

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект рекомендації для підвищення рівня
захищеності мобільних додатків»

Виконав студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»

 Олександр ІЛЬНИЦЬКИЙ

Керівник старший викладач кафедри КІ та КБ

 Олександр ПРОГ

Рецензент старший викладач кафедри КІ та КБ

 Ігор ФАЛЬКОВСЬКИЙ

Житомир – 2024

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 125 «Кібербезпека»

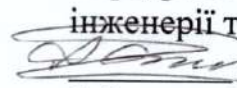
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Ільницький Олександр Сергійович

Тема роботи: «Проект рекомендації для підвищення рівня захищеності мобільних додатків»

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 10 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

вихідні дані для роботи;

Обладнання та програмне забезпечення:

1. Мобільний пристрій.
2. Appium.
3. Android Studio.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О.В.	5 березня	26 березня
2	Пірог О.В.	26 березня	20 квітня
3	Пірог О.В.	20 квітня	28 травня

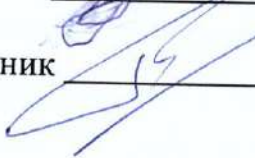
Студент  О. ІЛЬНИЦЬКИЙ

Керівник  О.ПІРОГ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	5 березня	
2	Пошук теоретичної інформації	26 березня	
3	Вибір програмного забезпечення для тестування	20 квітня	
4	Розробка плану тестування	30 квітня	
5	Проведення тестування	28 травня	
8	Оформлення пояснювальної записки	10 червня	

Студент  О. ІЛЬНИЦЬКИЙ

Керівник  О. ПІРОГ

АНОТАЦІЯ

Метою кваліфікаційної роботи є розробка рекомендацій для підвищення рівня захищеності мобільних додатків шляхом ідентифікації основних загроз, аналізу існуючих вразливостей, оцінки ефективності поточних методів захисту та впровадження нових підходів до безпеки.

Визначено основні завдання для підвищення захищеності мобільних додатків, включаючи ідентифікацію та класифікацію загроз і вразливостей, оцінку поточних методів захисту та їх ефективності, а також розробку рекомендацій для покращення безпеки мобільних додатків. Проаналізовано базові загрози, такі як віруси, шпигунські програми та мережеві атаки, а також вразливості в коді, ненадійне зберігання даних та недостатній захист мережевих з'єднань. Розглянуто особливості існуючих методів захисту, включаючи шифрування даних, багатофакторну аутентифікацію та регулярне тестування безпеки.

Показано розробку нових рекомендацій для покращення безпеки мобільних додатків, таких як впровадження кращих практик програмування, безпечне зберігання даних із використанням апаратного шифрування та вдосконалення механізмів аутентифікації, зокрема біометричної аутентифікації та динамічних паролів. Наведено результати тестування безпеки мобільних додатків за допомогою інструментів Appium та Android Studio.

Результати тестування показали, що впровадження запропонованих рекомендацій значно зменшило кількість вразливостей і підтвердило ефективність нових методів захисту на реальних додатках.

Висновки роботи свідчать про важливість системного підходу до безпеки мобільних додатків та підтверджують ефективність впроваджених рекомендацій у підвищенні їхньої захищеності.

Дипломна робота має обсяг 66 сторінок, містить 30 рисунків, 24 літературних джерел.

Ключові слова: Аналіз, безпека, мобільний додаток.

KKIK<.KP.B – 125 – 08 – ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата	Проект рекомендації для підвищення рівня захищеності мобільних додатків	Лім.	Арк.	Аркуші
Розроб.		Ільницький О.С.		29.06.24			4	70
Керівник		Пірог О.В.		29.06.24	ФІКТ, Гр. КБ-20-2			
Реценз.		Фальковський І.Г.		29.06.24				
Н. контр.		Пірог О.В.		29.06.24				
Затверд.		Сфіменко А.А.		29.06.24				

Дипломна робота має обсяг 60 сторінок, містить 30 рисунків, 24 літературних джерел.

Ключові слова: Аналіз, безпека, мобільний додаток.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ANNOTATION

The purpose of the qualification work is to develop recommendations for increasing the level of security of mobile applications by identifying the main threats, analyzing existing vulnerabilities, evaluating the effectiveness of current protection methods and implementing new approaches to security.

The main tasks for improving the security of mobile applications are defined, including the identification and classification of threats and vulnerabilities, the assessment of current protection methods and their effectiveness, as well as the development of recommendations for improving the security of mobile applications. Basic threats such as viruses, spyware and network attacks are analyzed, as well as vulnerabilities in code, insecure data storage and insufficient protection of network connections. Features of existing security methods are reviewed, including data encryption, multi-factor authentication, and regular security testing.

It shows the development of new recommendations for improving the security of mobile applications, such as implementing best programming practices, securely storing data using hardware encryption, and improving authentication mechanisms, including biometric authentication and dynamic passwords. The results of mobile application security testing using Appium and Android Studio tools are given.

The test results showed that the implementation of the proposed recommendations significantly reduced the number of vulnerabilities and confirmed the effectiveness of new protection methods on real applications.

The conclusions of the work indicate the importance of a systemic approach to the security of mobile applications and confirm the effectiveness of the implemented recommendations in increasing their security.

The thesis has a volume of 60 pages, contains 30 drawings, 24 literary sources.

Keywords: Analysis, security, mobile application.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 ТЕОРЕТИЧНИЙ АСПЕКТ	11
1.1 Обґрунтування значущості теми дослідження.....	11
1.2 Визначення та класифікація мобільних додатків, їх роль та значення в сучасному цифровому світі.	15
1.3 Аналіз потенційних загроз та ризиків, пов'язаних з використанням мобільних додатків.....	20
1.4 Правове регулювання в сфері мобільних додатків.....	24
РОЗДІЛ 2 РОЗРОБКА АБО НАЛУШТУВАННЯ СИСТЕМИ ЗАХИСТУ	27
2.1 Забезпечення безпеки мобільних додатків	27
2.2 Огляд методів які використовуються для аналізу мобільних додатків.....	31
2.3 Огляд інструментів аналізу безпеки мобільних додатків	42
РОЗДІЛ 3 ТЕСТУВАННЯ МОБІЛЬНИХ ДОДАТКІВ.....	53
3.1 Налаштування та проведення тестування.....	53
3.2 Рекомендації.....	64
ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	67

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

2FA - Двофакторна автентифікація

CI - Continuous Integration

CD - Compact Disc

iOS - iPhone OS

HTTP – HyperText Transfer Protocol

PDA - personal digital assistant

MFA – Multi-Factor Authentication

SSH – Secure Shell

SMTP – Simple Mail Transfer Protocol

IMAP – Internet Message Access Protocol

IP – Internet Protocol address

HTML –HyperText Markup Language

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Аналіз безпеки мобільних додатків є надзвичайно актуальною темою через постійне зростання використання мобільних додатків у повсякденному житті. Мобільні додатки обробляють величезні обсяги конфіденційних даних, таких як особиста інформація, фінансові дані та дані про здоров'я, що робить їх привабливою мішенню для кіберзлочинців. Уразливості в мобільних додатках можуть призвести до витоку даних, фінансових втрат та порушення конфіденційності користувачів. Крім того, законодавчі вимоги щодо захисту даних стають дедалі суворішими, і невідповідність цим вимогам може призвести до значних штрафів і втрати репутації. Усе це підвищує необхідність ретельного аналізу та забезпечення безпеки мобільних додатків.

Метою кваліфікаційної роботи "Проект рекомендації для підвищення рівня захищеності мобільних додатків" є розробка рекомендацій для підвищення рівня захищеності мобільних додатків шляхом ідентифікації основних загроз, аналізу існуючих вразливостей, оцінки ефективності поточних методів захисту та впровадження нових підходів до безпеки. Дослідження включає ідентифікацію загроз, таких як віруси, шпигунські програми та мережеві атаки, аналіз вразливостей у коді, ненадійного зберігання даних та захисту мережевих з'єднань, оцінку поточних методів захисту, таких як шифрування, багатофакторна аутентифікація та регулярне тестування безпеки, а також розробку нових рекомендацій для покращення безпеки мобільних додатків через впровадження кращих практик програмування, безпечного зберігання даних та покращення механізмів аутентифікації.

Визначена мета обумовлює наступні завдання:

- дослідження теоретичних відомостей безпеки мобільних додатків;
- огляд методів які використовуються для аналізу мобільних додатків;
- правове регулювання в сфері мобільних додатків;
- огляд інструментів аналізу;
- аналіз вибору програмного забезпечення Appium і Android Studio;
- налаштування, тестування Appium і Android Studio;

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

- надання користувачам рекомендацій з метою підвищення захисту мобільних додатків;

Об’єктом дослідження є мобільні додатки та їх захищеність від різноманітних загроз і вразливостей. Дослідження включає аналіз загроз, таких як віруси, шпигунські програми та мережеві атаки, а також оцінку вразливостей, що можуть виникнути у процесі розробки, зберігання даних та передачі інформації у мобільних додатках.

Предметом дослідження є підвищення рівня захищеності мобільних додатків шляхом ідентифікації основних загроз, аналізу існуючих вразливостей, оцінки ефективності поточних методів захисту та впровадження нових підходів до безпеки.

Методологія роботи. Під час дослідження було використано загальнонаукові та емпіричні наукові методи, що ґрунтуються на системному підході, такі як абстрагування, аналіз, синтез, порівняння, узагальнення, систематизація, методи експерименту та спостереження.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних літературних джерел та додатку. Основний зміст роботи викладено на 68 сторінках друкованого тексту. Робота містить 30 рисунків. Список використаної літератури налічує 24 джерела, що викладені на 2 сторінках.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНИЙ АСПЕКТ

1.1 Обґрунтування значущості теми дослідження

Мобільні додатки стали невід'ємною частиною сучасного цифрового світу, відіграючи ключову роль у багатьох аспектах життя. Вони забезпечують зручний доступ до інформації, послуг та розваг, сприяють ефективній комунікації та співпраці, а також підтримують особисту та професійну продуктивність. Мобільні додатки дозволяють користувачам здійснювати фінансові операції, стежити за здоров'ям, навчатися новим навичкам і залишатися на зв'язку з друзями та родиною.

Зростання популярності мобільних додатків робить їх привабливою мішенню для кіберзлочинців. Вразливість мобільних додатків може призвести до витоку чутливої інформації, такої як особисті дані, фінансова інформація, дані про здоров'я, що може мати серйозні наслідки для користувачів, як крадіжка особистості, фінансові втрати, пошкодження репутації та шантаж.

Мобільні додатки також можуть використовуватися для поширення шкідливого програмного забезпечення, що може пошкодити мобільні пристрої, красти дані або шпигувати за користувачами. Крім того, вони можуть бути мішенню для кібератак, які можуть призвести до збоїв у роботі мобільних мереж, вебсайтів або інших онлайн-сервісів.

Кібератаки на мобільні додатки також можуть завдати шкоди репутації компаній та організацій, які їх розробляють, а також національним інтересам, якщо йдеться про мобільні додатки, що використовуються урядами або критичною інфраструктурою.

Зловмисники постійно розробляють нові методи атак, використовуючи вразливості мобільних додатків для крадіжки особистих даних, фінансової інформації, а також для поширення шкідливого програмного забезпечення. Це може призвести до серйозних наслідків для користувачів, таких як фінансові втрати, втрата репутації, порушення конфіденційності та навіть шкода здоров'ю.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Пандемія COVID-19 суттєво вплинула на наше життя, значно збільшивши залежність від мобільних додатків. Це явище має як позитивні, так і негативні наслідки, що стали очевидними протягом останніх років. З одного боку, зростання використання мобільних додатків призвело до значного підвищення зручності та ефективності роботи, навчання, спілкування та доступу до різноманітних послуг. З іншого боку, це також створило нові кіберзагрози та виклики для безпеки мобільних додатків, які потребують негайного вирішення.

Одним із найважливіших позитивних аспектів є зручність та ефективність, яку забезпечили мобільні додатки. У сфері роботи зросла кількість використання таких платформ, як Zoom, Microsoft Teams та Slack, що дозволило людям працювати дистанційно з будь-якого місця. Це знизило потребу в фізичній присутності в офісі, забезпечуючи гнучкість та можливість підтримки робочого процесу під час карантинних обмежень. У сфері освіти освітні платформи, як-от Google Classroom і Moodle, надали можливість дистанційного навчання, що дозволило студентам та учням продовжувати своє навчання, незважаючи на закриття навчальних закладів. Для спілкування мобільні додатки, такі як WhatsApp, Facebook Messenger та Viber, допомогли людям залишатися на зв'язку з рідними та друзями, незважаючи на обмеження пересування. Крім того, додатки для доставки їжі покупок та медичних консультацій стали надзвичайно популярними, забезпечуючи доступ до важливих послуг без необхідності виходити з дому.

Із збільшенням використання мобільних додатків зросли й кіберзагрози. Хакери активно намагалися скористатися збільшеною кількістю користувачів та новими додатками, поширюючи шкідливе програмне забезпечення та фішингові атаки. Це створило серйозні проблеми для кібербезпеки, адже велика кількість людей працювала з чутливою інформацією через інтернет. Приватність даних також стала важливою проблемою, оскільки більша кількість особистої інформації стала зберігатися в мобільних додатках. Витоки даних та неналежне використання персональної інформації стали поширеними проблемами, які потребують ретельного

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

вирішення. Надійність додатків також викликала занепокоєння, оскільки багато нових додатків були створені в прискореному темпі, що часто призводило до помилок в їх розробці та створювало вразливості.

Війна в Україні загострила проблему кіберзагроз на мобільні додатки, і зловмисники активно використовують цю ситуацію для проведення кібератак з метою завдання шкоди українцям, їхнім даним та інфраструктурі. Кіберзлочинці можуть розповсюджувати шкідливе програмне забезпечення через мобільні додатки, щоб шпигувати за українцями, красти їхні дані або навіть виводити з ладу критичну інфраструктуру. Вони також створюють фейкові мобільні додатки або веб-сайти, щоб обманом змусити ввести свої особисті дані або дані банківських карток. Використовуючи соціальну інженерію, зловмисники можуть обманом змусити українців встановити шкідливі мобільні додатки або розкрити свої дані, а атаки на мобільні мережі перешкоджають спілкуватися, отримувати доступ до інформації або користуватися важливими послугами.

Ці ситуації викликають серйозні побоювання щодо безпеки особистих даних та фінансових ресурсів громадян. У період війни та інших кризових ситуацій громадяни стають значно вразливішими до атак кіберзлочинців.

Зростання кількості кібератак на мобільні додатки, що використовуються для спілкування, банківських операцій та доступу до інших важливих послуг, призводить до витоків особистої інформації, фінансових втрат та психологічного стресу. Крім того, загрози, пов'язані з втратою контролю над мобільними пристроями, можуть мати далекосяжні наслідки для безпеки та добробуту громадян.

Ці небезпеки підкреслюють необхідність посиленої уваги до кібербезпеки та впровадження заходів, спрямованих на захист особистих даних і фінансових ресурсів.

Незважаючи на ці виклики, є також і перспективи для розвитку безпеки мобільних додатків. Розробники постійно працюють над вдосконаленням методів захисту та виявлення вразливостей своїх додатків. За останні кілька років індустрія мобільних додатків бачила значний прогрес у сфері безпеки, включаючи розробку

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

нових інструментів для аналізу коду, підпису та шифрування даних, аутентифікації користувачів та механізмів контролю доступу. Технології шифрування даних стають все більш ефективними, забезпечуючи високий рівень захисту конфіденційної інформації під час передачі та зберігання на мобільних пристроях. Крім того, регулярні оновлення та патчі від розробників додатків і виробників операційних систем дозволяють вчасно виправляти виявлені вразливості та запобігати новим атакам.

Розвиток технологій штучного інтелекту (ШІ) також відіграє важливу роль у покращенні безпеки мобільних додатків. ШІ може використовуватися для аналізу великих обсягів даних та виявлення аномальних патернів, що можуть свідчити про атаки або зловмисну поведінку. Машинне навчання і алгоритми інтелектуального аналізу даних дозволяють розробникам створювати більш ефективні системи виявлення і запобігання загрозам безпеці.

За останні кілька років значно зросла увага до питань захисту приватності користувачів мобільних додатків. Регуляторні органи по всьому світу активно втручаються у сферу обробки особистих даних та встановлюють суворі вимоги до збору, зберігання та обробки особистої інформації. Це ставить перед розробниками мобільних додатків вимогу розробки додатків, які відповідають найвищим стандартам захисту приватності та дотримання вимог регуляторних органів.

Крім того, зростає популярність розробки мобільних додатків з використанням блокчейн технологій. Блокчейн забезпечує високий рівень безпеки та недоступності даних для зловмисників завдяки своїм принципам розподіленої бази даних та шифрування інформації. Мобільні додатки, побудовані на базі блокчейн технологій, можуть забезпечити користувачам максимальний рівень захисту їхніх особистих даних та транзакцій.

Не можна не згадати і про активну роль спільноти та професійних організацій у забезпеченні безпеки мобільних додатків. Велика кількість відкритих джерел, форумів, конференцій та професійних спілок сприяє обміну досвідом та кращими практиками в галузі безпеки програмного забезпечення. Регулярні аудити безпеки,

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

участь у відкритих програмах багфіндингу та співпраця зі спеціалізованими фірмами по аудиту та тестуванню допомагають розробникам підтримувати високий рівень безпеки своїх додатків.

Розвиток та підтримка безпеки мобільних додатків є важливим завданням для всіх учасників цього екосистеми, від розробників і виробників до користувачів і регуляторів. Зусилля в напрямку покращення безпеки дозволять забезпечити стабільний та надійний розвиток мобільних технологій, забезпечуючи захист інформації та приватності користувачів у цьому цифровому віці.

Отже, безпека мобільних додатків є актуальною та важливою проблемою, яка потребує постійного уваги та вдосконалення. Зростаюча кількість загроз та атак, різноманітність платформ та операційних систем, а також вимоги до захисту приватності користувачів ставлять перед розробниками та виробниками мобільних додатків великі виклики. Проте розвиток нових технологій, активна участь спільноти та впровадження кращих практик безпеки дозволяють нам сприймати ці виклики як можливості для забезпечення надійного та безпечного середовища для користувачів мобільних додатків.

1.2 Визначення та класифікація мобільних додатків, їх роль та значення в сучасному цифровому світі.

Мобільні додатки — це програмне забезпечення, розроблене для використання на смартфонах, планшетах та інших мобільних пристроях. Вони можуть бути представлені у вигляді ігор, інструментів для продуктивності, соціальних мереж, освітніх ресурсів тощо.

Розвиток мобільних додатків відображає значний прогрес у технологіях, який відбувся протягом останніх десятиліть. Від простих програм до сучасних багатофункціональних додатків, їх еволюція демонструє як зміну технологій, так і розвиток потреб користувачів.

Перші мобільні додатки з'явилися на початку 90-х років. У 1993 році IBM представила перший мобільний додаток для смартфонів на своїй пристрої IBM

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Simon. Цей додаток включав прості функції, такі як календар, адресна книга і калькулятор.

Значний прогрес був досягнутий у середині 90-х з появою Palm OS, яка була розроблена для персональних цифрових помічників (PDA). Palm OS включала сенсорний інтерфейс та базові додатки, а також підтримку сторонніх додатків.

У кінці 90-х років був розроблений протокол WAP (Wireless Application Protocol), який дозволив мобільним пристроям підключатися до Інтернету. Це було значним кроком вперед, що дало можливість створювати більш складні мобільні додатки.

У 2000-х роках розвиток мобільних додатків прискорився завдяки появі смартфонів на базі Symbian OS, яка стала однією з найбільш поширених операційних систем для мобільних пристроїв до 2008 року. Nokia та інші виробники активно використовували цю платформу у своїх пристроях.

У 2007 році Apple представила iPhone, який став революційним пристроєм завдяки своєму інтуїтивно зрозумілому інтерфейсу та широким можливостям для розробників додатків. У 2008 році Apple запустила App Store, що значно спростило доступ до додатків і зробило їх популярними серед користувачів.

Поява Android в 2008 році додала новий імпульс розвитку мобільних додатків. Відкритість платформи Android дозволила багатьом розробникам створювати додатки, що сприяло швидкому зростанню кількості доступних програм.

Протягом 2010-х років мобільні додатки стали невід'ємною частиною життя людей по всьому світу. З'явилися численні спеціалізовані додатки для соціальних мереж, банківських послуг, здоров'я та фітнесу, ігор, подорожей, покупок та новин.

Зараз мобільні додатки продовжують розвиватися, стаючи все більш інтегрованими з іншими технологіями, такими як IoT, AI та AR, що відкриває нові можливості для користувачів та бізнесу.

Але разом з їх розвитком виникли і численні загрози, які ставлять під загрозу безпеку даних користувачів, конфіденційність та навіть фізичну безпеку. Мобільне

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

шкідливе програмне забезпечення, таке як віруси, трояни, шпигунські програми та програми-вимагачі, стало великою загрозою. Ці програми можуть красти особисті дані, фінансову інформацію, контакти та інші конфіденційні дані. Шкідливе ПЗ часто поширюється через підроблені або заражені додатки, які користувачі завантажують зі сторонніх джерел або навіть офіційних магазинів додатків.

Фішинг через мобільні додатки є ще однією серйозною загрозою. Зловмисники створюють фейкові додатки або надсилають шкідливі посилання через повідомлення, щоб обманом змусити користувачів ввести свої облікові дані або іншу конфіденційну інформацію. Соціальна інженерія також використовується для отримання доступу до пристроїв користувачів, шляхом обману або маніпуляції.

З моменту створення мобільних додатків було кілька відомих атак, які мають великий вплив на безпеку та конфіденційність користувачів. Ось кілька з найбільш відомих які відбулись недавно:

- 2015 рік Stagefright - вразливість в Android, що дозволяла зловмисникам віддалено виконувати код через надсилання спеціально сформованого мультимедійного повідомлення (MMS).
- 2015 рік XcodeGhost - ця атака стосувалася розробки мобільних додатків на iOS. Зловмисні розробники вбудовували шкідливий код у додатки, які були створені за допомогою компрометованої версії розробницького середовища Xcode.
- 2007-2011 рік JailbreakMe - ця атака використовувала вразливості в iOS для отримання доступу до адміністративних привілеїв на пристроях, що дозволяло користувачам обходити захист та встановлювати неофіційне програмне забезпечення.
- 2016 рік HummingBad - це була широко розповсюджена кампанія Android-малвару, яка здійснювала уразливості в ОС для отримання контролю над пристроями та відправки шкідливої реклами.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

- 2019 рік StrandHogg - ця атака використовувала вразливість в Android, щоб вивести користувачів з легітимних додатків на фальшиві, які виглядали майже ідентично, для збору облікових даних.
- 2017 рік WannaCry - був в основному спрямований на комп'ютери, він також вплинув на деякі мобільні пристрої, особливо ті, що використовують застарілі версії Windows.

Такі приклади атак на мобільні додатки демонструють кілька ключових висновків щодо безпеки. Операційні системи мобільних пристроїв мають серйозні уразливості, які можуть використовувати зловмисники для віддаленого виконання коду або отримання привілеїв. Забезпечення безпеки інструментів розробки є критично важливим для запобігання вбудовуванню шкідливого коду в додатки. Використання неофіційних додатків та прошивок збільшує ризик інфікування шкідливим ПЗ. Зловмисники також використовують соціальні методи, такі як створення фальшивих додатків, для збору облікових даних. Нарешті, своєчасне оновлення операційних систем та додатків є необхідним для захисту від відомих вразливостей.

З ростом кількості мобільних пристроїв збільшується і потреба в розробці додатків. Щодня створюються сотні мобільних додатків, які роблять роботу з мобільним пристроєм більш комфортною. Існує кілька типів додатків, які використовують розробники.

Є декілька видів мобільних додатків:

- Нативні додатки
- Мобільні веб-додатки
- Гібридні додатки

Нативні додатки - ці додатки називають нативними тому, що вони написані рідною (з англ. Native – рідна) для певної платформи мовою програмування. Для Android цією мовою є Java, тоді як для iOS – objective-C або Swift.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Нативні додатки знаходяться на самому пристрої, доступ до яких можна отримати, натиснувши на іконку. Вони встановлюються через магазин додатків (Play Market на Android, App Store на iOS та ін.).

Вони розроблені спеціально для конкретної платформи і можуть використовувати всі можливості пристрою – камеру, GPS-датчик, акселерометр, компас, список контактів та все інше. Також вони можуть розпізнавати стандартні жести, встановлені операційною системою або зовсім нові жести, які використовуються в конкретному додатку.

Мобільні веб-додатки - насправді мобільні веб-додатки не є додатками, як такими. Адже справа в тому, що веб-додаток, по суті, являє собою сайт, який адаптований і оптимізований під будь-який смартфон. І для того, щоб скористатися ним, достатньо мати на пристрої браузер, знати його адресу та увімкнути інтернет-з'єднання (завдяки йому відбувається оновлення інформації в даному виді додатків).

Запускаючи мобільні веб-додатки, користувач виконує всі ті дії, які він виконує при переході на будь-який веб-сайт, а також отримує можливість «встановити» їх на свій робочий стіл, створивши закладку сторінки веб-сайту.

Веб-додатки відрізняються кроссплатформеністю, тобто здатні функціонувати, незалежно від платформи девайса. Козирем в їх рукаві виступає і те, що вони не використовують його програмне забезпечення. А через те, що є мобільною версією сайту з розширеним інтерактивом, веб-додатки не відбирають дорогоцінне місце в пам'яті смартфона.

Веб-додатки стали широко популярні в той час, коли почав розвиватися HTML5 і люди усвідомили, що можуть отримати доступ до безлічі функцій нативних додатків, просто зайшовши на веб-сайт через звичайний браузер. На сьогоднішній день складно сказати, де саме розташовується чітка межа між веб-додатками і звичайними веб-сторінками, оскільки функціонал HTML5 зростає з кожним днем і все більше і більше сайтів його використовують.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Гібридні додатки - являють собою поєднання веб і нативних додатків. Особливо, мається на увазі їх кроссплатформеність та доступ до функціоналу смартфона. Такі додатки можуть бути завантажені виключно з маркетів на кшталт Google Play і App Store. Разом з тим вони мають у своєму розпорядженні опцію автономного оновлення інформації, а для їх роботи необхідне інтернет-підключення. Без наявності останнього веб-функції просто не працюють.

Серед багатьох компаній вибір найчастіше падає на розробку саме гібридного додатка. Це можна пояснити тим, що гібридні програми здатні поєднувати переваги нативних з технологічною актуальністю, яка забезпечується останніми веб-технологіями. Однак, на відміну від нативних, вартість створення гібридних на порядок нижче, а його швидкість – вище. Спорідненість гібридних додатків з веб-додатками, в свою чергу, дає плоди у вигляді того, що в них можна легко і оперативно вносити корективи. Тобто розробникам не доводиться, як у випадку з нативними, повторно розміщувати додаток в магазині заради усунення помилок попередньої версії.

Таким чином було досліджено основні теоретичні поняття, такі як мобільні додатки, їх класифікацію, роль та значення в нашому світі. Вони стали важливою частиною нашого життя, пропонуючи широкий спектр функцій від розваг до робочих інструментів. Їх класифікація варіюється від ігор до фінансів, залежно від їхньої функціональності. Однак з їхнім зростанням з'явилися і кіберзагрози, що підкреслює важливість безпечного користування та захисту даних.

1.3 Аналіз потенційних загроз та ризиків, пов'язаних з використанням мобільних додатків.

Використання мобільних додатків супроводжується різноманітними загрозами та ризиками, які можуть вплинути на безпеку користувачів та їхніх даних. Основні ризики включають небезпечні дозволи, які додатки запитують для доступу до функцій пристрою, що може призвести до витоку конфіденційної інформації. Завантаження додатків з ненадійних джерел може встановити шкідливе ПЗ, яке ви-

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

крадає особисті дані, проводить шахрайські операції або пошкоджує пристрій. Уразливості в додатках, як-от SQL-ін'єкції чи XSS-атаки, можуть бути використані зловмисниками. Фішингові атаки та соціальна інженерія можуть обманом змусити користувачів надати свої конфіденційні дані. Багато додатків збирають та передають особисті дані без явної згоди користувачів, що порушує конфіденційність. Використання сторонніх бібліотек та SDK може містити уразливості або шкідливий код. Небезпечні мережі можуть призвести до перехоплення даних зловмисниками. Деякі додатки можуть здійснювати несанкціоновані фінансові операції, що створює фінансові ризики. Соціальні мережі та месенджери можуть сприяти кібербулінгу, поширенню неправдивої інформації або порушенню соціальних норм.

Потенційні загрози безпеки:

- Шкідливе програмне забезпечення
- Вразливості в операційних системах та додатках
- Фішинг та соціальна інженерія
- Несанкціонований доступ
- Недостатній захист даних



Рис. 1 – Потенційні загрози безпеки мобільних додатків

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Шкідливе програмне забезпечення – це одна з найбільших загроз при використанні мобільних додатків. Воно включає віруси, троянські програми, шпигунські програми, рекламне ПЗ, вимагачів та бекдори.

Шкідливе програмне забезпечення працює так, віруси поширюються на інші файли, трояни маскуються під легітимне ПЗ, шпигунські програми збирають інформацію про користувача, рекламне ПЗ показує небажану рекламу, вимагачі блокують доступ до пристрою або шифрують дані, а бекдори створюють приховані входи до системи. Шкідливе ПЗ поширюється через завантаження з ненадійних джерел, фішингові атаки та вразливості в додатках. Воно може викрадати особисті дані, призводити до фінансових втрат, пошкоджувати пристрої та дані, порушувати конфіденційність.

Вразливості в операційних системах та додатках - це слабкі місця або дефекти у програмному забезпеченні, які можуть бути використані зловмисниками для несанкціонованого доступу, атаки на пристрої або крадіжки конфіденційної інформації.

Вразливості можуть виникнути через помилки в коді програм, несанкціоновані зміни конфігурації, використання застарілих версій програмного забезпечення або недостатню увагу до безпеки під час розробки програми. Зловмисники можуть використовувати ці вразливості для здійснення різних видів атак, таких як введення в оман, викрадення даних або встановлення шкідливих програм на пристрої користувачів.

Фішинг - це вид атаки, при якому зловмисники намагаються отримати конфіденційну інформацію, таку як паролі, логіни або банківські дані, шляхом введення потенційних жертв в оманливі дії. Фішинг може включати відправлення підроблених електронних листів, повідомлень в соціальних мережах або створення підроблених веб-сайтів, що виглядають як відомі та довірені джерела, з метою змусити людей надавати свої особисті дані.

Соціальна інженерія - це процес маніпулювання людьми з метою отримання конфіденційної інформації або доступу до системи. Соціальна інженерія може

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

включати використання психологічних та соціальних методів для переконання людей здійснити певні дії, такі як розкриття паролів, надання доступу до захищеної інформації або встановлення шкідливого програмного забезпечення.

Несанкціонований доступ - це незаконне або несанкціоноване отримання доступу до інформації чи функціональності мобільного додатка без згоди користувача або власника додатка. Несанкціонований доступ може включати отримання доступу до особистих даних користувача, таких як контакти, повідомлення, фотографії або місцезнаходження, а також використання додатка для введення в оман інших користувачів чи виконання шкідливих дій на їхніх пристроях. Несанкціонований доступ до мобільних додатків може відбуватися через вразливості в програмному забезпеченні, неявне збирання даних або атаки на сервери, що зберігають інформацію користувачів.

Недостатній захист даних - це ситуація, коли конфіденційна інформація не має належного рівня захисту від несанкціонованого доступу чи втрати. Недостатній захист даних може бути викликано використанням слабких алгоритмів шифрування, неправильним налаштуванням систем безпеки, недостатнім контролем доступу до даних або недбалістю в управлінні інформаційною безпекою. Недостатній захист даних може призвести до витоку конфіденційної інформації, крадіжки особистих даних користувачів, фінансових втрат або пошкодження репутації компаній чи організацій.

Узагальнюючи, шкідливе програмне забезпечення та вразливості в операційних системах та додатках є серйозними загрозами для безпеки мобільних додатків, оскільки вони можуть спричинити крадіжку особистих даних, фінансові втрати та пошкодження пристроїв.

Для зниження ризиків користувачам рекомендується завантажувати додатки лише з офіційних магазинів (Google Play, App Store), ретельно перевіряти дозволи, оновлювати операційну систему та додатки, використовувати антивірусне ПЗ, бути обережними з підозрілими посиланнями та повідомленнями.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Також запобігання таких проблем необхідно використовувати сучасні методи шифрування, належно налаштовувати системи безпеки, встановлювати строгий контроль доступу до даних та проводити регулярну перевірку та аудит безпеки.

1.4 Правове регулювання в сфері мобільних додатків.

Правове регулювання в сфері мобільних додатків є важливою складовою цифрового правового простору України. З розвитком технологій та поширенням смартфонів та інших мобільних пристроїв, використання мобільних додатків стає все більш поширеним в різних сферах життя, таких як комунікація, фінанси, здоров'я, освіта та багато інших. Однак разом із зростанням популярності мобільних додатків виникають питання щодо їхнього правового статусу, захисту прав користувачів, конфіденційності даних та відповідальності розробників.

Українське законодавство щодо мобільних додатків базується на загальних принципах правової системи країни, а також на міжнародних нормативних актах, зокрема у сфері захисту персональних даних та інформаційної безпеки. Основні аспекти правового регулювання мобільних додатків включають в себе норми щодо захисту авторських прав на програмне забезпечення, відповідальності за порушення прав користувачів, вимог до зберігання та обробки персональних даних, а також правила рекламної діяльності в мобільних додатках.

Одним з ключових аспектів правового регулювання є захист авторських прав на програмне забезпечення. Українське законодавство передбачає, що програмне забезпечення, як і будь-яке інше творіння інтелектуальної власності, підлягає захисту відповідно до закону про авторське право. Це означає, що розробники мобільних додатків мають право на власні авторські права на свої програми, а також можуть вимагати відповідної охорони від будь-яких спроб їхнього незаконного використання чи копіювання.

Крім того, правове регулювання мобільних додатків включає в себе вимоги щодо захисту прав користувачів. Законодавство України передбачає, що користувачі мають право на захист своєї конфіденційної інформації та персональних даних,

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

які можуть бути зібрані та оброблені мобільними додатками. Розробники зобов'язані надавати користувачам достатньо інформації про те, як їхні дані будуть використовуватися, і отримувати згоду користувачів на обробку їхніх персональних даних відповідно до вимог законодавства.

Окрім того, мобільні додатки також підлягають регулюванню у сфері реклами. Українське законодавство містить вимоги щодо обмеження рекламних матеріалів у мобільних додатках, зокрема заборону реклами товарів або послуг, які обманюють споживачів або порушують їхні права. Рекламні матеріали в мобільних додатках повинні відповідати загальним принципам чесності та правдивості, а також не можуть містити непристойний контент чи спонсорську інформацію, яка не позначена відповідним чином.

Крім того, українське законодавство також передбачає відповідальність за порушення правил використання мобільних додатків. Розробники можуть бути притягнуті до відповідальності за незаконне використання програмного забезпечення, порушення прав користувачів, недотримання вимог щодо захисту персональних даних або розповсюдження шкідливого вмісту через мобільні додатки. Законодавство передбачає штрафні санкції, а також можливість позову на відшкодування завданих збитків у разі порушення прав користувачів або завдання шкоди третім особам через використання мобільних додатків.

Важливим аспектом правового регулювання мобільних додатків є також міжнародна співпраця в галузі інформаційної безпеки та боротьби з кіберзлочинністю. Україна активно співпрацює з іншими країнами та міжнародними організаціями у сфері захисту даних та боротьби з кіберзлочинністю, що дозволяє вдосконалювати національне законодавство та впроваджувати нові механізми захисту інформації в мобільних додатках.

На фоні швидкого розвитку технологій та поширення мобільних додатків, правове регулювання цієї сфери постійно вдосконалюється та адаптується до нових викликів і загроз. Однак необхідно звернути увагу на деякі проблеми, що виникають у контексті правового регулювання мобільних додатків.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Перш за все, необхідно удосконалювати механізми контролю за діяльністю розробників мобільних додатків та забезпеченням виконання ними вимог щодо захисту персональних даних та прав користувачів. У багатьох випадках виявляються порушення в цій сфері, що може призвести до серйозних наслідків для безпеки та конфіденційності користувачів.

Крім того, важливо забезпечити доступність та зрозумілість правил використання мобільних додатків для кінцевих користувачів. Часто умови користування мобільними додатками містять складні та непонятні положення, що може призвести до недорозумінь та конфліктів між розробниками та користувачами.

Також необхідно звернути увагу на питання захисту інтелектуальної власності у сфері мобільних додатків. Завдяки швидкому розвитку технологій, виникає явлення швидкого копіювання та підміни програмного забезпечення, що може призвести до порушення авторських прав та втрати доходів для оригінальних розробників.

Узагальнюючи, правове регулювання в сфері мобільних додатків в Україні є важливою складовою цифрової економіки та інформаційного суспільства. Воно забезпечує захист прав користувачів, конфіденційність даних та захист інтелектуальної власності, що сприяє розвитку цифрових технологій та забезпеченню безпеки та довіри до мобільних додатків. Однак для подальшого розвитку цієї сфери необхідно постійно вдосконалювати законодавство та механізми контролю за діяльністю розробників, зокрема у сферах захисту персональних даних, прав користувачів та інтелектуальної власності.

Висновок до першого розділу

Результати дослідження підкреслюють загальну вразливість мобільних додатків у сучасному цифровому середовищі. Насамперед, воно підкреслює потенційні загрози, які існують як для індивідуальних користувачів, так і для організацій, які використовують мобільні додатки у своїй діяльності.

Мобільне шкідливе програмне забезпечення, фішинг та витік конфіденційної інформації - це лише деякі з проблем, з якими стикаються користувачі мобільних

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

додатків. Ці загрози можуть призвести до втрати особистої інформації, фінансових втрат, а також до порушення робочих процесів та конфіденційності даних у бізнесі.

Для забезпечення безпеки мобільних додатків важливо вживати комплексний підхід, що включає в себе як технічні, так і організаційні заходи. Це включає аудит безпеки програмного забезпечення, регулярне оновлення програм та операційних систем, навчання користувачів основам кібербезпеки, а також впровадження механізмів моніторингу та реагування на потенційні загрози.

Безпека мобільних додатків є важливою складовою загальної кібербезпеки в цифровому світі. Забезпечення високого рівня безпеки мобільних додатків потребує спільних зусиль розробників, постачальників послуг та кінцевих користувачів. Тільки колективні дії можуть допомогти запобігти серйозним наслідкам, які можуть виникнути внаслідок недостатньої уваги до безпеки мобільних додатків.

РОЗДІЛ 2 РОЗРОБКА АБО НАЛУШТУВАННЯ СИСТЕМИ ЗАХИСТУ

2.1 Забезпечення безпеки мобільних додатків

Забезпечення безпеки мобільних додатків є критично важливим завданням у сучасному цифровому світі, де мобільні пристрої стають все більш важливою складовою нашого повсякденного життя. Поширення мобільних технологій сприяло значному зростанню у користуванні мобільними додатками у всьому світі. Від комунікації до розваг, від банківських транзакцій до бізнес-процесів - мобільні додатки стали невід'ємною частиною нашого життя.

Проте, разом із зростанням популярності мобільних додатків, збільшується і загроза їхньої безпеки. Хакерські атаки, витоки даних, вразливості безпеки - це лише деякі з проблем, з якими стикаються розробники та користувачі мобільних додатків. Тому забезпечення високого рівня безпеки мобільних додатків стає надзвичайно важливим завданням для компаній та розробників.

З метою забезпечення безпеки мобільних додатків рекомендується дотримуватися цілого ряду кроків та передових практик, що охоплюють усі аспекти процесу розробки, впровадження та експлуатації мобільних додатків.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Однією з перших і ключових задач при розробці мобільного додатка є аналіз потенційних загроз безпеці. Це включає в себе ідентифікацію та розуміння потенційних ризиків, які можуть виникнути під час розробки та експлуатації додатка. Розробники повинні враховувати різні аспекти додатка, включаючи його функціональність, обробку даних, взаємодію з сервером та інтерфейс користувача.

Після аналізу потенційних загроз безпеці необхідно провести оцінку ризиків. Це означає визначення ймовірності та наслідків потенційних загроз для безпеки додатка та його користувачів. Оцінка ризиків дозволяє визначити найбільш серйозні та найбільш ймовірні загрози, що допомагає розробникам приділити особливу увагу їх вирішенню.

На наступному етапі розробники повинні визначити та впровадити відповідні заходи безпеки для зменшення виявлених ризиків. Це може включати в себе широкий спектр технічних, організаційних та процедурних заходів, призначених для забезпечення високого рівня безпеки мобільного додатка та його користувачів. Серед таких заходів можуть бути механізми шифрування даних, обмеження доступу до конфіденційної інформації, використання механізмів аутентифікації, а також регулярні аудити безпеки.

Після впровадження заходів безпеки важливо проводити регулярні аудити та тестування безпеки мобільного додатка. Це дозволяє виявляти нові вразливості та оцінювати ефективність застосованих заходів безпеки. Такі аудити можуть бути проведені як внутрішніми експертами з безпеки, так і залученими зовнішніми аудиторами.

Однією з ключових аспектів забезпечення безпеки мобільних додатків є захист особистих даних користувачів. Із зростанням кількості особистих даних, які обробляються мобільними додатками, зростає і відповідальність розробників за їхню безпеку. Зокрема, це стосується конфіденційної інформації, такої як ім'я та прізвище користувача, адреса електронної пошти, номери телефонів, фінансова інформація та інші особисті дані, які можуть бути використані для ідентифікації конкретної особи.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Одним із способів захисту особистих даних користувачів є використання механізмів шифрування. Шифрування даних забезпечує конфіденційність та цілісність інформації, запобігаючи її несанкціонованому доступу чи модифікації. Розробники мобільних додатків повинні використовувати сучасні алгоритми шифрування для захисту особистих даних, зберігаючи їх у зашифрованому вигляді як в процесі передачі, так і зберігання на серверах.

Ще одним важливим аспектом є забезпечення безпеки взаємодії мобільного додатка з сервером. Всі дані, що передаються між мобільним додатком та сервером, повинні бути зашифрованими, щоб запобігти їхньому перехопленню або зміні. Для цього рекомендується використовувати протоколи забезпечення безпеки на транспортному рівні, такі як SSL або TLS, які забезпечують шифрування даних під час їхньої передачі через мережу Інтернет.

Окрім технічних заходів безпеки, важливо також приділяти увагу соціальним аспектам забезпечення безпеки мобільних додатків. Наприклад, розробники повинні стимулювати користувачів до використання безпечних паролів та інших методів аутентифікації, щоб запобігти несанкціонованому доступу до їх облікових записів. Також важливо включати в додаток засоби повідомлення та навчання користувачів щодо безпечних практик використання додатка та захисту їхніх особистих даних.

Крім того, важливим аспектом забезпечення безпеки мобільних додатків є вчасне виявлення та виправлення вразливостей. Регулярні аудити та тестування безпеки дозволяють виявляти нові вразливості та вживати заходів для їхнього усунення. Крім того, розробники мають використовувати оновлення додатків для виправлення виявлених вразливостей та забезпечення безпеки користувачів.

У зв'язку з постійним розвитком технологій та зміною умов на ринку мобільних додатків, забезпечення безпеки стає неперервним процесом, що вимагає постійного вдосконалення та адаптації. Розробники мобільних додатків повинні слідкувати за останніми тенденціями в галузі безпеки, вдосконалювати свої навички та

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

знання, а також впроваджувати нові методи та технології для забезпечення безпеки своїх додатків.

Нарешті, важливим аспектом забезпечення безпеки мобільних додатків є співпраця між розробниками, користувачами та організаціями з питань безпеки. Розробники повинні бути відкриті до отримання зворотного зв'язку від користувачів щодо можливих вразливостей та проблем з безпекою, а також реагувати на них швидко та ефективно. Користувачі, у свою чергу, повинні бути усвідомлені щодо загроз безпеці та вживати заходів для захисту своїх особистих даних, таких як використання складних паролів та вимог до безпеки даних. Організації з питань безпеки повинні надавати розробникам мобільних додатків необхідну підтримку, рекомендації та інструменти для забезпечення високого рівня безпеки їхніх додатків.

Ще однією важливою складовою забезпечення безпеки мобільних додатків є врахування локальних та міжнародних законодавчих вимог щодо захисту особистих даних користувачів. Наприклад, в Європейському Союзі існує Загальний регламент з захисту особистих даних (GDPR), який встановлює обов'язки щодо захисту особистих даних громадян ЄС. Розробники мобільних додатків, які працюють з особистими даними користувачів, повинні бути уважними до вимог GDPR та вживати заходів для їх виконання.

Необхідно також враховувати потенційні внутрішні загрози безпеці, такі як недбале використання прав доступу та можливість внутрішнього шпигунства. Розробники мають встановлювати строгий контроль над доступом до основних функцій та даних додатка, обмежувати права доступу співробітників лише до необхідного мінімуму та регулярно перевіряти активності користувачів для виявлення неправомірних дій.

Окрім того, розробники повинні бути готові до надзвичайних ситуацій та інцидентів безпеки, таких як хакерські атаки або витоки даних. Для цього рекомендується розробляти та впроваджувати плани реагування на інциденти безпеки, які включають в себе процедури виявлення, аналізу та відновлення після інциденту.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Також важливо підготувати команду для ефективного реагування на інциденти безпеки та співпрацювати зі сторонніми експертами та органами з питань безпеки для швидкого та ефективного вирішення проблем.

У кінцевому підсумку, забезпечення безпеки мобільних додатків - це складний та багатогранний процес, який вимагає поєднання технічних, організаційних та соціальних заходів. Розробники мобільних додатків повинні бути готовими до постійних змін у загрозах та викликах безпеки та постійно підтримувати високий рівень безпеки своїх додатків. Тільки таким чином можна забезпечити захист особистих даних користувачів та довіру споживачів до мобільних додатків.

2.2 Огляд методів які використовуються для аналізу мобільних додатків.

Аналіз мобільних додатків включає різноманітні методи та інструменти, що дозволяють виявляти вразливості, оцінювати безпеку та функціональність додатків. Основні методи аналізу можна поділити на три категорії: статичний аналіз, динамічний аналіз та аналіз вихідного коду.

Ось приклад деяких методів аналізу мобільних додатків:

- Статичний аналіз коду
- Динамічний аналіз
- Аналіз дозволів
- Аналіз шифрування
- Тестування на проникнення
- Аналіз вразливостей на рівні API
- Моніторинг мережевого трафіку
- Аналіз взаємодії з вбудованими компонентами
- Моделювання загроз
- Аналіз застосування криптографії

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Статичний аналіз коду - цей метод включає в себе перегляд вихідного коду додатка без його виконання. Аналізатори статичного коду використовуються для виявлення можливих вразливостей, таких як недостатні перевірки вводу даних, потенційні витоки пам'яті, недостатність автентифікації та авторизації, інженерія зворотного інженерії.

Переваги статичного аналізу коду включають можливість виявлення широкого спектру проблем, від простих синтаксичних помилок до складних вразливостей безпеки. Цей метод також дозволяє здійснювати аналіз всього коду програми, включаючи ті частини, які можуть бути важко або неможливо досягти під час реального виконання програми.

Під час статичного аналізу коду використовуються різноманітні інструменти та техніки. Це можуть бути спеціалізовані програми, які автоматично перевіряють код на наявність певних типів помилок або вразливостей, або ручний аналіз коду кваліфікованими спеціалістами з безпеки програмного забезпечення.

Ключовими етапами статичного аналізу є лексичний аналіз (розбір коду на токени), синтаксичний аналіз (перевірка граматичної структури) та аналіз контексту. Під час аналізу контексту враховуються особливості функціонування програми та її інтеракція з різними середовищами.

Інші підходи до статичного аналізу можуть включати виявлення аномалій у структурі даних, виявлення потенційних уразливостей безпеки, аналіз потенційних проблем з пам'яттю або ресурсами та ідентифікацію можливих точок виконання вразливого коду.

Загалом, статичний аналіз коду є важливим інструментом у процесі забезпечення безпеки мобільних додатків, який допомагає виявляти та виправляти потенційні проблеми ще до того, як вони можуть бути використані зловмисниками для атаки.

Переваги статичного тестування:

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

- Знижує вартість фіксу знайдених багів, оскільки виявляє баги на ранніх етапах циклу розробки програмного забезпечення
- Відгуки, отримані в ході цього тестування, допомагають покращити функціонування процесу, що також допомагає команді уникнути подібних дефектів і багів
- Підвищує інформованість про різні проблеми якості програмного забезпечення
- Покращує обмін критичної і важливої інформації між членами команди
- Істотно скорочуються зусилля по виправленню помилок, що ще більше сприяє продуктивності розробки

Недоліки статичного тестування:

- Процес статичного тестування може займати багато часу, так як в основному він виконується вручну
- Перешкоджає виявленню вразливостей, представлених в середовищі виконання

Динамічний аналіз - цей метод включає в себе виконання додатка в контрольованому середовищі для виявлення вразливостей під час його роботи. Інструменти для динамічного аналізу можуть відслідковувати взаємодію додатка з операційною системою, мережею та зовнішніми ресурсами, щоб виявити можливі проблеми з безпекою, такі як недостатність шифрування, незахищений обмін даними та вразливості мережі.

Під час динамічного аналізу спостерігають за виконанням програми та взаємодією з навколишнім середовищем. Цей процес може включати тестування введених даних, виявлення вразливостей забезпечення, аналіз мережевої взаємодії та перевірку відповідності дій програми заявленим вимогам безпеки.

Динамічний аналіз дозволяє виявляти проблеми, які можуть виникнути тільки під час виконання програми, такі як вразливості в мережевому взаємодії або

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

некоректне використання ресурсів пристрою. Він також дозволяє виявляти вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до даних або контролю над пристроєм.

Динамічний аналіз використовується разом із статичним аналізом для повного оцінювання безпеки мобільних додатків. Він допомагає ідентифікувати потенційні загрози та ризики, забезпечуючи високий рівень захисту для користувачів мобільних пристроїв.

Переваги динамічного тестування:

- Це ретельне дослідження, яке розглядає всю функціональність програми, тому якість відповідає найвищим стандартам.
- Процес динамічного тестування добре налагоджений, додаток тестується з точки зору користувача, що підвищує якість ПЗ.
- Виявлення складних помилок, які могли вислизнути на етапі код рев'ю.
- Динамічне тестування може бути автоматизовано за допомогою спеціальних інструментів.

Недоліки динамічного тестування :

- Оскільки динамічне тестування являє собою складний процес, воно займає багато часу.
- Висока вартість проведення тестування.
- Динамічне тестування зазвичай виконується після завершення кодування, і знайдені баги виявляються пізніше в життєвому циклі розробки.

Аналіз дозволів - додатки запитують різні дозволи для доступу до функцій та ресурсів пристрою. Цей метод включає в себе оцінку, які дозволи запитує додаток, і як вони використовуються в процесі роботи. Виявлення надмірних дозволів

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

або некоректного використання дозволів може свідчити про потенційні проблеми з безпекою.

Переваги аналізу дозволів:

- Аналіз дозволів дозволяє виявити можливі загрози приватності та безпеки, які можуть виникнути внаслідок надання додатком доступу до різних ресурсів пристрою.
- Даний аналіз дозволяє користувачам краще розуміти, які дозволи запитують додатки та на що саме це впливає, що дозволяє їм приймати інформовані рішення щодо встановлення чи використання додатків.
- Аналіз дозволів сприяє створенню прозорих стандартів щодо збору та використання особистої інформації користувачів, що сприяє підвищенню довіри до розробників додатків.

Недоліки аналізу дозволів:

- Деякі дозволи можуть бути недостатньо конкретними або неявними, що ускладнює оцінку їх впливу на безпеку та приватність користувачів.
- Деякі користувачі можуть не мати достатньої компетентності чи інтересу для ретельного аналізу дозволів, що може призвести до неправильних рішень щодо встановлення додатків.
- При наданні дозволів під час встановлення додатків користувачі можуть не мати достатнього контролю над тим, як саме їхні дані будуть використані розробниками.

Аналіз шифрування - даний метод включає в себе перевірку правильності використання шифрування для захисту конфіденційної інформації, такої як обмін даними між додатком та його сервером або зберігання чутливих даних на пристрої.

Переваги аналізу шифрування:

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- Шифрування даних дозволяє зберігати та передавати інформацію в зашифрованому вигляді, що робить її недоступною для несанкціонованого доступу.
- Шифрування ускладнює можливість перехоплення та прослуховування конфіденційної інформації, що підвищує рівень безпеки даних.
- Використання шифрування дозволяє відповідати вимогам щодо захисту даних, встановленим стандартами та регуляторними органами.

Недоліки аналізу шифрування:

- Шифрування вимагає обробки та зберігання ключів, що може бути складним завданням і призводити до потенційних проблем з безпекою, якщо ключі потраплять у несанкціоновані руки.
- Процес шифрування та розшифрування може займати певний час та витрачати ресурси пристрою, що може призвести до зменшення продуктивності додатків або пристроїв.
- Невірно налаштовані або застарілі алгоритми шифрування можуть бути вразливими до атак, що може призвести до компрометації конфіденційної інформації.

Тестування на проникнення - цей метод включає в себе спроби активно використовувати вразливості для незаконного доступу до додатку чи системи, на якій він працює. Тестування на проникнення може бути автоматизованим або виконуватися вручну для пошуку слабких місць в безпеці.

Переваги тестування на проникнення:

- Пенетраційне тестування дозволяє ідентифікувати потенційні вразливості та уразливі місця у системі або додатку, які можуть бути використані для несанкціонованого доступу.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

- Шляхом виявлення та виправлення вразливостей під час пенетраційного тестування можна підвищити загальний рівень безпеки системи або додатку.
- Тестування на проникнення дозволяє перевірити ефективність вже наявних заходів безпеки та виявити можливі недоліки у їх реалізації.

Недоліки тестування на проникнення:

- Проведення пенетраційного тестування може призвести до невідомих ризиків втрати даних або завдання шкоди системі, особливо якщо тестування проводиться неадекватно або без належної підготовки.
- Проведення пенетраційного тестування може бути дорогим процесом, особливо якщо воно здійснюється залученням зовнішніх експертів або спеціалізованих компаній.
- Пенетраційне тестування може не виявити всі можливі вразливості або недоліки в системі, особливо якщо воно проводиться у певному обмеженому контексті або з обмеженими ресурсами.

Аналіз вразливостей на рівні API - Перевірка використання API (Application Programming Interface) мобільних платформ, таких як Android або iOS, для виявлення можливих вразливостей або недоліків.

Переваги аналізу вразливостей на рівні API:

- Дозволяє ідентифікувати можливі вразливості та потенційні загрози на рівні API, що дозволяє розробникам або адміністраторам системи уникнути використання небезпечних методів або попередити можливі атаки.
- Дозволяє виявити потенційні вразливості в API, які можуть бути використані зловмисниками для атаки на мобільні додатки чи систему в цілому. Це дозволяє приймати вчасні заходи для запобігання можливим загрозам.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

- Розуміння вразливостей на рівні API дозволяє розробникам реалізувати більш безпечний код та приймати необхідні заходи для запобігання можливим атакам.

Недоліки аналізу вразливостей на рівні API:

- Аналіз вразливостей на рівні API може бути складним завданням через велику кількість можливих методів та функцій, які можуть бути використані у додатку.
- Деякі API можуть мати обмежений доступ до документації або іншої інформації, що ускладнює проведення аналізу вразливостей та виявлення можливих загроз.
- Аналіз вразливостей на рівні API вимагає від розробників або аналітиків високого рівня компетентності та розуміння принципів безпеки програмного забезпечення.

Моніторинг мережевого трафіку - Аналіз мережевого трафіку, який генерується мобільним додатком, для виявлення можливих проблем з безпекою, таких як передача незахищених даних через мережу.

Переваги моніторингу мережевого трафіку:

- Моніторинг мережевого трафіку дозволяє виявляти незвичайні чи підозрілі патерни трафіку, що можуть свідчити про атаки або інші проблеми в мережі.
- Аналіз мережевого трафіку дозволяє виявити потенційні загрози безпеці, такі як спроби несанкціонованого доступу до системи або намагання витоку конфіденційної інформації.
- Дозволяє перевірити, чи дотримуються користувачі встановлених політик безпеки, таких як обмеження доступу чи застосування шифрування.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

- Моніторинг мережевого трафіку дозволяє оперативно виявляти і реагувати на потенційні інциденти безпеки, зменшуючи можливість збитків.

Недоліки моніторингу мережевого трафіку:

- Постійний моніторинг може призвести до збільшення обсягу трафіку в мережі, що може призвести до перевантаження і зниження продуктивності.
- Аналіз великого обсягу мережевого трафіку може бути складним і часоміробійним завданням, особливо у великих мережах з багатьма пристроями.
- Збір та аналіз мережевого трафіку може порушити приватність користувачів та викликати питання щодо дотримання законодавства про захист персональних даних.

Аналіз взаємодії з вбудованими компонентами - Дослідження взаємодії мобільного додатка з вбудованими компонентами, такими як камера, мікрофон, GPS, для виявлення можливих проблем з конфіденційністю даних.

Переваги аналізу взаємодії з вбудованими компонентами:

- Дозволяє перевірити, чи дотримуються мобільні додатки встановлених політик конфіденційності щодо використання вбудованих компонентів пристрою.
- Допомогає виявити можливі загрози безпеці, пов'язані з недоцільним або несанкціонованим використанням вбудованих компонентів.
- Дозволяє забезпечити безпеку та конфіденційність інформації, яку обробляє мобільний додаток, за рахунок контролю за взаємодією з вбудованими компонентами.

Недоліки аналізу взаємодії з вбудованими компонентами:

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

- Аналіз взаємодії з вбудованими компонентами може бути складним завданням, оскільки вимагає детального вивчення різних аспектів роботи додатка з пристроєм.
- Для проведення аналізу може знадобитися збір додаткових даних про використання вбудованих компонентів, що може викликати питання щодо приватності та конфіденційності.
- Аналіз взаємодії з вбудованими компонентами може вимагати значних ресурсів, таких як час та технічні знання, що може ускладнити процес.

Моделювання загроз - Використання методів моделювання загроз для визначення потенційних сценаріїв атак та їх впливу на безпеку мобільного додатка.

Переваги моделювання загроз:

- Дозволяє передбачити можливі вразливості та проблеми безпеки, які можуть виникнути в мобільних додатках під час реальної експлуатації.
- Допомогає зменшити ризики та наслідки можливих загроз, оскільки дозволяє розробникам підготуватися до них та вжити відповідних заходів забезпечення безпеки.
- Надає можливість розробникам мобільних додатків визначити пріоритетність заходів забезпечення безпеки та витратити ресурси на найбільш критичні області.

Недоліки моделювання загроз:

- Моделювання загроз може бути складним завданням, оскільки вимагає детального розуміння архітектури мобільного додатка та його потенційних слабких місць.
- Результати моделювання можуть бути обмежені точністю, оскільки вони базуються на припущеннях та імітації реальних умов.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

- Моделювання загроз може вимагати значних часових та людських ресурсів для його проведення, що може ускладнити процес розробки мобільного додатка.

Аналіз застосування криптографії - Перевірка правильності використання криптографічних алгоритмів та протоколів для захисту даних в мобільних додатках.

Переваги аналізу застосування криптографії:

- Використання криптографії дозволяє зашифрувати конфіденційні дані, такі як паролі, особиста інформація та фінансові дані, що забезпечує їхню захищеність від несанкціонованого доступу.
- Шифрування дозволяє перевірити цілісність даних шляхом порівняння хеш-сум або цифрових підписів, що допомагає виявити будь-які спроби модифікації або підроблення інформації.
- Криптографія дозволяє перевірити автентичність користувачів та серверів шляхом використання цифрових підписів, сертифікатів та інших методів автентифікації.
- Використання криптографічних методів може допомогти мобільним додаткам відповідати вимогам стандартів безпеки та регуляторних вимог.

Недоліки аналізу застосування криптографії:

- Неправильне використання криптографії може призвести до вразливостей, таких як виток конфіденційної інформації, слабкі ключі шифрування або використання застарілих криптографічних алгоритмів.
- Деякі методи шифрування можуть бути вразливі до підбірки ключа або інших атак, особливо якщо вони використовуються неправильно або з недостатньою довжиною ключа.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

- Великий обсяг обробки даних, пов'язаний з криптографічними операціями, може призвести до зниження продуктивності мобільних додатків, особливо на пристроях з обмеженими ресурсами.
- Ефективне управління ключами шифрування може бути складною задачею, особливо при великому обсязі даних та масштабуванні мобільного додатка.

Узагальнюючи, аналіз мобільних додатків є надзвичайно важливим етапом у процесі їхньої розробки та випуску. Використання різних методів аналізу дозволяє забезпечити високу якість та безпеку програмного забезпечення, зменшуючи ризики для користувачів та підвищуючи їхнє задоволення від використання додатків.

Використання різних методів аналізу, таких як статичний, динамічний, методи на базі машинного навчання та спеціалізовані інструменти, дозволяє забезпечити високу якість та безпеку програмного забезпечення.

2.3 Огляд інструментів аналізу безпеки мобільних додатків

Аспекти кібербезпеки в мобільних додатках є дуже важливими, оскільки ці додатки використовуються для обробки та збереження особистих даних користувачів. Забезпечення безпеки даних від несанкціонованого доступу та захист від вразливостей і атак допомагає запобігти порушенням приватності та зберегти довіру користувачів до додатків, що є важливим для їхнього успішного використання та розвитку.

З поширенням мобільних додатків зростає і потреба у розвитку методів та інструментів для їхнього аналізу та захисту. Статичний і динамічний аналіз коду, сканування вразливостей та пентестинг допомагають виявляти потенційні загрози. Паралельно з цим збільшується різноманіття методів атак, тому постійне вдосконалення засобів оборони є критично важливим для забезпечення безпеки мобільних додатків та довіри користувачів.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

SonarQube - це платформа для автоматизованого аналізу якості вихідного коду. Вона надає інструменти для виявлення різноманітних проблем у програмному коді, таких як потенційні вразливості безпеки, недоліки в якості коду, невідповідність стандартам програмування та інші архітектурні або дизайнерські проблеми.

SonarQube дозволяє розробникам і командам розробки виявляти ці проблеми на ранніх етапах розробки, що дозволяє їм швидше виправити їх та покращити загальну якість програмного забезпечення. Він також надає зручний інтерфейс для візуалізації результатів аналізу та моніторингу якості коду протягом часу. SonarQube може бути інтегрований з різними інструментами розробки, такими як Maven, Jenkins, GitHub тощо, що робить його дуже потужним інструментом для автоматизованого контролю якості програмного забезпечення.



Рис. 2.1. SonarQube

Переваги:

- Автоматизований аналіз коду
- Широкий спектр функціональності
- Інтеграція з іншими інструментами розробки
- Постійний моніторинг якості коду

Недоліки:

- Складність налаштування
- Можливість неправильних результатів

Загальні принципи тестування ПЗ передбачають наявність трьох основних етапів: ревізія коду, статичний аналіз, динамічний аналіз.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Ревізія коду або Program understanding, зазвичай, проводиться фахівцем із тестування ПЗ у режимі перегляду на предмет виявлення у коді явних помилок, порушень у стилі коду та інших невідповідностей.

Статичний аналіз передбачає перевірку вихідного коду без його виконання. Він застосовується на початкових стадіях розробки та передбачає використання спеціального ПЗ для виявлення помилок, котре працює в автоматичному режимі. Його можна порівняти із аналізом, котрий виконується над програмою при «проходженні» звичайного компілятора, але на більш глибокому рівні.

Сервіс розповсюджується за GNU LGPL-ліцензією, створений на мові Java та має відкритий вихідний код. Він забезпечує виконання безперервного аналізу коду (Continuous inspection) та вимір його якості у відповідності із відомими сімома показниками (Seven Axes of Quality):

- Якість стилю коду;
- Виявлення потенційних помилок;
- Коментарі;
- Тестування;
- Дублювання фрагментів коду;
- Ступінь складності;
- Архітектура та проектування.

Відповідає стандартам MITRE/CWE, MISRA C/C++, CERT Secure Coding Standards та деяким неформалізованим міжнародним вимогам.

Сервіс забезпечує миттєвий зв'язок із розробником під час роботи у IDE-системі, що дозволяє у реальному режимі часу виправляти помилки ще до їх фіксації у коді.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Програма використовує систему плагінів, що потенційно дозволяє інтегруватися із будь-яким IDE та розширити список мов програмування. На даний час підтримується близько 30-ти мов. Зокрема, для вільно розповсюджуваної версії програми підтримуються наступні мови та технології:

- JavaScript
- Java
- AWS
- Ruby
- Scala
- Python
- HTML
- PHP
- Visual Basic
- C Sharp
- XML
- Kotlin
- Go

Він може бути використаний для виявлення проблем безпеки, дефектів коду, дублікатів, невиконання кодових стандартів та інших аспектів, які можуть впливати на ефективність та безпеку мобільних додатків. Шляхом інтеграції SonarQube в процес розробки мобільних додатків, розробники можуть підтримувати високий рівень якості коду та забезпечувати безпеку їхніх додатків на різних платформах, таких як Android та iOS.

Також цікавим інструментом буде **Burp Suite**, він є одним з найпопулярніших інструментів в галузі кібербезпеки та використовується для виявлення та управління різних типів вразливостей у веб-додатках.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Burp Suite - це інтегроване середовище для тестування безпеки веб-додатків, яке розробляється компанією PortSwigger Web Security.

Burp Suite має широкий спектр функціональності, включаючи проксі-сервер, сканер вразливостей, інструменти перехоплення трафіку та інші. Він дозволяє спеціалістам з безпеки аналізувати та тестувати веб-додатки на наявність різних уразливостей, таких як крос-сайт скриптинг, ін'єкції SQL та інші. Burp Suite також має активну спільноту користувачів, яка надає підтримку, документацію та обмін досвідом щодо використання цього інструменту.

Burp Suite використовують тисячі компаній по всьому світу, включаючи великі технологічні компанії, банки, фінансові установи, консалтингові фірми, стартапи та інші. Деякі з них включають в себе компанії, такі як Google, Facebook, Microsoft, Twitter, IBM, Amazon, PayPal, Visa, Mastercard, Goldman Sachs, Deloitte, PwC, Accenture та багато інших. Користувачі Burp Suite відомі своїми високими стандартами безпеки та використовують цей інструмент для забезпечення надійності та безпеки своїх веб-додатків.

Компанія PortSwigger також забезпечує регулярне оновлення Burp Suite, включаючи виправлення помилок, нові функції та покращення, що дозволяє тримати цей інструмент на передових позиціях у сфері тестування безпеки. Його активна спільнота користувачів надає підтримку, документацію та обмін досвідом для сприяння в подальшому розвитку та використанні Burp Suite.

Спільнота користувачів Burp Suite має значний вплив на розвиток та вдосконалення цього інструменту. Вона надає важливий зворотний зв'язок розробникам щодо виявлених проблем, запитів на нові функції та важливих покращень. Також активно обмінюється знаннями, досвідом та кращими практиками в області тестування безпеки веб-додатків, що сприяє росту компетентності користувачів та підвищенню якості їх роботи. Крім того, сприяє популяризації Burp Suite серед нових користувачів та сприяє його поширенню як основного інструменту для тестування безпеки веб-додатків.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

BurpSuite існує у 3-х версіях: Community Edition, Professional Edition та Enterprise Edition.

Перша надається безкоштовно і входить у склад ОС Kali Linux. Дві останні версії — платні, надають розширений функціонал, для них необхідно придбати ліцензію.

BurpSuite Professional можна спробувати також на безкоштовній основі в рамках випробовувального Trial-періоду. Для цього слід написати в технічну підтримку PortSwigger.



Рис. 2.2. Burp Suite

Переваги:

- Широкий спектр функціональності
- Підтримка спільноти
- Постійне оновлення

Недоліки:

- Вартість
- Навчання
- Обмеження функціональності безплатної версії

Burp Suite підходить для тестування мобільних додатків, включаючи як Android, так і iOS. Він надає можливості для перехоплення трафіку між мобільним

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

додатком та сервером, аналізу та зміни HTTP-запитів і відповідей, сканування вразливостей та інші функції, які допомагають виявляти та усувати потенційні проблеми з безпекою в мобільних додатках. Є популярним інструментом серед професіоналів у галузі кібербезпеки для проведення тестування безпеки мобільних додатків.

Використання Burp Suite вимагає певного рівня практики і знань, що може зайняти час на оволодіння навичками.

Незважаючи на високу вартість повної версії та необхідність певного рівня практики та знань для використання, Burp Suite залишається одним із провідних інструментів.

Appium — це популярний інструмент для автоматизації тестування мобільних додатків, який підтримує як Android, так і iOS. Він базується на відкритому вихідному коді і дозволяє тестувати мобільні додатки на різних платформах, використовуючи одні й ті ж тести.

Appium був розроблений Деном Кюрі у 2011 році як відкритий проект з метою створення універсального інструменту для автоматизації тестування мобільних додатків. Його розробка була спрямована на забезпечення простоти використання, крос-платформеності та інтеграції з Selenium, що забезпечило йому широку популярність та активну спільноту користувачів.

Ден Кюрі, розробник Appium, винайшов цей інструмент, використовуючи знання, накопичені під час його роботи в компанії Sauce Labs, де він працював над автоматизацією тестування мобільних додатків. Його мета була створити відкрите рішення, яке б дозволяло автоматизувати тестування різних типів мобільних додатків без обмежень щодо платформи чи мови програмування. Від тих пір Appium продовжує розвиватися завдяки активній спільноті розробників та тестувальників.

Appium є потужним інструментом для автоматизованого тестування мобільних додатків, який підходить для команд, що шукають універсальне рішення для тестування на різних платформах. Він забезпечує гнучкість у використанні різних

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

мов програмування і сумісність з існуючими інструментами для автоматизації тестування.

Підтримує режим "інспектора елементів" для мобільних додатків, що дозволяє розробникам та тестувальникам легко ідентифікувати та взаємодіяти з елементами інтерфейсу користувача безпосередньо з Appium. Це значно спрощує процес створення та налагодження автоматизованих тестів.



Рис. 2.3. Appium

Переваги:

- Підтримка кількох платформ
- Відкритий вихідний код
- Підтримка різних мов програмування
- Не потребує модифікації коду додатка
- Використання WebDriver протоколу

Недоліки:

- Налаштування та конфігурація
- Швидкість виконання тестів
- Проблеми сумісності

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Спільнота користувачів та активна база знань є ключовими аспектами успішного використання будь-якого програмного забезпечення, включаючи Appium. Appium має широку спільноту користувачів, які активно обговорюють питання, надають поради та діляться своїм досвідом на різних форумах і в онлайн-спільнотах, таких як Stack Overflow, Reddit, GitHub Discussions, а також на офіційному форумі Appium.

Документація детальна та оновлюється, містить інструкції з встановлення, налаштування та використання. Крім того, доступна велика кількість онлайн-ресурсів, таких як блоги, відеоуроки, курси та інші матеріали, що допомагають користувачам засвоїти Appium.

Є відкритим проектом з відкритим вихідним кодом, розміщеним на платформі GitHub. Це означає, що користувачі можуть приєднатися до розробки, надавати внесок у вигляді патчів, вносити пропозиції щодо покращень та взаємодіяти з іншими учасниками спільноти для подальшого розвитку і вдосконалення інструменту.

Він підтримує різні мови програмування для написання тестових сценаріїв. Основними мовами програмування, які використовуються для розробки тестів в Appium, є:

- Java
- Python
- JavaScript
- C#
- Ruby
- PHP, Perl, Swift і т. д.

Гнучкість і розширюваність Appium роблять його оптимальним вибором для різноманітних команд і проектів. Цей інструмент дозволяє тестувати різні аспекти мобільних додатків, включаючи їхні інтерфейси користувача, мережеві взаємодії

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

та роботу з базами даних. Однак для успішного використання користувачам варто ознайомитися з його особливостями та налаштуваннями.

Appium, заснований на протоколі WebDriver, спрощує перехід для користувачів, які вже працювали з Selenium. Він має вбудований інспектор елементів, підтримує хмарні сервіси, розширюється плагінами, тестує гібридні додатки, інтегрується з CI/CD, працює з різними інструментами автоматизації, активно розвивається.

У підсумку, Appium - це важливий інструмент для автоматизації тестування мобільних додатків, який сприяє підвищенню якості продукту та прискоренню процесу розробки.

Отже, мобільні додатки стають не лише невід'ємною частиною нашого повсякденного життя, але і критично важливими для бізнесу, забезпечення їх кібербезпеки набуває значущості, без якої неможливо уявити успіх та прийняття користувачами. У цьому контексті інструменти, такі як SonarQube, Burp Suite та Appium, виступають у ролі краївидних фортець, що забезпечують недоторканність мобільних додатків. Їхні можливості з виявлення та виправлення потенційних загроз не оціненні, бо саме вони дозволяють підтримувати високу якість програмного забезпечення та зберігати довіру користувачів. З постійним вдосконаленням, активною підтримкою спільноти та нескінченною гнучкістю використання ці інструменти виступають не просто як технологічні рішення, але як підстава сучасного цифрового світу.

Таким чином, можна прийти до висновка що безпека мобільних додатків стає все більшою проблемою, оскільки зростає кількість загроз та вразливостей, з якими стикаються користувачі. Щоб забезпечити надійність та безпеку програмного забезпечення, розробники використовують різноманітні інструменти, такі як SonarQube, Burp Suite та Appium.

SonarQube є незамінним інструментом для аналізу коду та виявлення потенційних проблем на ранніх стадіях розробки. Він допомагає забезпечити високу якість програмного забезпечення та уникнути можливих загроз безпеки.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Burp Suite спеціалізується на тестуванні вразливостей веб-додатків і дозволяє виявляти та виправляти різноманітні типи атак, що забезпечує надійність та безпеку веб-додатків.

Appium відкриває нові можливості для автоматизації тестування мобільних додатків, дозволяючи проводити тестування на різних платформах та мовах програмування.

Загалом, ці інструменти не лише допомагають забезпечити безпеку та надійність програмного забезпечення, але і відкривають нові можливості для розвитку та удосконалення процесів розробки. Їхня важливість у сучасному цифровому світі неможливо переоцінити, оскільки вони є ключовими у забезпеченні безпеки та надійності мобільних додатків.

Appium був вибраний як інструмент для автоматизації тестування мобільних додатків через свою універсальність, кросплатформеність, відкритість, легку інтеграцію з іншими інструментами тестування та доступність для всіх користувачів.

Висновок до другого розділу

У світі, де мобільні додатки стали неодмінною частиною повсякденного життя, забезпечення їх безпеки стає важливим завданням для розробників, користувачів та організацій. Постійний розвиток технологій і зростання кількості кіберзагроз ставлять під загрозу конфіденційність та безпеку інформації, що зберігається і оброблюється у мобільних додатках. Тому важливо вдосконалювати методи та інструменти для аналізу та виявлення потенційних загроз, щоб забезпечити безпеку та захист особистих даних користувачів.

На сьогоднішній день існують різні підходи до аналізу безпеки мобільних додатків, які включають в себе як стандартні методи, так і новітні технології. Серед них варто відзначити статичний аналіз, який дозволяє виявити потенційні вразливості шляхом аналізу вихідного коду додатків без його виконання. Динамічний аналіз, у свою чергу, передбачає тестування додатка у реальному середовищі з метою виявлення можливих загроз та вразливостей під час його виконання. Також дедалі більшу популярність набувають методи, засновані на

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

штучному інтелекті та машинному навчанні, які дозволяють автоматизувати процес аналізу та виявлення нових типів загроз.

Серед інструментів, що використовуються для аналізу безпеки мобільних додатків, можна виділити такі, як SonarQube, Burp Suite та Appium. Кожен з цих інструментів має свої особливості та переваги. Наприклад, SonarQube відомий своєю можливістю аналізувати якість вихідного коду та виявляти потенційні проблеми на ранніх стадіях розробки, що допомагає покращити безпеку та надійність програмного забезпечення. Burp Suite, з іншого боку, спеціалізується на тестуванні вразливостей веб-додатків і дозволяє виявляти та виправляти різноманітні типи атак, що забезпечує надійність та безпеку додатків у мережі Інтернет. Appium, у свою чергу, відкриває нові можливості для автоматизації тестування мобільних додатків, дозволяючи проводити тестування на різних платформах та мовах програмування.

Загалом, ці інструменти допомагають забезпечити безпеку та надійність програмного забезпечення, зменшуючи ризики для користувачів і підвищуючи їхню довіру до мобільних додатків. Але важливо зауважити, що безпека мобільних додатків - це постійний процес, який вимагає поєднання різних підходів та інструментів для ефективного виявлення та усунення потенційних загроз. Тільки завдяки цьому можна забезпечити захист особистих даних користувачів та підвищити рівень безпеки мобільних додатків в цілому.

РОЗДІЛ 3 ТЕСТУВАННЯ МОБІЛЬНИХ ДОДАТКІВ

3.1 Налаштування та проведення тестування

Для проведення тестування було обрано мобільний додаток Reddit – це соціальна мережа та новинний агрегатор, де користувачі можуть створювати, обговорювати та голосувати за вміст, який вони публікують.

Після встановлення Android Studio, Appium та іншого необхідного програмного забезпечення для роботи з цими додатками, заходимо в Android Studio.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

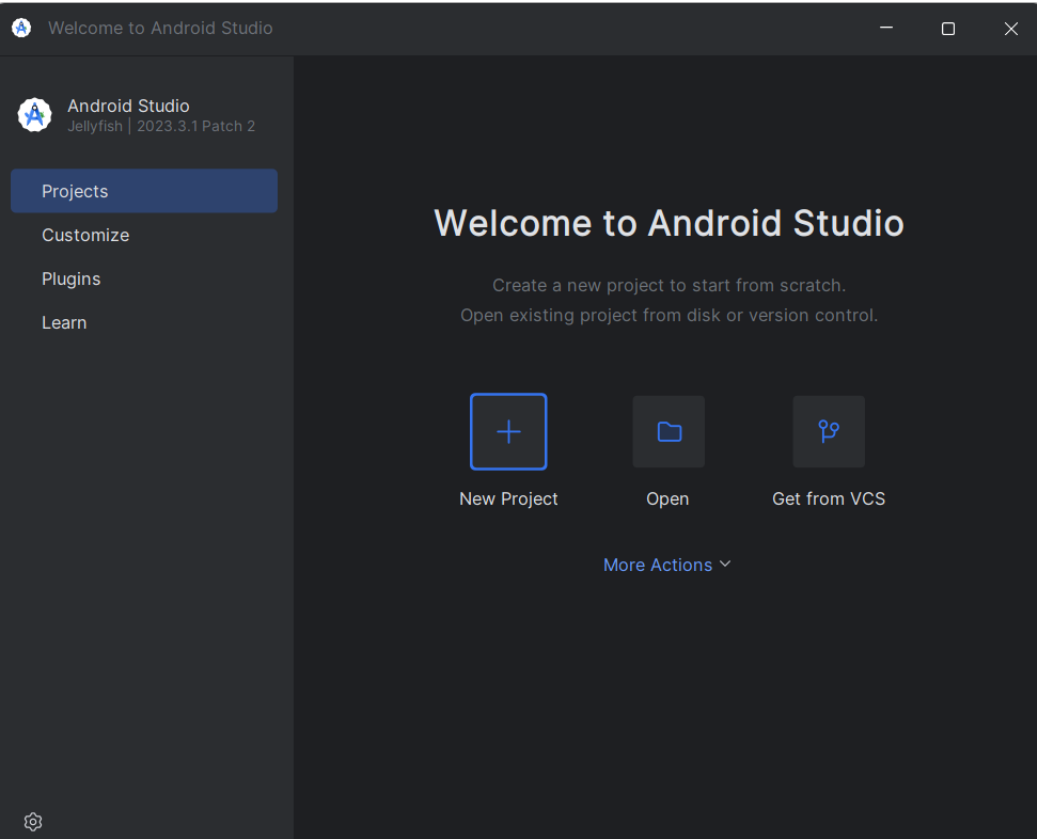


Рис.3.1 Меню Android Studio

Далі обираємо пристрій для додавання його у Device Manager.

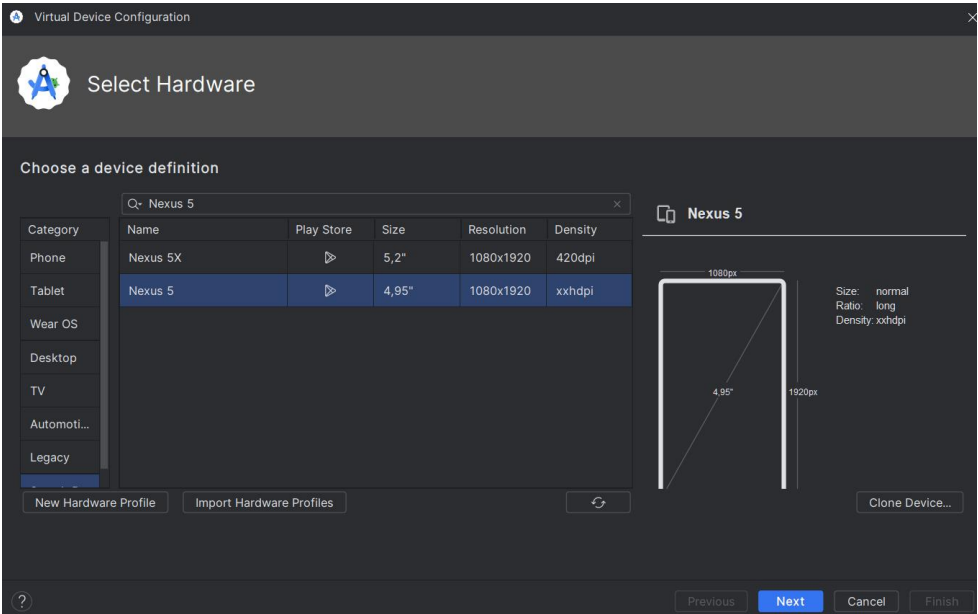


Рис.3.2 Вибір девайсу

Далі обираємо систему пристрою.

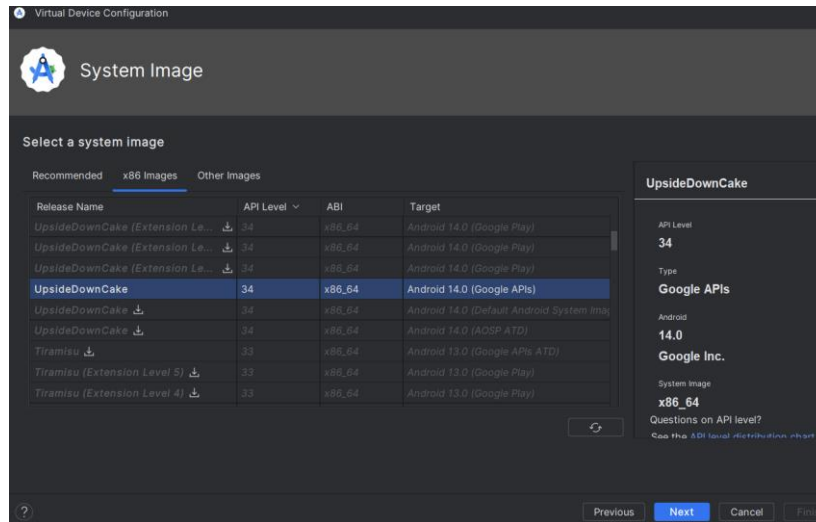


Рис.3.3 Система пристрою

Та конфігурація девайсу.

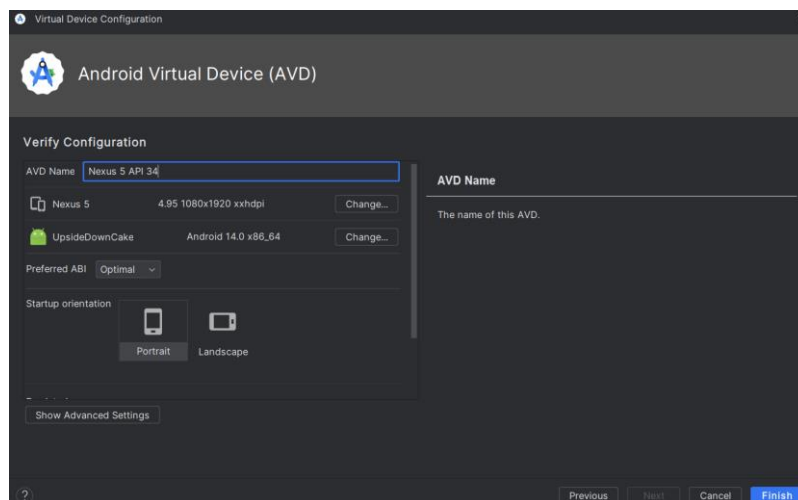


Рис.3.4 Конфігурація

Далі запуск пристрою.

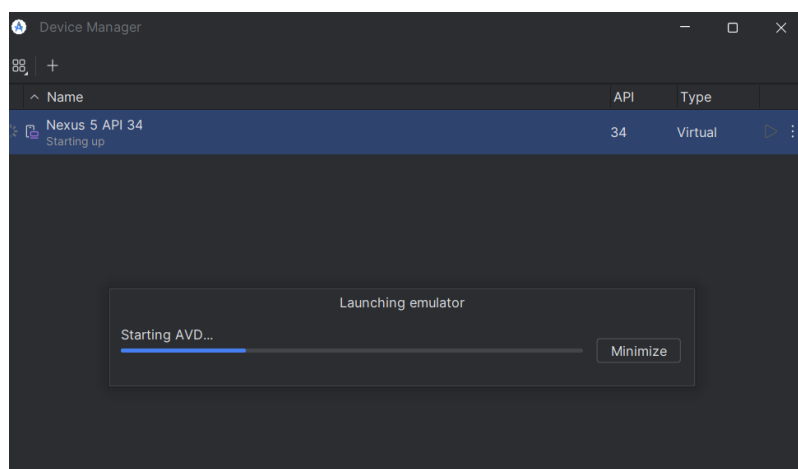


Рис.3.5 Запуск

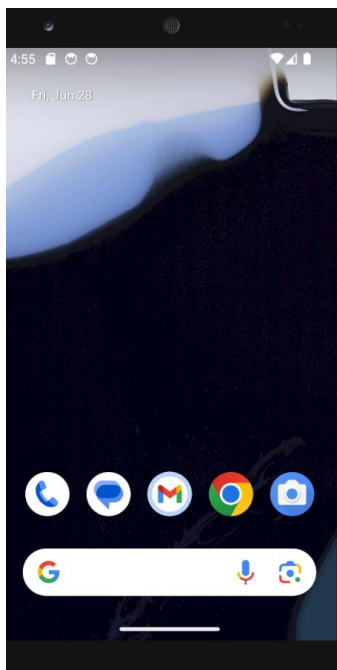


Рис.3.6 Робочий стіл Nexus 5

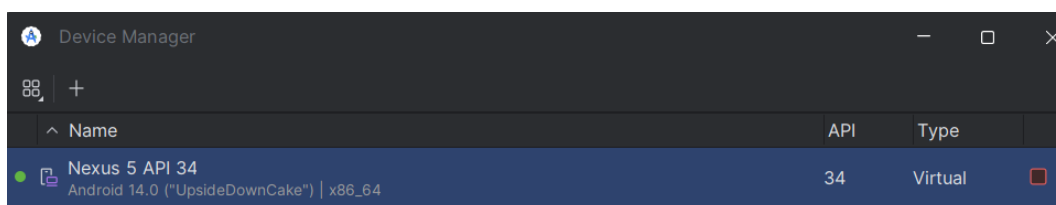


Рис.3.7 Запущений девайс

Далі заходимо в Appium Server.

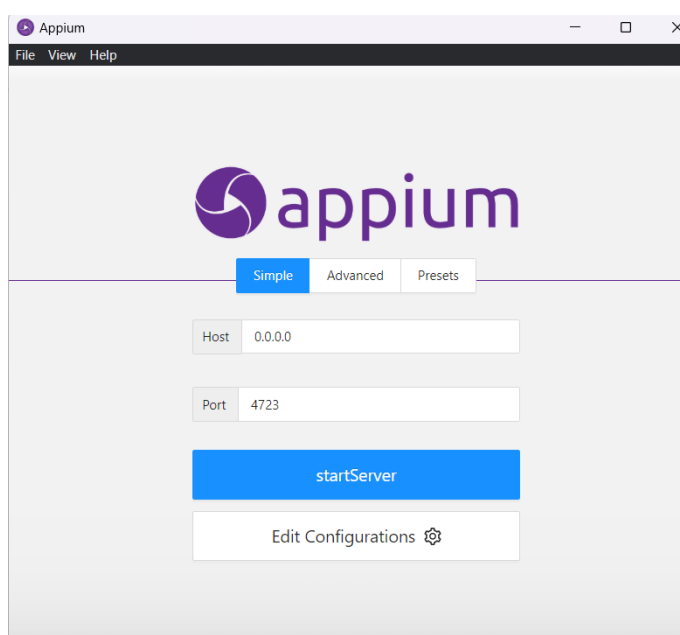


Рис.3.8 Appium Server

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Та вмикаємо його.

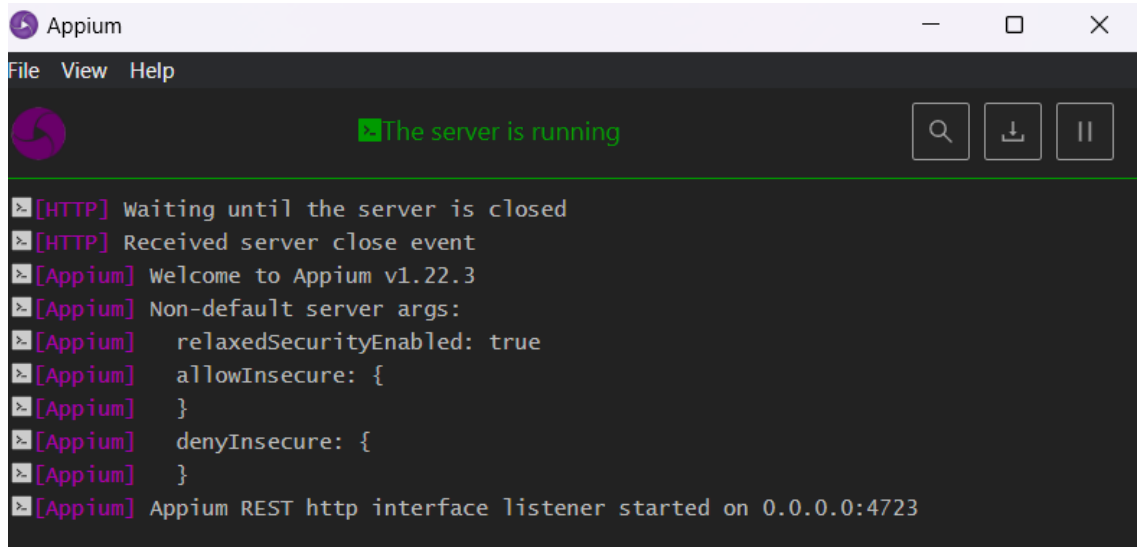


Рис.3.9 Уввімкнений Appium Server

Також можна зробити це через CMD.

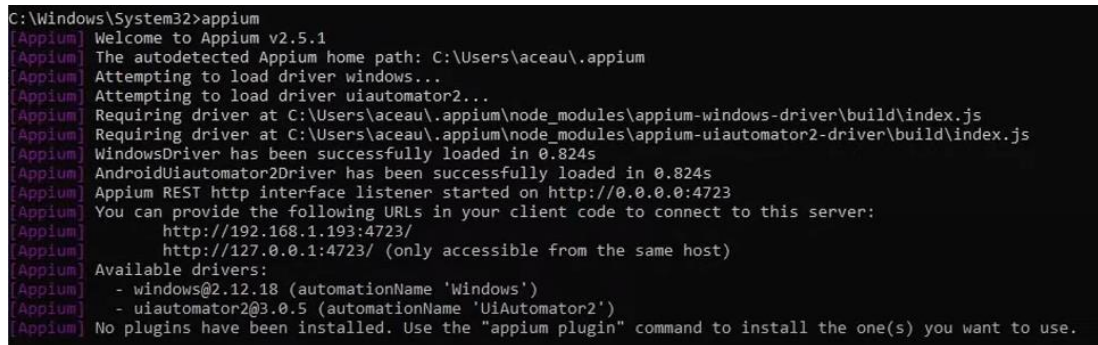


Рис.3.10 Запуск Appium через CMD

Далі запуск теста.

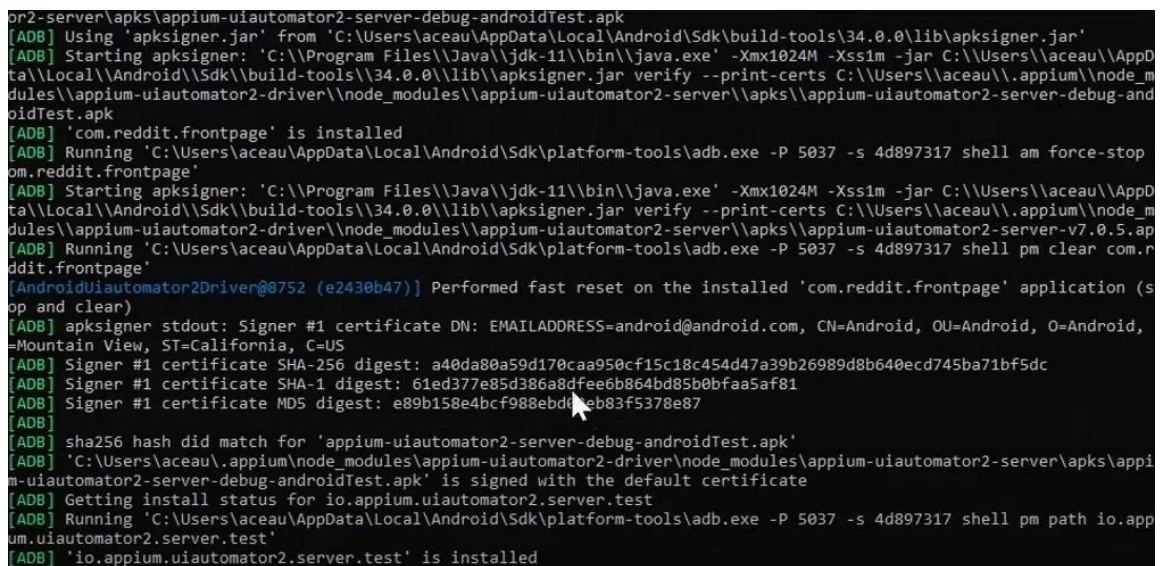


Рис.3.10 Тест

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

"C:\Program Files\Microsoft\j
Application started

Рис.3.11 Додаток запущений



Рис.3.12 Reddit

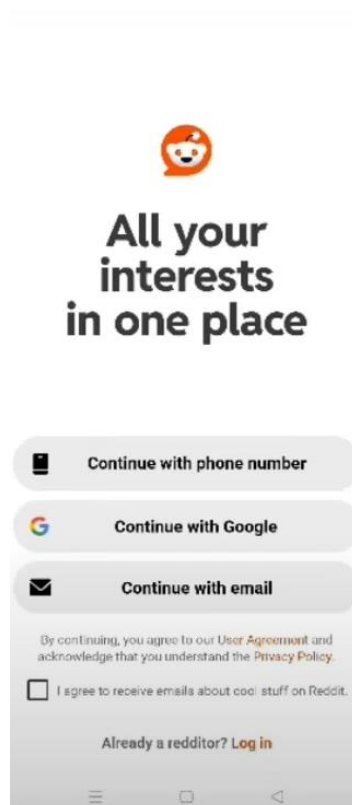


Рис.3.13 Reddit

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

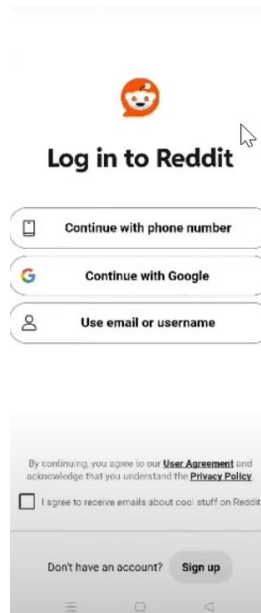


Рис.3.14 Вибір методу входу

Далі повторно запустимо Appium Server.

```
C:\Windows\System32>appium
[Appium] Welcome to Appium v2.5.1
[Appium] The autodetected Appium home path: C:\Users\aceau\.appium
[Appium] Attempting to load driver windows...
[Appium] Attempting to load driver uiautomator2...
[Appium] Requiring driver at C:\Users\aceau\.appium\node_modules\appium-uiautomator2-driver\build\index.js
[Appium] Requiring driver at C:\Users\aceau\.appium\node_modules\appium-windows-driver\build\index.js
[Appium] AndroidUiautomator2Driver has been successfully loaded in 1.121s
[Appium] WindowsDriver has been successfully loaded in 1.122s
[Appium] Appium REST http interface listener started on http://0.0.0.0:4723
[Appium] You can provide the following URLs in your client code to connect to this server:
[Appium] http://192.168.1.193:4723/
[Appium] http://127.0.0.1:4723/ (only accessible from the same host)
[Appium] Available drivers:
[Appium] - windows@2.12.18 (automationName 'Windows')
[Appium] - uiautomator2@3.0.5 (automationName 'UiAutomator2')
[Appium] No plugins have been installed. Use the "appium plugin" command to install the one(s) you want to use.
```

Рис.3.15 Повторний запуск

Наступний крок це введення значень в appium inspector та запуск сесії.

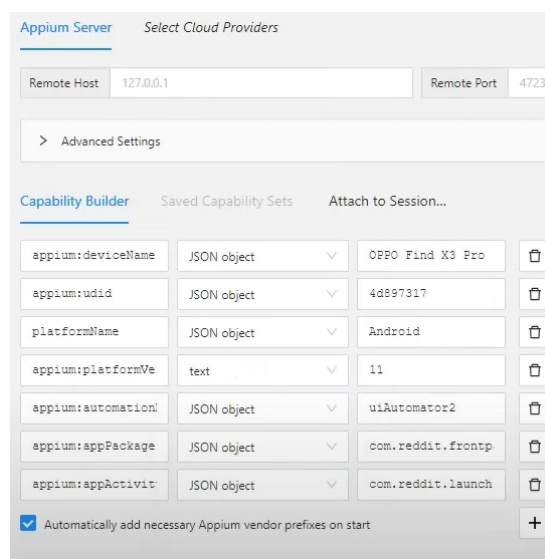


Рис.3.16 appium inspector

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

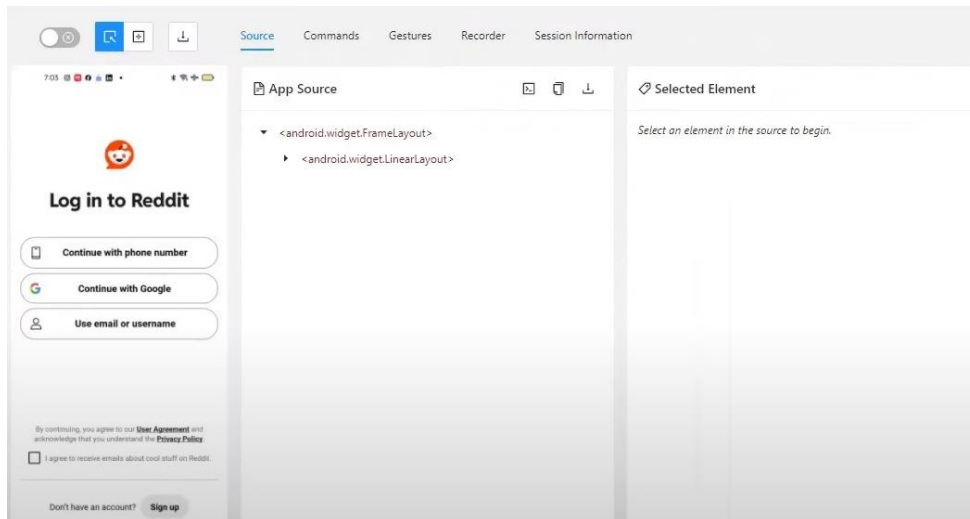


Рис.3.17. Сессія запущена

Запуск теста

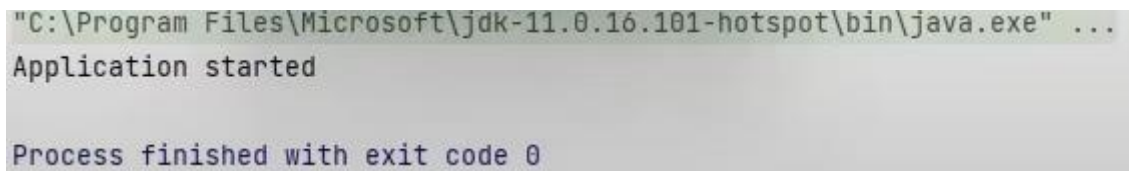


Рис.3.18

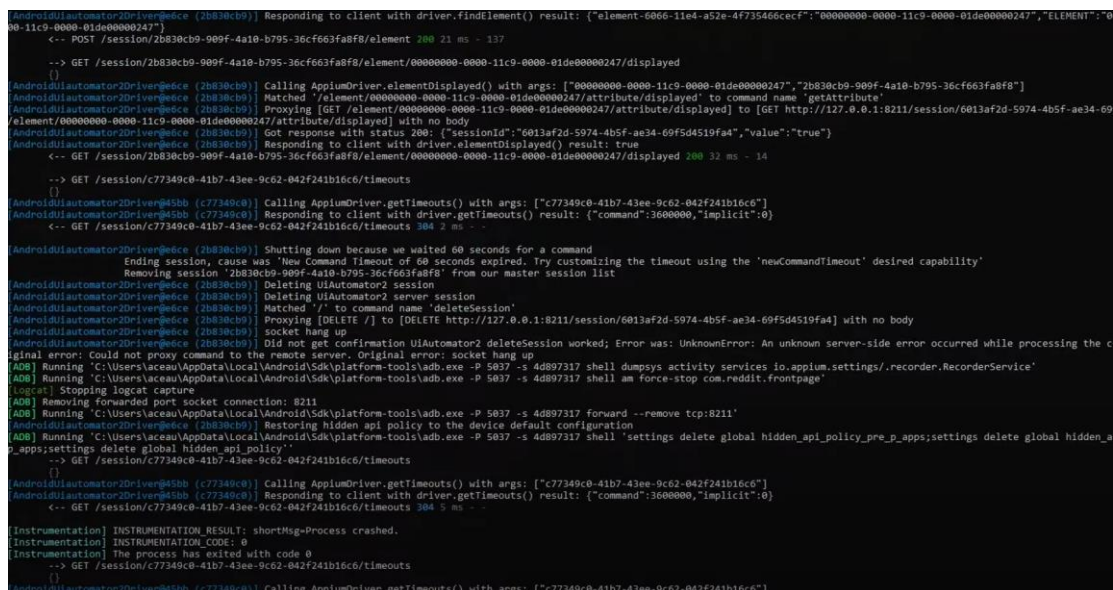


Рис.3.19 Appium Server в цей час

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштовуємо так щоб тест увійшов в акаунт та написав в пошуку Австралія.

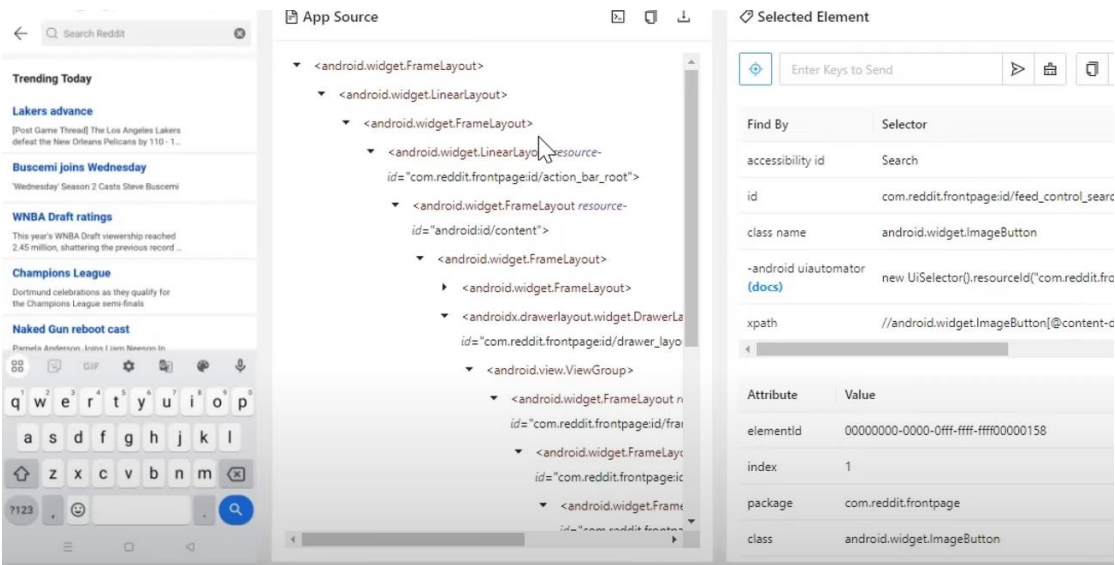


Рис.3.20

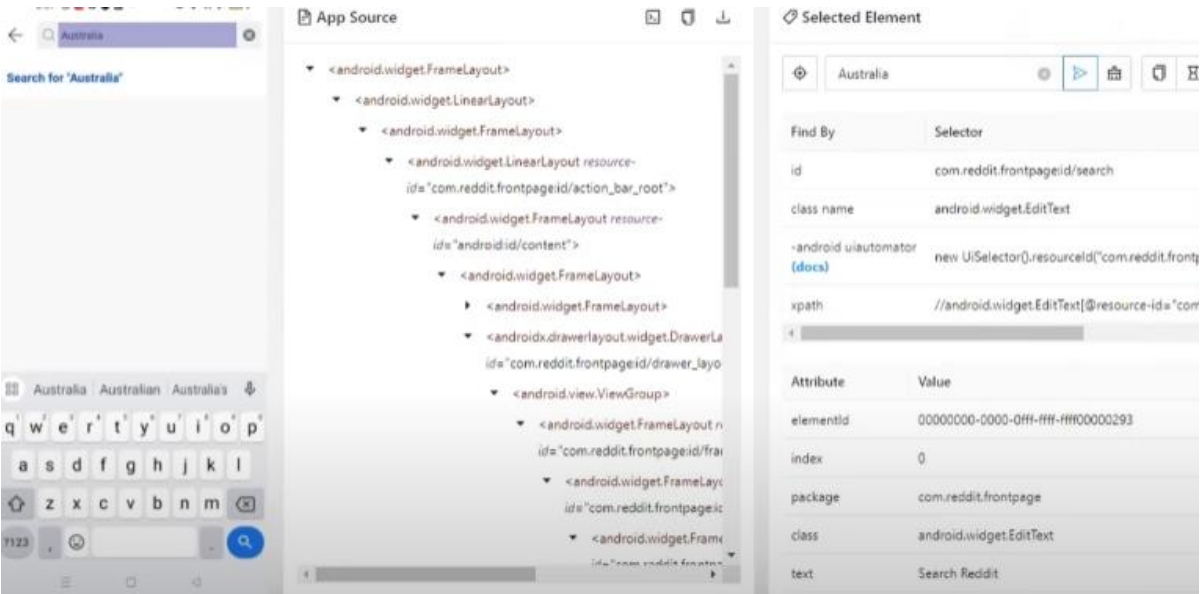


Рис.3.21

Запуск та вхід в Reddit

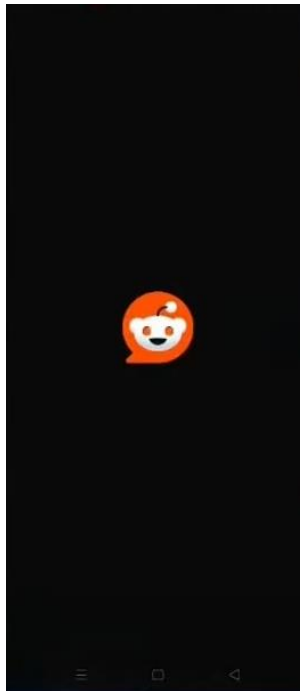


Рис.3.22 Reddit

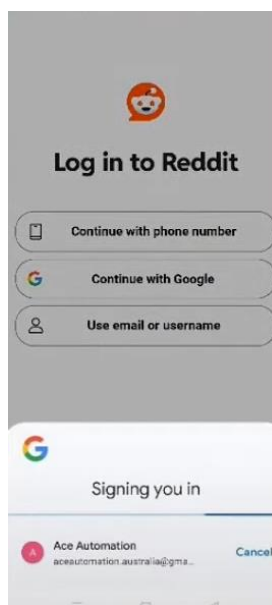


Рис.3.23 Вхід

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				62
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис.3.24 Вхід

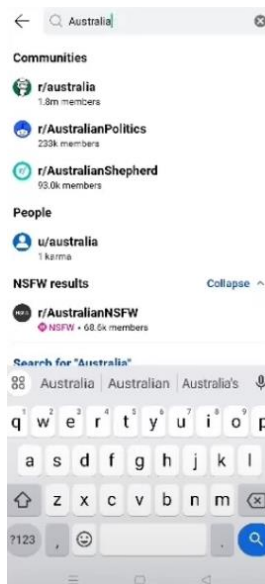


Рис.3.25 Пошук по запиту Австралія

Тестування вдале.

Для тестування мобільного додатка Reddit було налаштовано середовище з використанням Android Studio та Appium. Це дозволило ефективно автоматизувати процес тестування, включаючи авторизацію та пошук в додатку. Налаштування емулятора Android, запуск Appium Server та написання автоматизованих тестів забезпечили можливість проведення тестування на реальному пристрої чи емуляторі. Тестування продемонструвало успішний вхід у додаток та виконання пошуку за запитом що показало працездатність автоматизованого тестування.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Рекомендації

Увімкнути двофакторну аутентифікацію (2FA) - двофакторна аутентифікація додає додатковий рівень захисту, вимагаючи, крім пароля, ще й підтвердження через мобільний телефон або інший пристрій. У налаштуваннях облікового запису Reddit знайдіть розділ безпеки та увімкніть 2FA. Вам потрібно буде завантажити додаток для аутентифікації, наприклад, Google Authenticator.

Використовувати складний і унікальний пароль - складний пароль знижує ймовірність його підбору або зламу. Унікальний пароль, який не використовується на інших сайтах, зменшує ризик компрометації облікового запису через зламані інші сервіси. Пароль має містити комбінацію великих і малих літер, цифр і спеціальних символів. Використовуйте пароліні менеджери (наприклад, LastPass або 1Password) для створення та зберігання паролів.

Налаштувати конфіденційність - обмеження доступу до особистої інформації знижує ризик соціальної інженерії та небажаного доступу до вашого облікового запису. У налаштуваннях облікового запису Reddit, у розділі конфіденційності, обмежте видимість вашої особистої інформації, активності та постів тільки для довірених користувачів або друзів.

Регулярно оновлювати додаток - розробники регулярно випускають оновлення, які виправляють вразливості та покращують безпеку додатка. Увімкніть автоматичне оновлення додатків на вашому пристрої або регулярно перевіряйте наявність оновлень у Google Play Store або Apple App Store і встановлюйте їх.

Відслідковувати підозрілі дії - швидке виявлення підозрілої активності може допомогти запобігти несанкціонованому доступу до облікового запису та мінімізувати шкоду. Регулярно перевіряйте розділ безпеки в налаштуваннях облікового запису на наявність невідомих входів або підозрілих дій. Увімкніть повідомлення про підозрілу активність, якщо така функція доступна.

Регулярно дізнавайтеся про нові методи кібербезпеки і слідкуйте за новинами про потенційні загрози та вразливості.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Для підвищення безпеки інтернет-з'єднання використовуйте VPN, особливо при підключенні до публічних або незахищених мереж.

Робіть резервні копії важливих даних, щоб уникнути втрати інформації у разі зламу або технічних проблем.

Дотримуючись цих рекомендацій, ви значно знизите ризики для безпеки вашого облікового запису на Reddit та інших онлайн-сервісах.

Отже, забезпечення безпеки облікових записів є критично важливим для захисту особистої інформації та запобігання кіберзагрозам. Дотримуючись рекомендацій, таких як увімкнення двофакторної аутентифікації, використання складних паролів, налаштування конфіденційності та регулярне оновлення додатків, ви значно знизите ризик несанкціонованого доступу до ваших облікових записів. Постійне відслідковування підозрілої активності та підвищення обізнаності про нові методи кібербезпеки забезпечать додатковий рівень захисту ваших онлайн-активностей.

Висновок до третього розділу

У процесі тестування мобільного додатку було успішно налаштовано середовище розробки з використанням Android Studio та Appium, що дозволило ефективно автоматизувати тестування функціоналу, зокрема авторизації та виконання основних операцій у додатку. Застосування сучасних інструментів розробки та методик тестування забезпечило надійність та стабільність тестів.

З метою підвищення безпеки облікових записів рекомендується впровадження двофакторної аутентифікації, використання складних і унікальних паролів, а також регулярне оновлення програмного забезпечення. Крім того, важливо відслідковувати підозрілі активності та підвищувати обізнаність про нові методи кібербезпеки. Ці практики допоможуть знизити ризики несанкціонованого доступу до особистих даних та забезпечити безпеку користувачів під час використання мобільних додатків.

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

ВИСНОВКИ

Результати дослідження підкреслюють загальну вразливість мобільних додатків у сучасному цифровому середовищі. Мобільне шкідливе програмне забезпечення, фішинг та витік конфіденційної інформації є лише деякими з проблем, з якими стикаються користувачі та організації. Ці загрози можуть призвести до втрати особистої інформації, фінансових втрат, а також порушення робочих процесів та конфіденційності даних в бізнесі.

Для забезпечення безпеки мобільних додатків важливо вживати комплексний підхід, що включає технічні та організаційні заходи. Серед них - аудит безпеки програмного забезпечення, регулярне оновлення програм та операційних систем, навчання користувачів основам кібербезпеки та впровадження механізмів моніторингу та реагування на потенційні загрози.

Безпека мобільних додатків є важливою складовою загальної кібербезпеки в цифровому світі. Забезпечення високого рівня безпеки мобільних додатків потребує спільних зусиль розробників, постачальників послуг та кінцевих користувачів. Тільки колективні дії можуть допомогти запобігти серйозним наслідкам, які можуть виникнути внаслідок недостатньої уваги до безпеки мобільних додатків.

У світі, де мобільні додатки стали неодмінною частиною повсякденного життя, забезпечення їх безпеки є важливим завданням для розробників, користувачів та організацій. Постійний розвиток технологій і зростання кількості кіберзагроз ставлять під загрозу конфіденційність та безпеку інформації, що зберігається і оброблюється у мобільних додатках. Тому важливо вдосконалювати методи та інструменти для аналізу та виявлення потенційних загроз, щоб забезпечити безпеку та захист особистих даних користувачів.

Це дослідження підкреслює значення вживання різних підходів до аналізу безпеки мобільних додатків, включаючи статичний та динамічний аналіз, а також методи на основі штучного інтелекту. Інструменти, такі як SonarQube, Burp Suite

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

та Appium, допомагають у виявленні та виправленні вразливостей, забезпечуючи надійність та безпеку програмного забезпечення.

Загалом, застосування сучасних методів тестування та заходів забезпечення безпеки є критично важливим для забезпечення захисту інформації у мобільних додатках. Тільки за умови систематичного вдосконалення цих підходів можна забезпечити надійність та захист даних користувачів у цифровому віці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. Державна служба спеціального зв'язку та захисту інформації України. [Електроний ресурс] — Режим доступу: <https://scpc.gov.ua/uk/articles/334>
2. СТАТИЧНА І ДИНАМІЧНА МЕТОДИКИ ТЕСТУВАННЯ [Електроний ресурс] — Режим доступу: <https://training.qatestlab.com/blog/technical-articles/static-and-dynamic-testing-methods>
3. ТИПИ МОБІЛЬНИХ ДОДАТКИ [Електроний ресурс] — Режим доступу: <https://training.qatestlab.com/blog/technical-articles/types-of-mobile-applications/>
4. OWASP Mobile Application Security [Електроний ресурс] — Режим доступу: <https://owasp.org/www-project-mobile-app-security/>
5. SEC575: iOS and Android Application Security Analysis and Penetration Testing [Електроний ресурс] — Режим доступу: <https://www.sans.org/cyber-security-courses/ios-android-application-security-analysis-penetration-testing/>
6. Mobile Code Security, Improve the Security of Your Mobile Applications [Електроний ресурс] — Режим доступу: <https://www.veracode.com/security/mobile-code-security>

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

7. The Hacker News [Електроний ресурс] — Режим доступу: <https://thehackernews.com/search/label/mobile%20security>
8. Mobile App Security Best Practices In 2024 [Електроний ресурс] — Режим доступу: <https://www.wattlecorp.com/mobile-app-security-best-practices>
9. Захищеність і безпека мобільних додатків: Важливість аналізу [Електроний ресурс] — Режим доступу: <https://socserve.net/application-security.html>
10. What is Mobile Application Security? [Електроний ресурс] — Режим доступу: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/what-is-mobile-application-security/>
11. Identifying User-Input Privacy in Mobile Applications at a Large Scale [Електроний ресурс] — Режим доступу: <https://ieeexplore.ieee.org/document/7752986>
12. 2024 Mobile Application Security Trends [Електроний ресурс] — Режим доступу: <https://cybersecurity.asee.io/blog/mobile-application-security-trends/>
13. Mobile Security [Електроний ресурс] — Режим доступу: <https://www.mcafee.com/blogs/mobile-security/>
14. Mobile Security Definition and Solutions [Електроний ресурс] — Режим доступу: <https://www.cio.com/article/272207/mobile-mobile-security-definition-and-solutions.html>
15. 9 top mobile security threats and how you can avoid them [Електроний ресурс] — Режим доступу: <https://www.zdnet.com/article/9-top-mobile-security-threats-and-how-you-can-avoid-them/>
16. Як вберегти себе при встановленні мобільних додатків [Електроний ресурс] — Режим доступу: <https://nadiyno.org/yak-vberegty-sebe-pry-vstanovlenni-mobilnyh-dodatktiv/>

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

17. Android codelabs [Електроний ресурс] — Режим доступу:
<https://developer.android.com/get-started/codelabs>
18. Training courses [Електроний ресурс] — Режим доступу:
<https://developer.android.com/courses>
19. Appium in a Nutshell [Електроний ресурс] — Режим доступу:
<https://appium.io/docs/en/latest/intro/>
20. Migrating to Appium 2 [Електроний ресурс] — Режим доступу:
<https://appium.io/docs/en/latest/guides/migrating-1-to-2/>
21. Managing Drivers and Plugins [Електроний ресурс] — Режим доступу:
<https://appium.io/docs/en/latest/guides/managing-exts/>
22. Session Capabilities [Електроний ресурс] — Режим доступу:
<https://appium.io/docs/en/latest/guides/caps/>
23. Безпека в мобільних додатках: На що звернути увагу? [Електроний ресурс] — Режим доступу: <https://mindscope.biz.ua/bezpeka-v-mobilnyh-dodatkah-na-shho-zvernuty-uvagu/>
24. «Кібербезпека під час війни» [Електроний ресурс] — Режим доступу:
<https://rozdilna-rda.od.gov.ua/2023/05/kiberbezpeka-pid-chas-vijny/>

		Ільницький О.С.			ККІКБ.КР.Б – 125 – 08 – ПЗ	Арк.
		Пірог О.В.				69
Змн.	Арк.	№ докум.	Підпис	Дата		