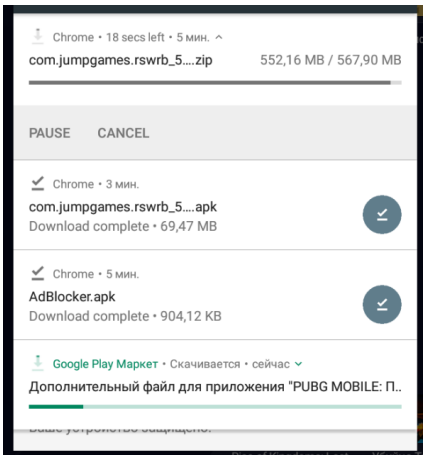

Рисунок 4.5 – Завантаження шкідливого ПЗ

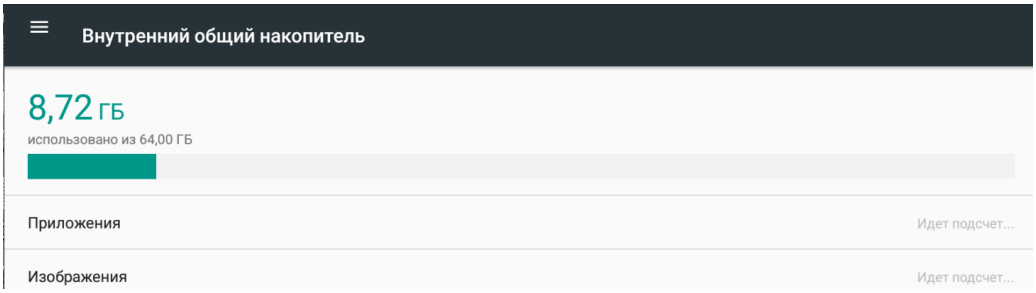

Рисунок 4.6 – Використання пам’яті пристрою

2. Було проведенно встановлення ПЗ для контролю тестованих параметрів

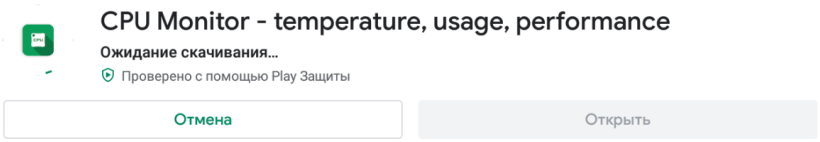

Рисунок 4.7 – Встановлення CPU Monitor

3. Було встановленно об'єкт дослідження.

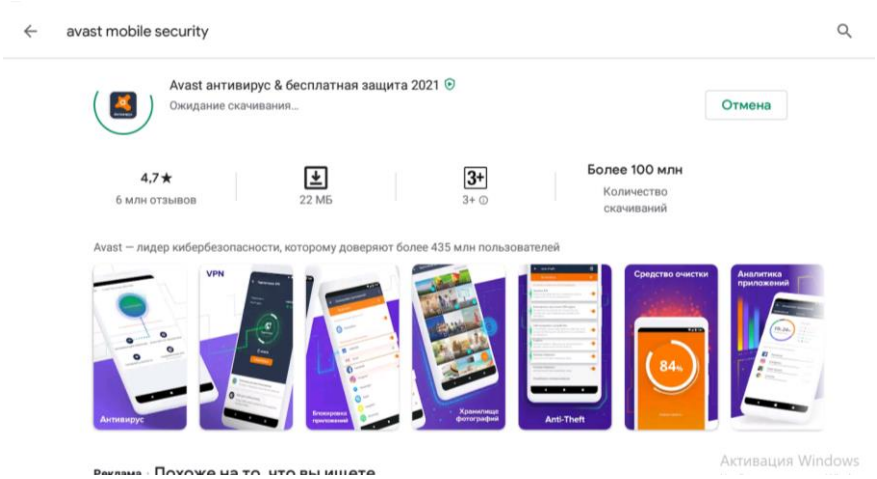

Рисунок 4.8 – Встановлення об’єкту дослідження

Рисунок 4.9 – Завершення встановлення об’єкту дослідження

4. Було проведенно процес тестування.

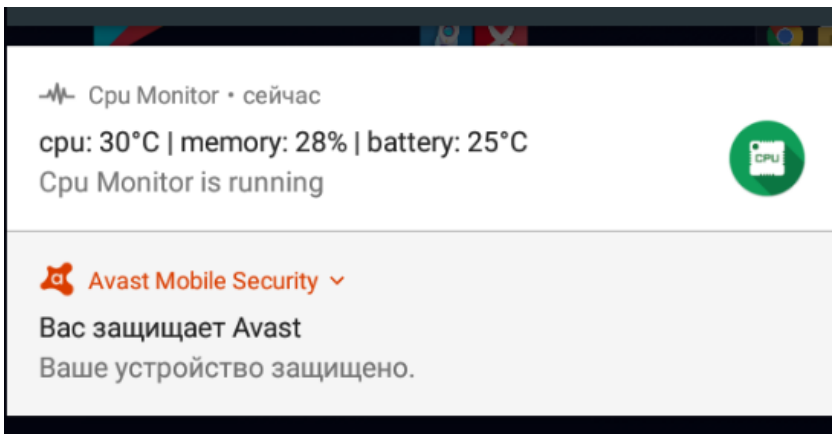

Рисунок 4.10 – Фіксація результатів в стані спокою

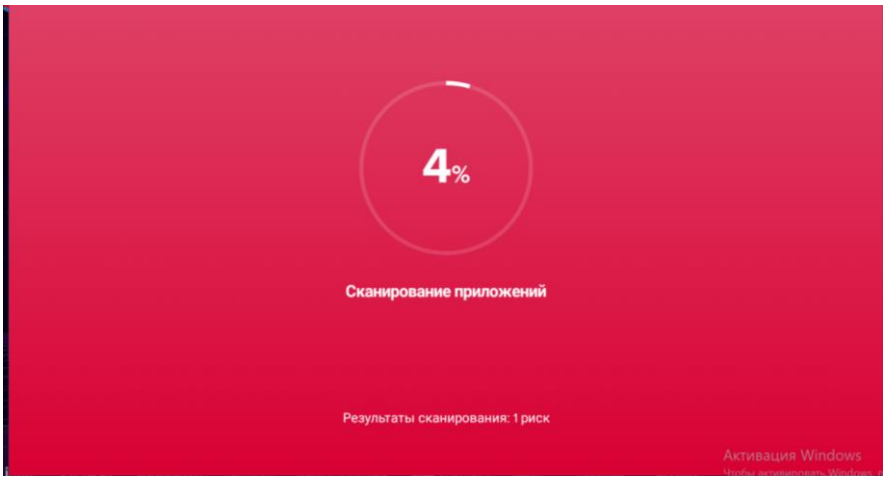

Рисунок 4.11 – Запуск сканування

Рисунок 4.12 – Фіксація часу сканування

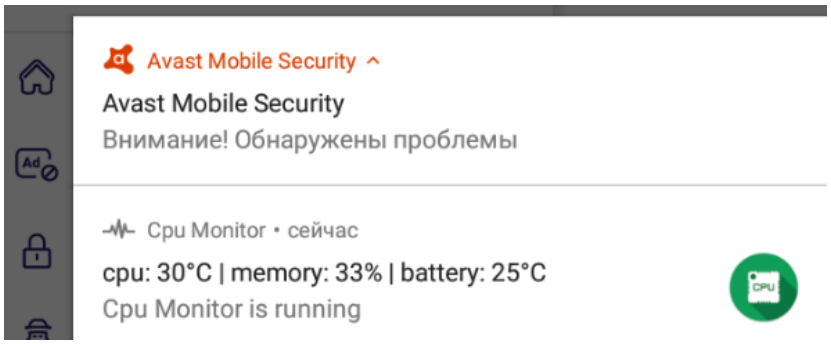

Рисунок 4.13 – Фіксація параметрів під час сканування

4.5 Результати тестування

1. Було провереденно тестування за параметрами.

Назва ПЗ	Avast Premium Security	ESET SMART SECURITY	F-Secure SAFE	Avira Prime	Trend Micro	McAfee AntiVirus Plus	NORTON ANTIVIRUS	KASPERSKY SECURITY CLOUD	Bitdefender	Надання балу
GPU спокій	28 C°	29 C°	27 C°	31 C°	30 C°	29 C°	32 C°	33 C°	29 C°	<= 30 / 1 балл
Пам'ять спокій	28%	28%	28%	28%	31%	28%	29%	32%	26%	<= 30 / 1 балл
Температура спокій	25 C°	26 C°	25 C°	27 C°	30 C°	25 C°	26 C°	27 C°	25 C°	<= 27 / 1 балл
GPU при скануванні	30 C°	32 C°	31 C°	31 C°	35 C°	31 C°	34 C°	37 C°	32 C°	<= 35 / 1 балл
Пам'ять при скануванні	33%	32%	37%	40%	39%	32%	35%	41%	31%	<= 39 / 1 балл
Температура при скануванні	26 C°	27 C°	26 C°	29 C°	32 C°	27 C°	28 C°	30 C°	25 C°	<= 30 / 1 балл
Час сканування (хв:с)	01:35	01:46	01:54	02:22	01:32	01:42	01:11	01:07	01:21	<= 1:50 / 2 бали
Загальна кількість балів	8	7	6	4	6	8	7	6	8	

Рисунок 4.14 – Результати тестування на швидкодію

Назва ПЗ	Avast Premium Security	ESET SMART SECURITY	F-Secure SAFE	Avira Prime	Trend Micro	McAfee AntiVirus Plus	NORTON ANTIVIRUS	KASPERSKY SECURITY CLOUD	Bitdefender
Перевірка приватності додатків	Так	Так	Так	Так	Так	Так	Так	Так	Так
Функція фотографування викрадача	Ні	Так	Ні	Ні	Так	Так	Так	Так	Ні
Блокування небажаних викликів	Так	Так	Ні	Ні	Так	Так	Так	Так	Так
Функція знаходження загубленного пристрою	Так	Ні	Так	Ні	Так	Ні	Ні	Так	Так
Перевірка захисту WiFi	Так	Так	Ні	Ні	Так	Так	Так	Так	Так
Оцінка перевірених додатків в офіційному магазині	Так	Ні	Ні	Ні	Так	Ні	Так	Ні	Ні
Загальна кількість балів	**5**	**4**	**2**	**1**	**6**	**4**	**5**	**5**	**4**

Рисунок 4.15 – Результати тестування на захист

2. Було підсумовано бали за формулою (Швидкодія)/2 + (Захист).

Назва ПЗ	Avast Premium Security	ESET SMART SECURITY	F-Secure SAFE	Avira Prime	Trend Micro	McAfee AntiVirus Plus	NORTON ANTIVIRUS	KASPERSKY SECURITY CLOUD	Bitdefender
Бали швидкодія	8	7	6	4	6	8	7	6	8
Бали захист	5	4	2	1	6	4	5	5	4
Загальна кількість балів	9	7,5	5	3	9	8	8,5	8	8

Рисунок 4.16 – Підсумок результатів тестування

3. Результати тестування

Не рекомендованно до використання:

1. F-Secure SAFE;
2. Avira Prime;
3. ESET SMART SECURITY.

Рекомендованно до використання:

1. Avast Premium Security;
2. Trend Micro;
3. McAfee AntiVirus Plus;
4. NORTON ANTIVIRUS;
5. KASPERSKY SECURITY CLOUD;
6. Bitdefender.

Висновки за розділом 4

Було проведенно тестування популярного антивірусного ПЗ та надано рекомендації користувачам щодо вибору програмного забезпечення

ВИСНОВКИ

Хакери люблять орієнтуватися на мобільні пристрої, які багаті на особисті дані та інформацію про платіжні картки. Наші результати вказують на те, що розробники мобільних додатків часто нехтують безпекою, головним питанням є небезпечне зберігання даних. Інформація про користувача, що зберігається у чистому тексті, незамасковані дані на знімках екрана, а також ключі та паролі у вихідному коді - це лише деякі недоліки, які надають можливості кібератакам.

Самі користувачі можуть мимоволі сприяти компрометації своїх пристроїв, розширюючи можливості смартфонів, відключаючи захист, відкриваючи підозрілі посилання в SMS-повідомленнях та завантажуючи програмне забезпечення з неофіційних джерел. Захист даних користувачів вимагає відповідального ставлення як з боку розробників додатків, так і з боку власників пристроїв.

Також ми не можемо недооцінювати роль вразливостей серверів. Захист серверів мобільних додатків не кращий за захист клієнтів. У 2020 році, що дозволяє здійснювати різні атаки на користувачів, включаючи видавання себе за розробника у фішинг-листах, що ставить під загрозу репутацію розробника. Щоб запобігти використанню вразливостей сервера, ми рекомендуємо використовувати брандмауер веб-додатків (WAF).

Крім уразливості клієнта та сервера, ризики включають також зв'язок клієнт-сервер. Дані, надіслані через незахищений протокол, можуть бути повністю скомпрометовані. Але навіть безпечні зв’язки не завжди безпечні. Розробники ще мають глибоко зрозуміти важливість безпеки.

Механізми захисту є слабким місцем мобільних додатків. Більшість виявлених вразливих місць були виявлені на етапі проектування та є наслідком неможливості "продумати" питання, пов'язані з безпекою. Я рекомендую методичний підхід до розробки та забезпечення безпеки мобільних додатків, регулярно тестуючи його, починаючи з 1-го дня життєвого циклу програмного забезпечення.

Найефективнішим методом є тестування білих скриньок, при якому аналітики безпеки мають повний доступ до вихідного коду.

Отже метою данної дипломної роботи було проведення опису апаратної частини, нормативно правової бази та ОС мобільних пристроїв, а також характеристичних особливостей вразливостей та загроз для мобільних пристроїв. Огляд інструментів, які використовуються при захисті мобільних пристроїв, а також загальні рекомендації щодо роботи з мобільними банками. Завершальною частиною роботи був процесс тестування популярного антивірусного ПЗ та надання рекомендації користувачам щодо вибору програмного забезпечення.

Згідно з метою роботи всі завдання були успішно виконані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. FastTrack To Mobile and laptop Hardware [Електронний ресурс] – Режим доступу до документа: https://www.digit.in/technology-guides/fasttrack-to-mobile-and-laptop-hardware/unity-in-diversity.html

2. Методологія проектування та інструментарій для створення мобільних додатків. Вісник НТУ “ХПІ». 2013. No56(1029) 135 с.

3. RetoMeier. ProfessionalAndroid2. ApplicationDevelopment. –Wiley Publishing, Inc, 2010.

4. Грицунов О. В. Інформаційні системи та технології: навч. посіб. Для студентів за напрямом підготовки «Транспортні технології» / О. В. Грицунов; Харк. нац. акад. міськ. госп-ва. –Х.: ХНАМГ, 2010. 125-140 с.

5. Mobile Operating System Market Share Worldwide [Електронний ресурс] – Режим доступу до документа: https://gs.statcounter.com/os-market-share/mobile/worldwide

6. ДНТБ України [Електронний ресурс] – Режим доступу до документа: https://dntb.gov.ua/

7. FastTrack To Mobile and laptop Hardware [Електронний ресурс] – Режим доступу до документа: http://itzashita.ru/mobilnyie-ustroystva/bezopasnost-mobilnyih-ustroystv-sistem-i-prilozheniy-chast-1.html

8. В. А. Артамонов ПРОБЛЕМЫ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ, СИСТЕМ И ПРИЛОЖЕНИЙ [Електронний ресурс] – Режим доступу до документа: http://freeprotection.ru/mobilnaya-bezopasnost-vsyo-chto-nuzhno-znat/

9. Уязвимости платформы Android. Настоящее и будущее Блог компании Доктор Веб [Електронний ресурс] – Режим доступу до документа: https://habrahabr.ru/company/drweb/blog/142993/

10. Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of GDPR NOVEMBER 2017 ENISA

11. Importance of a BYOD Policy for Companies January 2, 2013 by Pierluigi Paganini [Електронний ресурс] – Режим доступу до документа: http://resources.infosecinstitute.com/byod-policy-for-companies/#gref

12. Beginner's Guide to BYOD

13. Jane McConnell Tracking the Trends in Bringing Our Own Devices to Work [Електронний ресурс] – Режим доступу до документа: https://hbr.org/2016/05/tracking-the-trends-in-bringing-our-own-devices-to-work

14. Dave Johnson BYOD alert: Confidential data on personal devices [Електронний ресурс] – Режим доступу до документа: https://www.cbsnews.com/news/byod-alert-confidential-data-on-personal-devices/

15. The Pros and Cons of Bring-Your-Own-Device (BYOD) for Your Mobile Field Workforce – Field Force Friday

16. What is BYOD (Bring Your Own Device) and Why Is It Important?

17. The Advantages and Disadvantages of BYOD [Електронний ресурс] – Режим доступу до документа: http://www.optimuslearningservices.com/blog/practical-ld/advantages-disadvantages-byod-in-learning/

18. The Good, The Bad, and the Ugly of Mobility and BYOD. Архів оригіналу за 27 квітень 2018.

19. BYOD in the Workplace: Benefits, Risks and Insurance Implications

20. Преимущества и недостатки политики BYOD [Електронний ресурс] – Режим доступу до документа: https://promodo.ua/blog/preimuschestva-i-nedostatki-politiki-byod.html

21. Технології захисту інформації [Електронний ресурс] – Режим доступу до документа: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

22. "Що таке мобільна безпека (бездротова безпека)? - Визначення з WhatIs.com". WhatIs.com.

23. "BYOD та збільшення загрози зловмисному програмному забезпеченню сприяють стимулюванню ринку послуг мобільного захисту в мільярди доларів у 2020 році". Дослідження ABI. 2013-03-29.