Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Розробка рекомендацій щодо безпечного використання онлайн-гаманців у криптовалютній індустрії»

Виконавець: студент IV курсу, групи КБ-42

(підпис) **Дарія БЛОТНИЦЬКА** (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Андрій ФЕСЕНКО	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Дарії Володимирівні Блотницькій**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Розробка рекомендацій щодо безпечного використання онлайн-гаманців у криптовалютній індустрії

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Структури, класифікація, засоби функціонування криптогаманців. Алгоритми роботи. Злам та та порушення безпеки криптогаманців

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту інформації, нормативна база у сфері криптовалют та криптогаманців, будова та функціональність криптогаманців, ієрархія та систематизація, рекомендації, випадки зламу, компрометації та порушень безпеки криптогаманців, захист від загроз з боку користувача

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено рекомендації щодо використання онлайн-гаманців. Запропоновано класифікацію гаманців.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 01 листопада 2021 року

Завдання видав _____ Андрій ФЕСЕНКО
(підпис) (ініціали, прізвище)

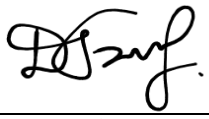
Завдання прийняв до виконання _____ Дарія БЛОТНИЦЬКА
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	01.11.2021 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2022 – 11.02.2022	*виконано*
3	Дослідження класифікації гаманців	12.02.2022 – 24.02.2022	*виконано*
4	Оцінка принципу роботи гаманців залежно від виду	25.02.2022 – 24.03.2022	*виконано*
5	Визначення та візуалізація функцій криатогаманців	25.03.2022 – 07.04.2022	*виконано*
6	Класифікація та структуризація методів зламу	08.04.2022 – 20.04.2022	*виконано*
7	Оцінка ефективності та доречності рішень щодо захисту гаманців	21.04.2022 – 05.05.2022	*виконано*
8	Формування рекомендацій щодо механізмів захисту гаманців	06.05.2022 – 20.05.2022	*виконано*
9	Обговорення із науковим керівником, виправлення помилок, коригування	21.05.2022 – 04.06.2022	*виконано*
10	Оформлення пояснювальної записки	05.06.2022 – 02.06.2022	*виконано*
11	Підготовка до захисту дипломної роботи	03.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ Андрій ФЕСЕНКО
(підпис) (ініціали, прізвище)

Завдання прийняв
до виконання



(підпис)

Дарія БЛОТНИЦЬКА
(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 60 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, список скорочень, висновки, список джерел. та 4 додатки із загальною кількістю сторінок 4. У пояснювальній записці дипломної роботи міститься 8 рисунків і 2 таблиці.

Метою роботи є розробка рекомендацій до захисту від кіберзагроз електронних криптогаманців користувачів.

Для розробки рекомендацій було поставлено такі цілі в роботі:

— дослідити законодавчу врегульованість та визначення гаманців в Україні;

— дослідити класифікацію гаманців за принципом роботи;

— дослідити, структурувати випадки зламу гаманців;

— визначити найбільші вразливості у гаманцях із точки зору користувача;

— розробити функціональну схему рекомендацій;

— розробити рекомендації щодо безпечного використання гаманців.

Об’єктом дослідження є процес протидії зламу гаманців.

Предметом дослідження є способи та методи захисту електронних криптогаманців, що надають можливість використовувати криптогаманці безпечно.

Наукова новизна полягає у розроблених рекомендаціях щодо використання криптогаманців, які не було представлено у жодних дослідженнях.

Практичною цінністю отриманих результатів є рекомендації щодо використання криптогаманців.

Результати здійснених у дипломній роботі досліджень можуть бути використані для убезпечення користувачів, коригування дизайну криптогаманців, розробки загальних рекомендацій та політики поводження із криптогаманцями.

Ключові слова: криптогаманці, онлайн-гаманці, криптовалюта, рекомендації використання.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

2FA – Two-Factor Authentication, двофакторна автентифікація

BTS – BitCoin, Біткоїн

FIN – FinCoin, Фінкоїн

MFA – Multi-Factor Authentication, багатофакторна автентифікація

OCR – Optical Character Recognition, оптичне роспізнавання символів

P2P – person to person, людина до людини

PIN – Personal Identification Number, особистий ідентифікаційний номер

SPV – Simplified Payment Verification, спрощена верифікація платежу

VPN – Virtual Private Network, віртуальна приватна мережа

WIF – Wallet Import Format, формат імпорту гаманця

ВСТУП

Україна є досить цифровою європейською країною. В Україні одні з найвищих показників широти розповсюдження та використання криптовалют у світі, згідно із останніми дослідами.

Актуальність роботи полягає у створенні рекомендацій для використання онлайн-гаманців в області криптовалютної індустрії, яка все більше розвивається. Вартість більшості криптовалют зростає. Вони набувають ширшого розповсюдження порівняно зі станом декількома роками раніше. У зв'язку із цим ціна втрати чи викрадення криптовалют збільшується. Цінність безпечних гаманців та, власне, валют, якщо вони у безпеці, усе збільшується із ціною криптовалют.

Новизна роботи полягає у вивченні способів забезпечити безпеку із боку користувача. Спеціалізованих досліджень щодо загроз та заходів безпеки саме з боку користувача, із боку використання, ще не проводилося.

Для розробки рекомендацій було поставлено такі цілі в роботі:

— дослідити законодавчу врегульованість та визначення гаманців в Україні;
— дослідити класифікацію гаманців за принципом роботи;
— дослідити, структурувати випадки зламу гаманців;
— визначити найбільші вразливості у гаманцях із точки зору користувача;
— розробити рекомендації щодо безпечного використання гаманців.

Робота містить у собі схему класифікації криптогаманців за їхніми функціями, інформацію щодо них, короткий метааналіз декількох робіт із дослідженнями виду роботи, вразливостей та відмінностей онлайн-гаманців, а також було розроблено рекомендації щодо використання гаманців. Крім того, було розглянуто законодавчі документи та визначено функціональність та законодавчу врегульованість криптовалют у різних країнах, включно із Україною.

Тези стосовно важливості цієї теми, актуальності та коректності даних, було апробовано на IV Науково-практичній конференції «Інтеграція інформаційних систем і інтелектуальних технологій в умовах трансформації інформаційного

суспільства», м. Полтава. Саме ця конференція була обрана через важливість розгляду теми в умовах сучасних технологій та змін у інформаційному середовищі, що ми бачимо на прикладі, зокрема, криптогаманців та криптовалют загалом.

РОЗДІЛ 1
НОРМАТИВНЕ ВИЗНАЧЕННЯ, СТРУКТУРА, КЛАСИФІКАЦІЯ КРИПТОГАМАНЦІВ

1.1 Нормативно-правова база у сфері криптовалют

Криптовалюта та операції із нею керуються у багатьох державах. Використання криптовалют урегульовано в Україні деяким чином. Проте досить багато аспектів усе ще є проблемою, адже операції із криптовалютами – одні із найшвидших, через що реакція на порушення має бути миттєвою. Також операції відслідковувати важче, ніж інші банківські операції. Проте усе ще легше, ніж обіг готівки в країні.

Обіг та операції із криптовалютами врегульовані в Україні лише двома законами і легальні межі (а отже, і вимоги). Обидва із цих законів не спеціалізуються суто на криптовалютах, через що потребують уточнення із розвитком криптовалют.

1.1.1 Нормативно-правова база в Україні

Найважливішим документом, який безпосередньо регулює криптовалют, є Закон України «Про запобігання та протидію легалізації доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового ураження». Зокрема, до переліку для фінансового моніторингу додано організації, діяльність яких пов’язана з обліком в електронній валюті. Тому, якщо компанія має платежі в будь-якій криптовалюті на суму 30 тис. грн та більше, вона має перевірити цю транзакцію та визначити інформацію про клієнта. Із боку клієнта, останній зобов’язаний надавати повну інформацію про походження та призначення своїх віртуальних активів. Якщо буде встановлено, що ці кошти було

отримано незаконно, операцію зупинити неможливо, але криптовалюта може бути заблокована, а незаконно придбані криптовалюти можуть бути конфісковані. [1]

Також розглядатимуть законопроєкт № 2461 «Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами», зокрема там визначено такі слова як: «віртуальний актив», «криптовалюта операція», «криптовалюта», «токен», що допоможе уникнути проблем у законодавстві щодо тлумачення таких виразів. Законопроект також встановлює правила оподаткування операцій щодо криптовалют, 18% податку для організацій і 5% для фізичних осіб. Цей проект іще знаходиться на розгляді органів влади. [2][3][4]

1.1.2 Розповсюдженість криптовалют в Україні та світі

Таблиця 1

Розповсюдженість криптовалют за зваженим індексом

Країна	Бал	Місце	Місце індивідуально зваженої метрики			
			Отримана вартість криптовалюти в мережі	Перенесена роздрібна вартість	Кількість криптовалютних депозитів у мережі	Торгівля P2P
Україна	1	1	4	4	7	11
Росія	0.931	2	7	8	5	9
Венесуела	0.799	3	19	14	15	1
Китай	0.672	4	1	1	95	53
Кенія	0.645	5	37	11	57	1
США	0.627	6	5	6	39	16

Раніше були проведені дослідження щодо широти розповсюдження та використання криптовалют у світі. Тут ми маємо оцінку того, наскільки в країнах часто та багато використовуються криптоактиви. аналіз проводився на основі індивідуально розробленої системи оцінювання за чотирма параметрами:

— Отримана вартість криптовалюти в мережі, зважена за паритетом купівельної спроможності (ПКС) на душу населення.

Метою цього показника є ранжування кожної країни за загальною криптовалютною активністю, але оцінка рейтингу на користь країн, де ця сума є більш значною, виходячи з багатства середньої людини та вартості грошей загалом у країні.

— Перенесена роздрібна вартість у мережі, зважена за ПКС на душу населення.

Метою цього показника є вимірювання активності непрофесійних індивідуальних користувачів криптовалюти на основі того, скільки криптовалюти вони здійснюють трансакції в порівнянні з багатством середньої людини.

— Кількість криптовалютних депозитів у мережі, зважена за кількістю користувачів Інтернету.

Мета цього показника — ранжувати країни на основі того, чиї резиденти здійснюють найбільшу кількість транзакцій з криптовалютою.

— Одноранговий обсяг біржової торгівлі, зважений за ПКС на душу населення та кількістю користувачів Інтернету.

На відміну від наших трьох інших показників, обсяг торгівлі P2P не виражається в блокчейнах, але все ще становить значний відсоток усієї криптовалютної активності, особливо в країнах, що розвиваються. Ми ранжуємо країни за обсягом P2P-торгівлі та враховуємо його, щоб надати перевагу країнам з нижчим ППС на душу населення та меншою кількістю користувачів Інтернету, метою є виділення країн, де більше жителів вкладають більшу частку свого загального багатства в транзакції з криптовалютою P2P. Отже, Україна посідає найперше місце за зваженим індексом використання криптовалют незважаючи на недостатність юридичної бази із цього питання. [5]

1.1.3 Регулювання в інших країнах та загрози

У багатьох країнах криптовалюти використовуються для відмивання коштів, торгівлі зброєю або наркотиками, фінансування тероризму. Це відбувається, бо всі

дані про криптовалютні транзакції зберігаються у децентралізованому загальному доступі системи блокчейн. Зазначене дає більші можливості для регуляції з боку держави, та не створює проблем як з регуляцією обігу готівкових операцій. Наприклад, Податковою службою Сполучених Штатів Америки з 2015 року використовується програмне забезпечення, яке надає можливість відстежувати рух криптовалюти, визначати її походження та ідентифікувати власника, у Японії повністю легалізована криптовалюта та контроль за діяльністю здійснює Агентство фінансових послуг. [6]

1.2 Гаманці: функція та класифікація

Криптовалютний гаманець - це захищений цифровий гаманець, який використовується для зберігання, надсилання та отримання цифрових валют. Більшість монет мають офіційний гаманець, проте є вони часто підтримують і інші валюти.

Для цієї роботи критично необхідно визначити види та функції гаманців для криптовалюти, щоб базувати вимоги до них, слабкі місця та очікувані проблеми, що розглядатимуться у третьому розділі.

1.2.1 Функції гаманців

Гаманець служить таким функціям:

— зберігання криптовалют;
— надсилання криптовалют (створення транзакцій);
— отримання криптовалют;
— зберігання приватного ключа на носії;
— витягування та дешифрування приватного ключа;
— перевірка балансу;
— підпис транзакції;

— вхід або реєстрація;

— отримання та робота із хешем транзакції.

Отже, гаманці дозволяють робити деякі операції, включно із такими, як взаємодіяти з блокчейном, робити покупки
та транзакції, контролювати баланс. Це основні категорії, у які можна об’єднати найкритичніші функції гаманців. [7]

1.2.2 Класифікація гаманців

Коли один користувач надсилає іншому криптовалюту, одержувач повинен мати можливість зіставити приватний ключ із відкритим ключем, щоб розблокувати кошти та витратити активи. Хоча обміну монет або валюти немає, здійснена транзакція відображається в записі транзакції в блокчейні. Це, у свою чергу, призводить до зміни балансу криптовалютного гаманця відправника та одержувача. Існують різні типи гаманців, наприклад: настільні, мобільні та веб-гаманці, залежно від платформи та пристрою, на якому вони використовуються. Залежно від типу криптовалюти, гаманця та типу транзакції може бути додана комісія за транзакцію, значення якої змінне. Холодні гаманці – найбезпечніший метод зберігання криптовалют. Але вони потребують більш технічних знань для налаштування. Хороший спосіб налаштувати гаманці — це мати три речі: біржовий рахунок для покупки та продажу, гарячий гаманець для утримання малих або середніх сум криптовалют, які є у швидкому доступі для різноманітних маніпуляцій, і холодний апаратний гаманець для зберігання великих сум в довгострокові терміни. Холодний гаманець немає доступу до інтернету, та має набагато менші ризики бути скомпрометованим. Ці гаманці також можуть називатися автономними гаманцями або апаратними гаманцями. Ці гаманці утримують приватні ключі користувача на чомусь, що не підключено до інтернету, і може постачатися з програмним забезпеченням, яке працює паралельно, щоб користувач міг переглядати свої накопичення, не наражаючи на ризик закритий ключ. Найбезпечніший спосіб

зберігання криптовалюти в автономному режимі - це паперовий гаманець. Паперовий гаманець – це гаманець, який можна створити на певних веб-сайтах. Потім він створює відкриті та закриті ключі, які потрібно роздрукувати на аркуші паперу. Можливість отримати доступ до криптовалюти за цими адресами можлива, лише за наявності приватного ключа. Ці гаманці призначені для довгострокових інвестицій, не можливо швидко продати або обміняти біткойни, збережені таким чином.

Більш поширеним типом холодного гаманця є апаратний гаманець. Апаратний гаманець, як правило, є USB-накопичувачем, який безпечно зберігає приватні ключі користувача в автономному режимі. Такі гаманці мають серйозні переваги перед гарячими гаманцями, оскільки на них не впливають віруси, які можуть бути на приватному комп'ютері. З апаратними гаманцями приватні ключі ніколи не контактують з комп'ютером, підключеним до мережі, або потенційно вразливим програмним забезпеченням. Ці пристрої також зазвичай мають відкритий код, що дозволяє спільноті визначити їх безпеку за допомогою аудиту коду, а не компанії, яка оголошує, що вони безпечні у використанні.

Настільні гаманці встановлюються на настільний або портативний комп'ютер і надають користувачеві повний контроль над гаманцем. Деякі гаманці для настільних комп'ютерів також містять додаткові функції, наприклад програмне забезпечення вузлів або інтеграцію обміну. Проте настільні гаманці вважаються відносно небезпечними через небезпеку скомпрометації комп'ютера. Деякі добре відомі гаманці для настільних комп'ютерів – це Bitcoin Core, Armory, Hive OS X і Electrum.1.

Мобільні гаманці виконують ті ж функції, що й настільний гаманець, але на смартфоні чи іншому мобільному пристрої. Мобільні гаманці можуть полегшити швидкі платежі у фізичних магазинах за допомогою зв'язку ближнього поля (NFC) або сканування QR-коду. Мобільні гаманці, як правило, сумісні з iOS або Android. Прикладами мобільних гаманців є Bitcoin Wallet, Hive Android і Mycelium Bitcoin Wallet. Було багато випадків шкідливого програмного забезпечення, замаскованого

під гаманець біткойн, тому потрібно ретельно дослідити їх різновидність, перш ніж вирішити, який з них використовувати.

Веб-гаманець — це онлайн-сервіс, який може надсилати та зберігати криптовалюту від імені користувача. Основна перевага вебгаманців полягає в тому, що до них можна отримати доступ з будь-якого місця, з будьякого пристрою, так само легко, як і перевірити електронну пошту. Однак безпека є серйозною проблемою. Окрім ризиків зловмисного програмного забезпечення та фішингу для крадіжки паролів користувачів, існує також значний ризик контрагентів. [8]

Отже, види гаманців:

1. За принципом роботи

— холодні;

— гарячі.

У системі гарячих/холодних гаманців гарячий гаманець постійно підключений до мережі, а холодний гаманець зберігає секретний ключ на незалежному від мережі носії і працює автономно. Тобто, останній може функціонувати і без підключення до Інтернету.

2. За побудовою гаманці поділяють на:

— електронні: (мобільні, десктопні, веб-);

— апаратні;

— паперові. [9]

Паперовий гаманець – здебільшого папір, на якому надрукована інформація щодо деталей акаунту. А саме криптоадреса та її приватний ключ у вигляді QR коду. Паперові криптогаманці мають такі переваги:

— вони простий у використанні;

— забезпечують дуже високий рівень безпеки.

Хоча слово «паперовий гаманець» стосується також фізичної копії або роздруківки ваших публічних та приватних ключів, він також може означати програмне забезпечення, яке використовується для генерації ключів, надрукованих пізніше. Наразі використовують обидва значення.

Вони визнані найбільш ризикованою формою холодних гаманців, оскільки їх можливо випадково викинути, втратити фізично, пролити на них щось, загубити. Також, такі гаманці призначені для пересилання повністю усіх коштів за раз. Тому буде неможливо їх використовувати для маленьких транзакцій.

Апаратні гаманці є фізичними електронними пристроями. Вони використовують генератор випадкових чисел для генерування приватного та відкритого ключа. Вищезгадані паролі зберігаються на автономному пристрої, який не має підключення до мережі Інтернет. Апаратний гаманець відноситься до типу холодного зберігання і вважається найбільш безпечним.

Як правило, апаратний гаманець схожий на USB-пристрій, який має OLED-екран і керується кнопками з боків. Зазвичай має власні настільні програми для різних криптовалют.

Цей тип гаманців відрізняється від інших тим, що він зберігає приватні ключі оффлайн, на самому гаманці, фізично. Такі гаманці передають кошти в режимі онлайн, але залишаються в автономному режимі для додаткової безпеки. Хоча ці гаманці вразливі до кібератак, вони можуть бути пошкоджені через погану реалізацію мікропрограми.

Електронний гаманець – це гаманець, який працює при підключенні до Інтернету, це може бути програма, завантажена на комп’ютер чи телефон, або веб-гаманець. На даний момент електронні гаманці є найпопулярнішими, оскільки вони досить прості у використанні і їх можна використовувати в будь-якому місці та в будь-який час через Інтернет.

Існують різні типи електронних гаманців, кожен з яких має свої унікальні особливості.

Веб-гаманці є підвидом електронних гаманців. Такі гаманці доступні через браузери. Веб-облікові акаунти отримують доступ до блокчейнів через інтерфейс браузера, без того, щоб встановлювати документи безпосередньо на пристрій, що використовується. Це включає обмінні гаманці, а також інші гаманці на основі браузера. Часто є можливість створити гаманець і поставити на нього свій

особистий пароль, але не в усіх випадках. Багато служб та сервісів зберігають та керують приватними ключами замість користувача, що, безумовно, є проблемою безпеки.

Ще один вид електронного гаманця – настільні програми. Як випливає з назви, це програмне забезпечення, що завантажується та запускаєте локально на своєму комп'ютері. На відміну від деяких онлайн-версій, вони надають користувачеві повний контроль над ключами та грошима. Такі гаманці прості у використанні, забезпечують конфіденційність, анонімність і не залучають жодних посередників. Загалом настільні гаманці можна вважати більш безпечними, ніж більшість онлайн-версій. Проте це працює лише якщо на досліджуваному комп'ютері немає вірусів та шкідливих програм.

Мобільні гаманці працюють так само, як і настільні, але розроблені спеціально для додатків для смартфонів. Вони досить практичні, оскільки дозволяють відправляти та отримувати криптовалюти через QR-коди. Як висновок, такі гаманці якнайкраще підходять для повсякденних транзакцій і платежів, що робить їх адекватним способом витрачання криптовалюти в реальному світі. [10]

Базуючись на усьому вищезгаданому, автором було розроблено схему для класифікації гаманців (рисунок 1).

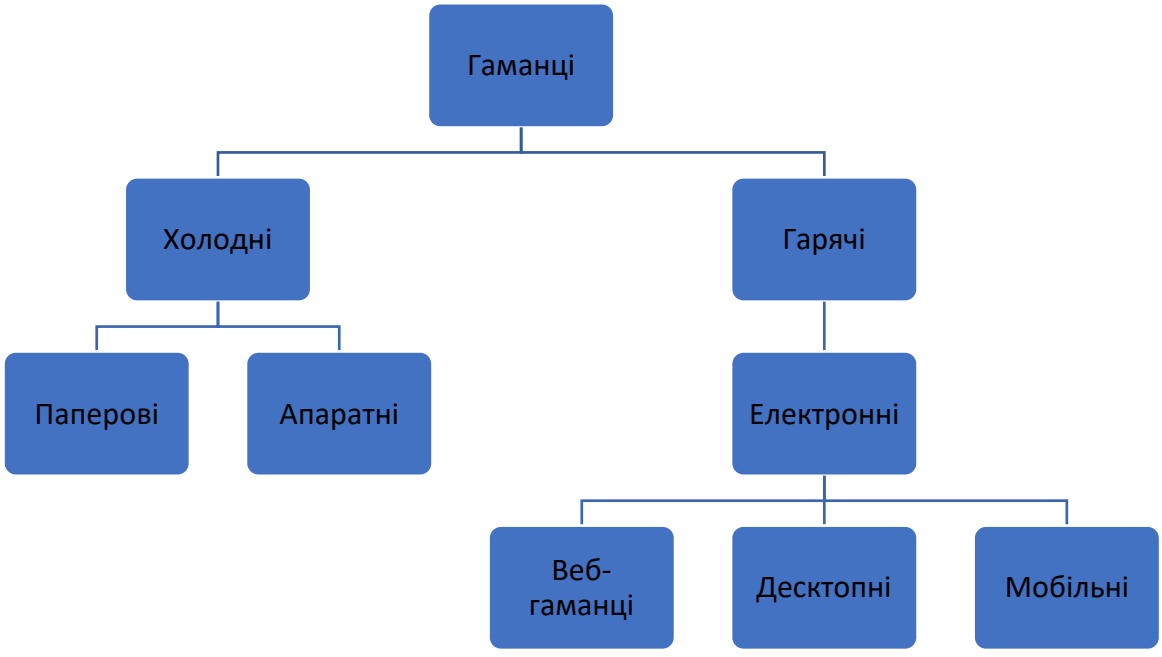


Рисунок 1 – Схема класифікації криптогаманців

Висновки за розділом 1

У розділі 1 було розглянуто деякі базові поняття, які необхідні для подальшого вивчення та аналізу безпечного використання криптогаманців. Було представлено схему класифікації гаманців. Було розглянуто юридичні особливості регулювання криптовалюти та криптогаманців у різних країнах. У багатьох закони щодо цієї частини недостатньо розвинені чи ще формуються. Держава може сприймати криптовалюту у різні способи. Не врегульовано, які саме вимоги ставляться до криптогаманців. Проте було визначено функції, які гаманці мають виконувати, залежно від виду. Було визначено основні та критичні функції.

Проведено аналітичний огляд документів, що регулюють обіг та роботу із криптовалютами, зокрема в Україні. Проведено огляд та аналіз наявних криптогаманців, візуалізовано класифікацію криптогаманців за типом роботи. Визначено функції криптогаманців, які є критичними для їхнього функціонування, на основі аналізу даних щодо їхньої роботи та звітів розробників криптогаманців.

РОЗДІЛ 2
ВРАЗЛИВОСТІ ТА АТАКИ НА КРИПТОГАМАНЦІ

Для створення рекомендацій у цьому розділі буде насамперед розглянуто те, яким атакам піддаються онлайн-гаманці та що саме є вузьким місцем у забезпеченні безпеки гаманців. На рисунку 2 представлено модель зображення криптогаманців за їхніми якостями з точки зору користувача.

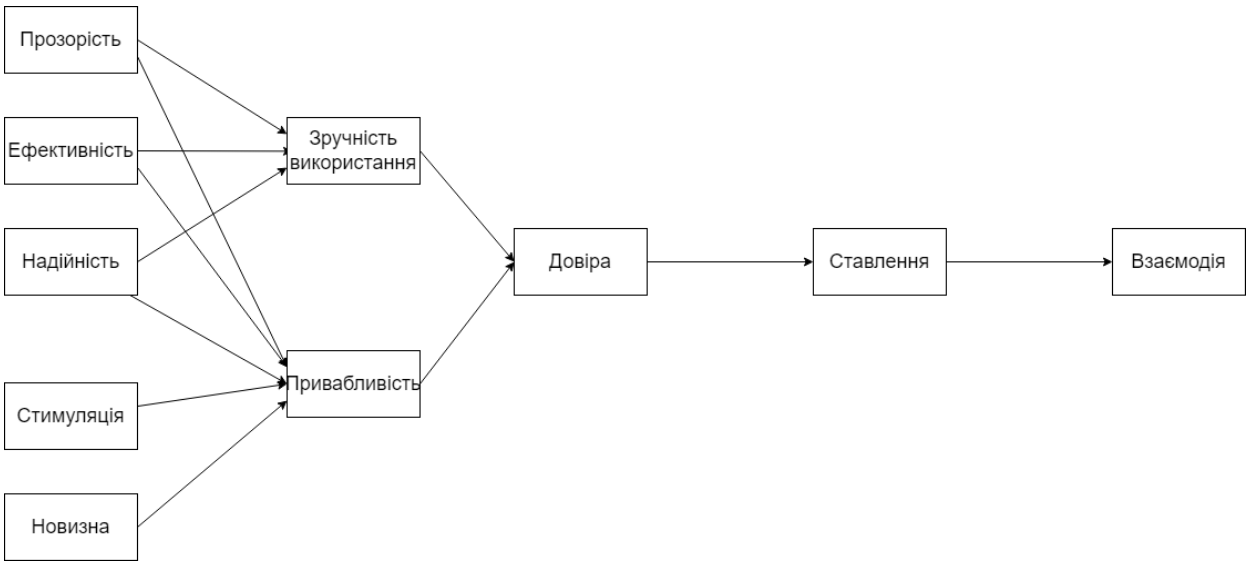


Рисунок 2 – Схема зображення криптогаманців з точки зору користувача

Оскільки ми розглядаємо рекомендації для користувачів, ми маємо також прийняти до уваги те, як ця робота виглядатиме з перспективи користувачів. У межах іншого дослідження було розроблено модель взаємодії та досвіду користувачів під час використання та щодо використання електронних гаманців. В моделі розглядаються аспекти User Experience, на які користувачі звертають увагу.

Однією із проміжних цілей створення безпечних гаманців є адекватна оцінка користувачем ситуацій із довірою та надійністю, які можуть виникати у додатку; наданих додатку прав; оцінки небезпечних ситуацій. Менше з тим, необхідно також упевнитися в ефективності та юзабельності гаманців.

Надійність — це рівень автономності, який показує, чи є послуга чи продукт незалежними чи контрольованими користувачем. Під час взаємодії між користувачем і сервісом відбувається багато речей; він може показувати безпечне та підтримуване середовище та відповідати очікуванням користувачів. Надійність відповіла на питання, чи відчуває користувач, що контролює взаємодію? Надійність продукту символізує унікальність та ідеал послуги. Чим надійніший продукт, тим вище зручність використання і тим він привабливіший. У цій статті надійність використовується для вимірювання автономності криптовалютних гаманців, показуючи, чи відчуває користувач захищеним і підтримується гаманцем, і чи очікуються функції.

Довіра визначається як враження, що дані, введені в продукт, перебувають у надійних руках і не шкодять. Довіру можна оцінити за різними категоріями: надійними, чесними, залежними та не опортуністичними. Довіра актуальна в ситуаціях, коли користувач стикається з ризиком і коли він/вона не може контролювати, що там відбуватиметься заздалегідь. Насправді, довіра є невід’ємним елементом додатка на основі технології блокчейн, який змушує користувачів відчувати себе впевнено під час використання. Зв'язок між довірою та ставленням демонструє сильну кореляцію, яка опосередковано впливає на поведінку клієнтів. Довіра добре відома як фактор, який позитивно впливає на ставлення користувачів, що відбивається на намірах клієнта. Існує багато непорозумінь щодо технології блокчейн та криптовалюти, і багато звичайних користувачів мають проблеми з довірою. Підвищення довіри до криптовалюти показало позитивний вплив на рівень використання. У цій статті довіра використовувалася як залежна змінна для вимірювання довіри користувачів до криптовалютних гаманців. Важливо оцінити рівень довіри та переконатися, що гаманець заслуговує на довіру. Використання криптовалютного гаманця зазвичай супроводжується певним рівнем ризику, що змушує терміново оцінити та підтримати довіру користувачів.

Схему було розроблено на прикладі гаманців, базованих на Android. [11]

2.1 Аналіз атак та випадків зламу

Не зважаючи на досить широку розповсюдженість гаманців та велику роботу, вкладену в їхню ефективність, можна визначити найслабші місця у безпеці з точки зору використання, тобто, тих заходів, які може запровадити користувач до своїх онлайн-гаманців. На рисунку 3 зазначено кількість шкідливих біткойн-акаунтів чи зловживань такими акаунтами залежно від року.

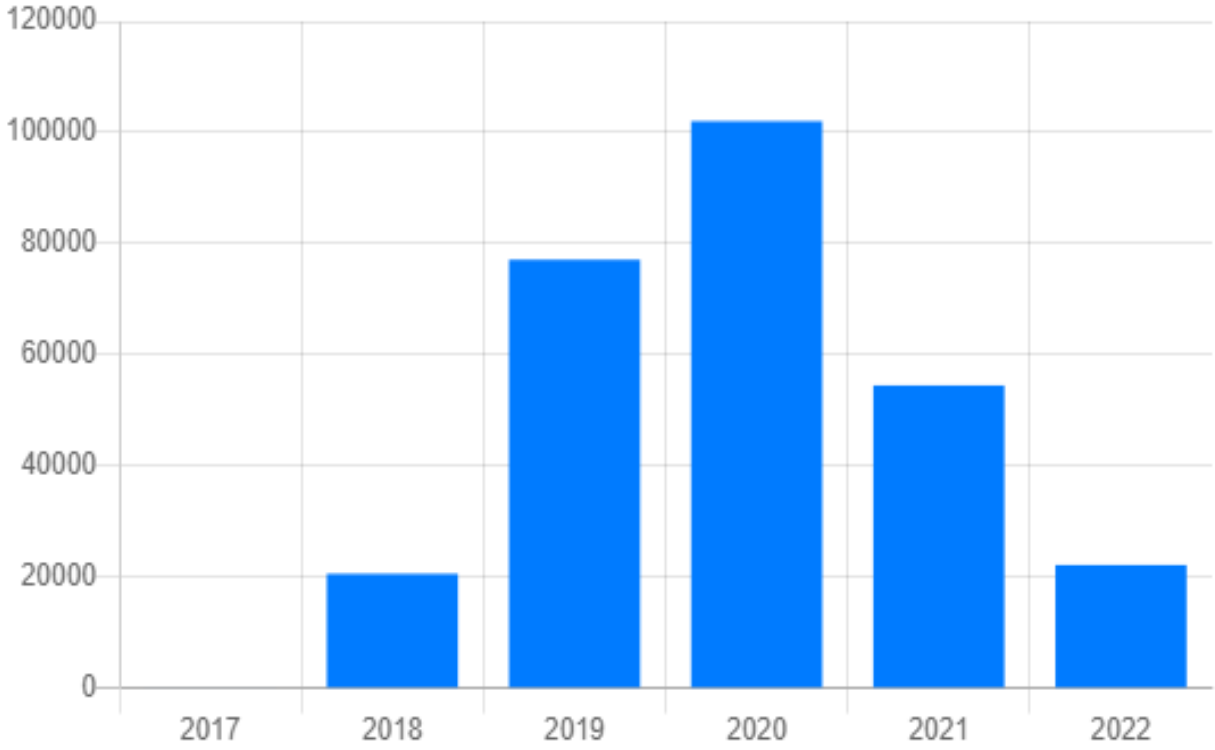


Рисунок 3 – Кількість шкідливих біткойн-акаунтів чи зловживань акаунтами

Згідно до статистики, зловживання онлайн-гаманцями та атаки на них є досить розповсюдженою проблемою. У статистику включено кількість адрес, якими користуються програми-вимагачі, шантажисти, шахраї тощо. Як бачимо, їхня кількість сягає десятків та навіть до сотні тисяч на рік. Необхідно дослідити детальніше, які саме атаки розповсюджені найбільше. [12]

2.1.1 Отримання конфіденційної інформації з файлу резервної копії за допомогою USB Debugging

Коли розробники програмного забезпечення Android проводять тестування на пристроях Android, їм потрібно увімкнути режим налагодження USB, коли вони підключають пристрій Android до комп’ютера для резервного копіювання або розробки. Зловмисник може використовувати комп’ютер для роботи на пристрої користувача, якщо на комп’ютері встановлено шкідливе програмне забезпечення. При цьому користувач не отримає жодних сповіщень. Параметр android:allowBackup=true у профілі AndroidManifest.xml , який міститься в кожній програмі, має значення true за замовчуванням. Якщо для нього встановлено значення false, ми не зможемо створити резервну копію даних програми за допомогою команди adb backup. Навіть якщо це не спрацює, зловмисник також може спробувати отримати локальні файли резервної копії на мобільному пристрої. Деякі локальні реалізації резервного копіювання можуть ігноруватиandroid:allowBackup=false конфігурація в профілі Android Manifest.xml . У системі MIUI на базі Android, проходячи через кожен файл у локальному каталозі резервної копії "/sdcard/MIUI/Backup/AllBackup/backup/backup time/", імена файлів видають відповідну програму файлу резервної копії.

Детальніше проілюстровано на рисунку 4.

Рисунок 4 – Використання USB Debugging для отримання інформації

Після отримання файлу резервної копії він розпаковується відповідно до формату файлу резервної копії. Потім, відповідно до певних форматів приватного ключа, мнемонічного слова, сховища ключів і WIF (формат імпорту гаманця), кожен з них може бути витягнутий. Конфіденційну інформацію можна проаналізувати за допомогою зіставлення регулярних виразів.

Після виконання команди adb backup на комп’ютері для гаманців Bitcoin.com і BitPay ми можемо отримати доступ до файлу резервної копії. Оскільки гаманці Bitcoin.com і BitPay не встановлюють PIN-код, мнемонічне слово можна отримати з файлу резервної копії. Неможливо створити резервну копію інших гаманців, оскільки налаштування параметра для android:allowBackup = false.

2.1.2 Визначення конфіденційної інформації на знімках екрана

Деякі користувачі можуть зберігати скріншоти, що містять конфіденційну інформацію, локально, це дає зловмиснику можливість отримати конфіденційну інформацію. Зловмисник може створити шкідливе програмне забезпечення та отримати дозвіл READ_EXTERNAL_STORAGE. Коли зловмисне програмне забезпечення знаходить знімок екрана, пов'язаний з гаманцем, OCR (Optical Character Recognition) може допомогти перетворити зображення в текст і отримати з нього інформацію. Нижче це описано більш детально:

1. Виявлення змін зображення: Android надає постачальник вмісту ContentProvider і відповідний механізм ContentResolver для обміну інформацією між додатками. Використовуючи ContentResolver для реєстрації слухача за допомогою MediaStore.Images.Media.EXTERNAL_-CONTENT_URI, зловмисне програмне забезпечення отримуватиме сповіщення, коли зображення на пристрої змінюються.

2. Коли створюється новий знімок екрана, процес прослуховування запитує останню картинку медіа-бібліотеки: запускається функція handleWindowContentChange() , і ContentResolver використовується для отримання останнього зображення. Потім, відповідно до розміру зображення, ключові слова шляху зберігання (наприклад, назва пакета гаманця), скріншоти гаманця ідентифікуються.

3. Вилучення конфіденційної інформації на знімку екрана: спочатку ідентифікований скріншот гаманця перетворюється у форму байтів. Потім він передається в Tencent OCR (або будь-який інший інструмент оптичного розпізнавання символів) для вилучення конфіденційної інформації. Результат повертається у вигляді рядка у форматі JSON.

Детальніше показано на рисунку 5.

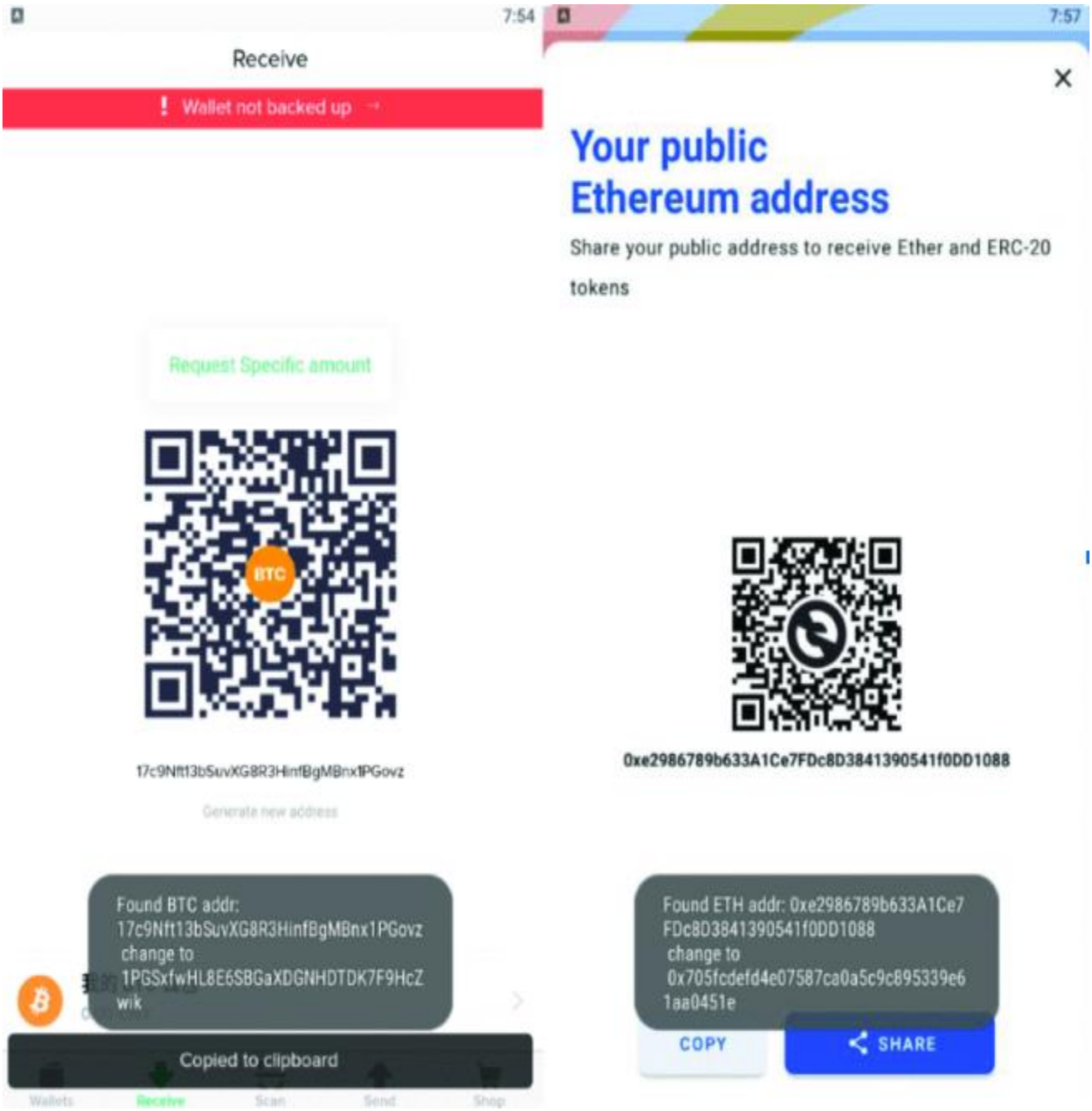


Рисунок 5 – Копіювання з екрана

Для більшості гаманців криптовалюти, як правило, WindowManager.LayoutParams.FLAG_SECURE буде встановлено в активності Android для безпеки. Це означає, що ця програма забороняє робити знімки екрана та записувати екран. Проте все ще є гаманці, які дозволяють робити знімки екрана, як-от Coinbase. Таким чином, зловмисник може захопити приватний ключ, мнемоніку тощо.

2.1.2 Отримання конфіденційної інформації з копіювання та вставляння

Як правило, закритий ключ криптовалютних гаманців, сховища ключів та іншої конфіденційної інформації складається здебільшого з випадкових символів і занадто довгі, щоб їх запам’ятати. Тому цілком ймовірно, що користувач введе їх шляхом копіювання та вставки. Звичайно, є деякі фреймворки, що забезпечують автоматичне заповнення приватних ключів, наприклад AutoFill Framework, openYOLO, але вони піддаються ризику витоку паролів користувачів . [13]

Android надає ClipboardManager для програм для повного моніторингу, читання та зміни вмісту буфера обміну. Коли слухача додають до буфера обміну, слухач отримує сповіщення про зміну вмісту буфера обміну. Шкідливе програмне забезпечення може використовувати цю функцію для вилучення конфіденційної інформації з буфера обміну відповідно до формату приватного ключа, мнемоніки, сховища ключів, приватного ключа формату WIF.

На рисунку 6 представлено виконання вищеописаної атаки на гаманець.

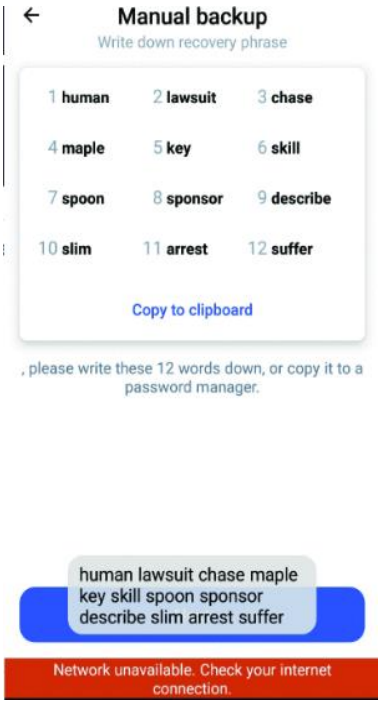


Рисунок 6 – Отримання інформації через буфер обміну

Для деяких гаманців конфіденційна інформація автоматично отримується, коли користувач копіює конфіденційну інформацію, таку як мнемоніки та закритий ключ. За допомогою цієї атаки успішно отримано 12 повних мнемонік. Для всіх гаманців, коли користувач копіює адресу гаманця, вона може бути автоматично замінена адресою, встановленою зловмисником без будь-якого попередження.

2.1.3 Крадіжка конфіденційної інформації за допомогою служби доступності

На рисунку 7 продемонстровано виконання атаки крадіжки конфіденційної інформації за допомогою служби доступності. Отже, служба доступності надає дозволи на отримання більшості інформації, що відображається на екрані, за винятком текстового поля пароля, яке за замовчуванням захищене. Однак існують методи отримання пароля, наприклад контроль введення користувача за допомогою програмної клавіатури. Ці програмні клавіатури часто використовують різні сторонні методи введення. У популярному програмному забезпеченні для керування паролями keepass2android, коли натискається його власна віртуальна клавіатура, слот для клавіші створює візуальний зворотний зв’язок і запускає події TYPE_WINDOW_-STATE_CHANGED. Коли введено пароль гаманця, зловмисник може визначити пароль користувача, прослухавши подію кліку.

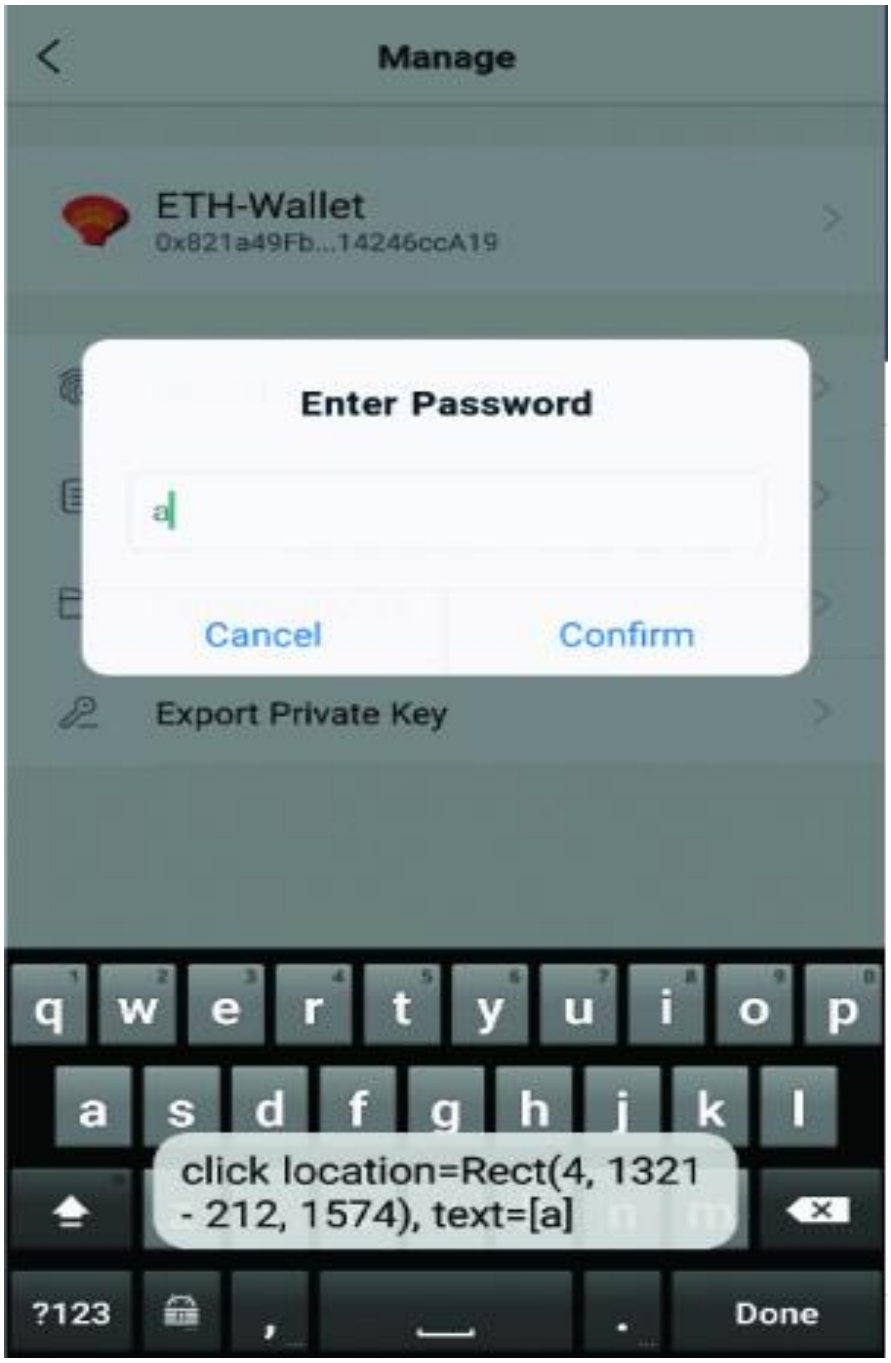


Рисунок 7 – Атака на сервіс доступності

Якщо припустити, що під час введення пароля використовується метод введення Keepass2android, зловмисник спочатку отримує розкладку клавіатури Keepass2android, яка залишається незмінною, тож зловмисник може записати та визначити ключ-значення, на якому було натиснуто клавішу, за місцем з часом. Деякі гаманці дозволяють вводити паролі сторонніми методами введення, а інші повинні використовувати власні захищені клавіатури. [14]

2.1.4. Атака деанонімізації

Ця атака спрямована на деанонімізацію анонімних біткойн-адрес і транзакцій користувача додатка для смартфона-гаманця біткойн.

Останніми роками деанонімізація біткойна є популярною темою дослідження. Gervais та ін. продемонстрували, що якщо клієнт SPV-додатку має невелику кількість біткойн-адрес (наприклад, < 20), то ймовірність того, що супротивники зможуть правильно вгадати всі ці адреси біткойн, використовуючи один фільтр із перехопленого повідомлення про завантаження фільтра, становить 80%. , тоді як фільтр використовує цільову частоту помилкових позитивних результатів 0,05%. Однак рівень техніки має три ключові обмеження. По-перше, супротивники можуть бути не в змозі перехопити фільтр, переданий жертвами, якщо супротивники не можуть постійно спостерігати за жертвами протягом дуже тривалого часу. По-друге, точність вгадування всіх біткойн-адрес жертви значною мірою залежить від кількості біткойн-адрес, які використовує жертва. Наприклад, коли клієнт SPV володіє 50 адресами біткойн (буде досягнуто цільове помилкове спрацьовування 0,05%), ймовірність того, що супротивники правильно вгадають усі ці біткойн-адреси, значно зменшується до 6,67 × 10−212%4, якщо врахувати 714,9 мільйонів біткойн. адреси були додані в блокчейн Bitcoin до 01.09.2020. По-третє, попередній рівень техніки не ідентифікував справжні особи (наприклад, імена) користувачів програми біткойн-гаманця, і таким чином реальні збитки обмежені. Наша атака деанонімізації біткойн спрямована на вирішення вищевказаних проблем. Використовуючи вразливість, зловмисники можуть змусити клієнтів SPV гаманців-жертв активно передавати кілька окремих повідомлень про завантаження фільтрів; кожне повідомлення має створений фільтр із частотою помилкових спрацьовувань за замовчуванням 0,001%, що в 50 разів менше. Використовуючи кілька фільтрів, зловмисники можуть знизити частоту помилок ідентифікованих біткойн-адрес до прийнятного рівня (наприклад, три різні фільтри призводять до частоти помилок 10-

13%). Зокрема, в цій атаці кількість помилково розпізнаних біткойн-адрес становить 0,00000072, враховуючи всі використані біткойн-адреси (тобто 714,9 мільйонів).

Завдяки низькому відсотку помилок ідентифіковані біткойн-адреси, таким чином, можуть бути розроблені як новий унікальний відбиток гаманця; вкрай малоймовірно, що два користувачі створять одну і ту саму адресу Bitcoin.

Крім того, користуючись уразливими місцями популярної служби дзвінків Wi-Fi (він же Voice over WiFi, VoWiFi) на смартфонах, зловмисники можуть виявити ідентичність користувача програми біткойн-гаманця. Зверніть увагу, що послуга дзвінків по Wi-Fi, яка до лютого 2019 року широко підтримувалася багатьма операторами стільникових мереж у 52 країнах.

2.1.5. Спам-атака відображення та збільшення кількості біткойнів

Ця атака спрямована на те, щоб використовувати безпечні клієнти повного вузла біткойн, щоб забезпечити безперервний небажаний трафік біткойн (наприклад, 14-20 МБ/год) жертвам, що спричиняє збільшення рахунків за передачу даних стільникової мережі та збільшення споживання енергії на 96%. Використовуючи відповідну вразливість, зловмисники, таким чином, можуть змусити програми біткойн-гаманця постійно завантажувати небажані транзакції біткойн із підключених біткойн FNC. Далі ми спочатку коротко представляємо дизайн цієї атаки, обговорюємо її реалізацію і, нарешті, переважно оцінюємо її негативний вплив.

2.1.6. Мобільні шахрайські атаки на біткойн гаманці

Завдяки централізованій моделі обслуговування постачальник послуг гаманця може легко маніпулювати біткойн-рахунками своїх користувачів без їхнього схвалення. Зокрема, було розроблено додаток для смартфона для біткойн-гаманця, який не є P2P, MyBitcoin, що включає клієнт і сервер. Клієнт - це проста програма

для Android, що забезпечує простий користувальницький інтерфейс для користувачів, щоб надсилати та отримувати BTC. Сервер підтримує функції біткойн-гаманця та мережевої маршрутизації. Клієнт MyBitcoin спочатку з'єднується із сервером через HTTPS, а сервер потім з'єднується з мережами Bitcoin через протокол Bitcoin. Наша оцінка показує, що користувачі MyBitcoin можуть успішно передавати BTC на інші адреси Bitcoin без будь-яких проблем. Це підтверджує, що в мережах біткойн не застосовуються додаткові механізми безпеки для запобігання порушення децентралізації на практиці.

Цю шкідливу програму гаманця можна активно просувати серед користувачів, оскільки на практиці користувачі зазвичай вибирають програму з великою кількістю завантажень або високою оцінкою. Ми проаналізували завантаження популярної програми біткойн-гаманця Mycelium. Ми виявили, що коли кількість завантажень перевищує 1000, темпи зростання завантажень значно збільшуються. Подібні спостереження були також зроблені щодо інших додатків Bitcoin. Іншими словами, якщо супротивники зможуть збільшити кількість завантажень до понад тисячу, очікується, що більше жертв завантажуватимуть програми.

На практиці це не є технічно складним для супротивників для досягнення цієї мети. Багато компаній надають послуги просування, які збільшують кількість завантажень програм і позитивні відгуки про певні програми. Згідно з нашими обговореннями з цими рекламними компаніями, додавання 500 завантажень і 100 позитивних коментарів до певних програм коштує менше ніж 100 доларів США. Після того, як жертви встановлять шкідливі програми, вони постраждають від різних атак шахрайства з біткойн-гаманцями. Однак, на жаль, через обмеження нашого гаманця під назвою IRB ми не змогли розробити справжній шкідливий додаток біткойн-гаманця та оцінити його негативний вплив у реальному світі.

Шахрайська атака не вимагає складних методів атаки; однак негативний вплив цієї атаки є далекосяжним порівняно з іншими типами атак фінансового шахрайства: шахрайськими атаками з мобільного банківського обслуговування та шахрайськими атаками з мобільних платежів проти користувачів смартфонів.

Перша атака спрямована на отримання імен користувачів і паролів жертв, а також крадіжку депозитів жертв шляхом розгортання підроблених мобільних банківських програм. Остання атака має на меті викрадення депозитів жертв з їхніх банківських рахунків або використання кредитних карток жертв без їхнього схвалення шляхом розгортання шкідливих програм для онлайн-платежів, подібних до Paypal, Venmo, CashApp. Ми можемо порівняти розроблену атаку шахрайства з біткойнами з цими двома атаками з чотирьох аспектів: складність розгортання, кредитні транзакції, дебетові транзакції та захист від шахрайства. Маємо чотири спостереження. По-перше, складність розгортання шахрайської атаки мобільного біткойн-гаманця нижча, ніж інші атаки. Для шахрайських атак із мобільним банком підроблені програми мобільного банкінгу повинні пройти перевірку, яку проводять магазини мобільних додатків (наприклад, Google Play і Apple Store). Для атак шахрайства з мобільними платежами, оскільки грошові перекази зазвичай обмежуються користувачами, які використовують ті самі мобільні платіжні програми, новому додатку для мобільних платежів нелегко мати велику кількість клієнтів за короткий час.

По-друге, гроші користувачів мобільного банкінгу додатків для шахрайства з оплатою вносяться на депозит банківські рахунки користувачів, тоді як гроші користувачів мобільних додатків для шахрайства з біткойн-гаманцями зберігаються на біткойн-адресах зловмисників.

По-третє, усі ці атаки можуть переказувати гроші жертв на інші рахунки без схвалення користувачів. Проте атаки мобільного банкінгу та мобільних платежів мають обмеження щодо суми грошей, яку можна переказати, тоді як атака шахрайства з біткойн-гаманцем – ні. Більше того, атака шахрайства з біткойн-гаманцем може перешкодити жертвам отримувати будь-які сповіщення про шахрайські транзакції, проте дві інші атаки не можуть, оскільки сповіщення надходять від фінансових інститутів (наприклад, Chase, Citi) жертв, які не працюють. контролю супротивників.

По-четверте, жертви атак шахрайства з мобільним біткойн-гаманцем навряд чи повернуть гроші (тобто BTC), вкрадені ворогами, оскільки біткойн не є державним застрахованим активом у багатьох країнах, тоді як жертви двох інших атак все ще можуть мати шанси відшкодувати свої збитки шляхом подання спорів до своїх банків. Наприклад, користувачам кредитних карток у США зазвичай не потрібно платити за аномальні транзакції через подання заяв. [15]

Посилаючись на роботи, присвячені аналізу особливостей роботи криптогаманців, було досліджено їхні вразливості з боку користувача. Для визначення вразливостей було використано метод метааналізу досліджень, а також спостереження, пошук.

В загальному, було розглянуто деякі вразливості специфічно за гаманцями, в яких вони зустрічаються частіше. Результати наведено у таблиці нижче. [7]

Таблиця 2

Випадки витоку даних та їх причини за гаманцями

Криптовалютні сервіси	Причина	Наслідок
Tether	Погане зберігання приватних даних	Втрачено приватний ключ гаманця
BitHumb	Використання входу до систему лише за допомогою пароля. Шифрування персональних даних не було.	Втрата персональної інформації користувачів.
BitGo	Вразливість проникнення у мережу та отримати віддалений доступ до серверів. Не шифрування даних.	Ключі для підпису транзакцій було втрачено.
AllCrypt	Слабкий захист на проникнення у мережу.	Незашифровані приватні ключі бази даних було втрачено.
Inputs.io	Використання старих електронних адрес без приєднаного номеру телефону.	Був отриманий доступ до бази даних користувачів.
BitcoinCentral	Використання сумнівного хостингпровайдера, який не використовував 2FA автентифікацію.	Активи та приватні ключі було втрачено.
BitFloor	Використання сумнівного хостингпровайдера.	Зловмисник отримав доступ до незашифрованої резервної копії ключів гаманця.

2.2 Вразливості гаманців

Гаманці мають досить багато вразливостей і усі їх важко охопити в одній роботі. Проте для коректних результатів цієї роботи ми можемо обмежити деякі фактори впливу і зосередитися на вразливостях до необхідної для дослідження моделі порушника. У межах дослідження вразливостей ми припускаємо такі дані про зловмисників, нападів яких зазнає система:

- Зловмисник не володіє особливими знаннями про ціль: тобто зловмисник не знає пароля облікового запису користувача перед здійсненням атаки.
- Зловмисник має можливість заманити користувача до встановлення деяких шкідливих програм, і такі шкідливі програми можуть отримати необхідні дозволи.

2.2.1 Читання та запис зовнішнього сховища

Операційна система Android поділяє сховище на внутрішнє та зовнішнє. За відсутності прав root за замовчуванням доступ до файлів, збережених у внутрішній пам’яті, може мати лише сама програма, тому вона підходить для збереження приватних файлів програми у внутрішній пам’яті. Програми з правом читання зовнішньої пам’яті READ_EXTERNAL_STORAGE або запису в зовнішній сховище WRITE_EXTERNAL_STORAGE можуть читати або записувати будь-які дані у зовнішній пам’яті, не привертаючи уваги користувача. Дозволи зовнішнього сховища широко використовуються різними програмами. Деякі приватні дані, зокрема фотографії, відео, документи, знімки екрана та інші, зазвичай зберігаються у зовнішньому сховищі.

Щоб краще контролювати використання зовнішньої пам’яті, Android 6.0 і новіші версії вимагають, щоб програми зверталися за дозволами під час виконання. Користувачам буде запропоновано під час запуску програми, а не лише під час її встановлення, із запитом, чи дозволено програмі читати та записувати у зовнішній

сховище. Однак програма може постійно просити користувача надати дозвіл, коли користувач відмовляється авторизуватися; інакше користувачеві буде відмовлено у використанні програми. Таким чином, користувач змушений надати дозвіл. Оскільки цей дозвіл запитують більшість програм, користувачі, ймовірно, дозволять програмам читати та записувати на зовнішній сховище. Крім того, якщо програма встановлює для своєї targetSdkVersion значення 22 або нижче, що означає, що цільова версія програми Android 5.1 або нижче, система вважатиме, що програма не відповідає ОС Android 6.0, тому вона все ще використовує управління дозволами старого стилю, у якому під час виконання не з’являється спливаюче вікно запиту на дозвіл.

2.2.2 Резервні копії файлів

Щоб запобігти випадковій втраті даних програми через пошкодження пристрою, неправильну роботу користувача та інші несподівані обставини, що завдають шкоди доступності даних, ОС Android постачається зі службою резервного копіювання програми, яка може створити резервну копію програми та її даних у локальний файл. або хмарний сервер для подальшого відновлення. Файл резервної копії системи може містити дані з приватного каталогу програми. Деякі системи створюють резервні копії даних без шифрування на зовнішнє сховище, що дозволяє програмам з дозволом читати зовнішнє сховище отримувати приватні дані з інших програм. Дані часто містять більш конфіденційну інформацію. Якщо сама програма не шифрує дані, її файл резервної копії порушить конфіденційність конфіденційної інформації.

2.2.3 Спливаюче вікно

Програми з дозволами SYSTEM_ALERT_WINDOW можуть малювати що завгодно на екрані. Доброякісні програми можуть використовувати цю функцію для

виконання законних дій, таких як створення плаваючого вікна, щоб забезпечити певну зручність для користувачів, або змінити яскравість екрана відповідно до вимог користувача. Шкідлива програма може намалювати накладене вікно в інших програмах, щоб змінити інтерфейс користувача, наприклад, запитувати у користувачів паролі, змінювати записи транзакцій або маскувати те, що насправді виконується.

2.2.4 Буфер обміну для читання або запису

Запущені програми Android можуть читати та записувати буфер обміну через компонент ClipboardManager, наданий системою, навіть без надання спеціальних дозволів або повідомлення користувача. Доброякісні програми можуть використовувати цю функцію для швидкого копіювання самостійно визначених даних у буфер обміну або аналізу даних у буфері обміну, щоб спростити операції та покращити роботу користувача. Однак шкідливий додаток може використовувати цю функцію для моніторингу вмісту буфера обміну користувача та вкрасти або замінити конфіденційні дані.

2.2.5 Служба дебагінгу USB

Служба дебагінгу USB призначена для розробників для налагодження та тестування програм. Зазвичай це вимагає підключення пристрою до комп’ютера за допомогою кабелю USB. Оскільки комп’ютер і пристрій Android фізично пов’язані, запустити атаки на з’єднання непросто. Однак Android підтримує бездротове налагодження з комп’ютера в одній локальній мережі. Бездротове налагодження потрібно ввімкнути заздалегідь, або через програму з правами root на пристрої, або за допомогою команди "adb tcpip" під час останнього налагодження дротового USB.

Бездротове налагодження робить можливим налагодження без інформування користувачів. Команда оболонки adb може запускати виконувані файли в

середовищі оболонки Linux пристроїв Android з привілеями оболонки. Можна запустити команду у фоновому режимі, додавши до команди «&». Linux також надає команду nohup, яка підтримує роботу програми після відключення користувача. Завдяки цим функціям атакуваний пристрій може запускати процес із певними привілеями у фоновому режимі, виконувати привілейовані операції, які використовуються під час налагодження USB. Процес також може взаємодіяти з іншими програмами на пристрої, наприклад, через сокети, і виконувати інструкції, надіслані іншими програмами, таким чином підвищуючи інші програми до привілеїв оболонки. [16]

2.2.6. Витік біткоїн-адрес гаманців

Перша вразливість у безпеці полягає в тому, що біткойн-адреси програм гаманця для смартфонів можуть бути передані супротивникам. Зокрема, BitcoinJ, клієнтська бібліотека біткойн, яка широко використовується великою кількістю додатків для смартфонів біткойн-гаманця (наприклад, Bitcoin Wallet, Mycelium) для зв’язку з мережами біткойн, викриває конфіденційність користувачів гаманця біткойн.

Відповідно до стандартів біткойн, після того, як клієнт SPV (тобто програма гаманця біткойн) з’єднається з біткойн FNC (клієнтом повного вузла), до FNC буде надіслано повідомлення про завантаження фільтра. Це повідомлення використовується для визначення зацікавленості користувачів біткойн-гаманця до певних транзакцій. На практиці клієнти SPV зазвичай налаштовані так, щоб бути зацікавленими в транзакціях, в яких беруть участь біткойн-адреси користувачів біткойн-гаманця. Повідомлення містить три ключові параметри, а саме filter, nHashFuncs і nTweak. Сам фільтр є фільтром Блума з бітовим полем, тому FNC може знати адреси свого підключеного додатка гаманця Bitcoin. Фільтр Блума встановлюється на основі подачі елемента даних (наприклад, біткойн-адрес користувачів) набору різних хеш-функцій nHashFuncs MurmurHash3.

Ці хеш-функції nHashFuncs MurmurHash3 ініціалізуються за допомогою nHashNum × 0xFBA4C795 + nTweak, де nHashNum — індекс хеш-функції (наприклад, 1-й, 2-й, 3-й), а nTweak — це випадкове число клієнтів, вибране фільтром SPV. Щоб додати елемент даних (наприклад, адресу Bitcoin) до фільтра, елемент даних повинен бути хешований різними хеш-функціями nHashFuncs і встановити відповідні біти у фільтрі за допомогою операції побітового АБО. Наприклад, елементи даних будуть додані до чистого 6-бітового фільтра (значення 000000) з використанням 2 різних хеш-функцій, і ми припускаємо, що результати першої та другої хеш-функцій будуть 7 (000111) і 9 (001001), відповідно, фільтр встановлюється на 001111 (000111 АБО 001001).

Наше дослідження показує, що для запобігання зловмисникам точного виявлення всіх біткойн-адрес, які коли-небудь використовувалися користувачами біткойн-гаманця, шляхом перехоплення та аналізу повідомлення про завантаження фільтра у вигляді простого тексту, в BitcoinJ реалізовано два механізми безпеки. По-перше, деякі помилкові адреси, які не належать користувачу, будуть відфільтровані фільтром через частоту помилкових спрацьовувань фільтра Блума. По-друге, повідомлення про завантаження фільтрів створюється та передається до біткойн-FNC лише один раз (у разі успішного встановлення TCP-з'єднань з FNC), що означає, що якщо супротивники не можуть контролювати всю діяльність клієнтів SPV з самого початку, вони не можуть перехопити навантаження фільтра. повідомлення. Під час подальшого аналізу ми виявили, що ці два механізми безпеки не є куленепробивними з наступних причин. По-перше, коефіцієнт помилкових спрацьовувань (кількість помилкових адрес над кількістю всіх адрес, доданих до фільтра) фільтра Блума, який використовується в BitcoinJ, становить 0,001%. По-друге, повідомлення про завантаження фільтрів, яке включає обчислений фільтр Блума, передається до FNC після того, як буде встановлено TCP-з'єднання між клієнтом SPV і FNC. Однак наше дослідження показує, що BitcoinJ автоматично виявить і з’єднається з новим FNC, якщо існуюче TCP-з’єднання клієнта SPV з FNC розірвано Таким чином, клієнт SPV може постраждати від атак скидання TCP (тобто

навмисне руйнування TCP-з'єднань жертв зі старими FNC) і повторно передавати повідомлення про завантаження фільтрів до нових FNC. І останнє, але не менш важливе, ми виявили, що після того, як мережевий інтерфейс, який використовується клієнтом SPV, стане недоступним більше ніж на 5 секунд, BitcoinJ використовуватиме абсолютно нове випадкове число (тобто nTweak) для створення повідомлень про завантаження фільтрів. Основна причина полягає в тому, що BitcoinJ підтримує таймер скидання (тобто 5 секунд), щоб відстежувати, чи все ще існує доступний мережевий інтерфейс. Після отримання повідомлень біткойн таймер буде оновлено. Після його закінчення кілька змінних, збережених у пам'яті, будуть очищені та повторно ініціалізовані, включаючи nTweak для створення фільтра. Зауважте, що два повідомлення filterload, згенеровані двома різними nTweaks, можуть допомогти супротивникам значно знизити частоту хибних позитивних результатів визначення адрес користувачів Bitcoin, оскільки nTweak використовується для ініціалізації хеш-функцій nHashFuncs MurmurHash3, що використовуються в повідомленнях filterload. Наприклад, ми припускаємо, що є два повідомлення про завантаження фільтрів, згенеровані двома різними nTweaks, і частота помилкових спрацьовувань встановлена на 0,001%. Імовірність того, що ми неправильно розпізнаємо помилкову адресу як справжню, становить 0,001% × 0,001%, оскільки адреса повинна пройти два різні фільтри, кожен з яких дозволяє пройти лише 0,001% помилкових адрес.

2.2.7. Відсутній захист від спаму при завантаженні транзакцій з біткойнами

Друга вразливість у безпеці полягає в тому, що програми для смартфонів біткойн-гаманця, які використовують BitcoinJ, будуть продовжувати завантажувати транзакції біткойн, які не цікавляться клієнтами SPV, із підключених біткойн FNC у фоновому режимі, не надаючи жодних попереджень або сповіщень для користувачів SPV-клієнтів. Зокрема, як ми описували раніше, клієнт SPV надсилає повідомлення

про завантаження фільтрів, вказуючи його зацікавленість у конкретних біткойн-адресах та транзакціях до біткойн FNC. Щоб FNC або супротивники (посередині) не могли точно визначити конфіденційність користувача/гаманця Bitcoin, клієнт SPV додасть деякі помилкові елементи даних (тобто елементи не цікавлять клієнта SPV), налаштувавши поля фільтра повідомлень про завантаження фільтрів (тобто, встановивши коефіцієнт хибних позитивних результатів на 0,001%). Якщо FNC виявить будь-які транзакції з біткойнами, що відповідають інтересам клієнта SPV, FNC підготує повідомлення про інвентаризацію (тобто inv), що містить ідентифікатори відповідних транзакцій, і надішле повідомлення клієнту SPV. Потім клієнт SPV використовує BitcoinJ для обробки повідомлення inv.

BitcoinJ проведе перевірку всіх транзакцій, які містяться в повідомленні inv, перш ніж завантажувати їх; однак перевірка є хибною, як показано BitcoinJ Code 2. Зокрема, проводяться дві перевірки: (1) чи транзакція не була завантажена раніше та (2) чи транзакція не була самостійно створена. Якщо транзакції немає в будь-якому випадку, BitcoinJ завантажить транзакцію Bitcoin. Це підтверджує, що BitcoinJ не перевіряє, чи може завантажувана транзакція біткойн пройти попередній фільтр, надісланий FNC перед завантаженням транзакції. Якщо в BitcoinJ немає додаткових механізмів безпеки (наприклад, відключення зловмисного FNC), клієнт SPV завантажуватиме транзакції Bitcoin, зазначені в отриманому повідомленні inv, незалежно від того, чи не цікавлять ці транзакції. Таким чином, користувачі клієнта SPV страждають від різних атак і не знають про це.

2.2.8. Децентралізація служби криптовалютних гаманців може бути порушена

Користувачів гаманця біткойн (наприклад, не потрібна реєстрація користувача на стороні сервера і немає контрольних точок, які контролюють усі дії власників біткойн), але також запобігає компрометації послуг біткойн-гаманця кількома вузлами в мережах біткойн. Зловмисникам потрібно контролювати більшість

майнерів біткойн і повні вузли; інакше супротивники не зможуть втрутитися в платіжні транзакції біткойн. Щоб зберегти біткойн децентралізованим, офіційний сайт біткойн https://bitcoin.org/ також випускає еталонну реалізацію вузлів біткойн, Bitcoin Core, що підтримує всі функції біткойн (наприклад, гаманець, мережева маршрутизація, майнер). Однак Bitcoin.org розробив і випустив Bitcoin Core лише для користувачів ПК (Windows, Mac OS і Linux), а не для користувачів смартфонів, а це означає, що всі програми для смартфонів Bitcoin гаманців на ринку розробляються іншими сторонами. Ще гірше те, що, наскільки нам відомо, біткойн не передбачає жодних механізмів цензури, які перевіряють та забезпечують відповідність додатків для смартфонів гаманця Bitcoin. Таким чином, виникає два питання: чи будуть ці програми для смартфонів-гаманців біткойн продовжувати децентралізувати біткойн? Якщо ні, чи знають користувачі про порушення? Дослідження безпеки та дослідження користувачів було проведено відповідно до 10 популярних додатків для смартфонів біткойн-гаманця та їхніх користувачів. На жаль, наші результати показують, що відповіді на обидва вищезазначені запитання є негативними. Маємо три висновки.

По-перше, бажана децентралізація Bitcoin не пропонується в деяких програмах гаманця. Ці програми гаманця не дають користувачам прямого доступу до мереж Bitcoin; всі транзакції біткойн повинні передаватися на проміжні сервери, розгорнуті розробниками додатків, через захищені канали (наприклад, TLS). Після цього ми називаємо ці програми, що порушують децентралізацію біткойн, не P2P гаманцями.

По-друге, ми виявили, що користувачі деяких програм гаманців, які не належать до P2P, не можуть повністю контролювати свої приватні очі гаманця Bitcoin. Таким чином, BTC, внесені користувачами на їхні адреси Bitcoin, можуть передаватися іншими сторонами на інші адреси Bitcoin без попередньої згоди користувача. І останнє, але не менш важливо, більшість користувачів програми гаманця не знають про порушення децентралізації біткойн. Таким чином, ці

користувачі можуть постраждати від різних атак шахрайства з біткойн-гаманцями. [15]

Підсумовуючи атаки, у додатку А представлено вразливості додатків для смартфонів біткойн-гаманців, класифіковані за мережами, в яких вони можливі.

Висновки за розділом 2

Було проведено аналіз наявних атак на криптогаманці, зокрема електронні. Було проаналізовано та досліджено детально деякі з них, які стосуються боку користувачів. Визначено основні вразливості криптогаманців.

Було систематизовано деякі вразливості за типом гаманців та за мережами. Деякі з них було досліджено докладно, було розглянуто конкретні атаки, можливі до виконання. Частина даних щодо атак та вразливостей було структуровано і надано у вигляді таблиць, а саме випадки витоку даних та їх причини (досліджено за конкретними випадками гаманців) та вразливості додатків для смартфонів біткойн-гаманців (досліджено за мережами, в яких вони можливі). Обидві проаналізовано та представлено в бакалаврській роботі. Дані було структуровано і подано в зручному для сприйняття вигляді. Досліджено деякі випадки атак прицільно. Було описано ті з них, які рідко висвітлюються. Вони представлені детальним описом та знімками екрану, що демонструють проведення атаки.

В розділі було розглянуто атаки та вразливості гаманців, що слугуватиме основою для написання наступного розділу. Ця частина роботи критична через необхідність інформації про вразливості, щоб будувати рекомендації щодо їх усунення чи захисту.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ КРИПТОГАМАНЦІВ

3.1 Базові положення безпечного використання криптогаманців

Щоб забезпечити безпеку свого крипто-гаманця, необхідно правильно використовувати свій гаманець і правильно зберігати свої дані. Перш за все, потрібно звернути увагу на свій закритий ключ. Його необхідно зберігати в автономному режимі, без доступу до Інтернету. На жаль, хоча їх дуже легко підключити до Інтернету, поки ваш гаманець залишається на зв'язку, він може бути під атакою фішингових шахрайств, вірусів, шкідливого програмного забезпечення. Гаманці, такі як паперові та апаратні, зберігають закриті ключі у автономному режимі. Не можна надавати свій приватний ключ третім особам. Будь-хто, хто має доступ до приватного ключа, має доступ до коштів, які під ним зберігаються. Необхідно тримати такий ключ в секреті, щоб ніхто не зловживав інформацією. Також не варто недооцінювати важливість надійних паролів, коли мова йде про безпеку. Необхідно змінювати, запам'ятовувати, не використовувати той самий пароль для декількох акаунтів чи гаманців. Необхідно виключити можливість втрати паролю, інакше кошти на рахунку будуть втрачені назавжди. На відміну від багатьох банків, біткойн надає дуже мало можливостей для скидання паролів. Насправді, необхідно пам'ятати свій пароль навіть після багатьох років без використання. Це необхідно, адже багато паролів було втрачено, і їхні власники більше не мають доступу до валют. Можливо зберігати копію паперу з паролем у надійному місці, якщо це безпечно.

Будь-який пароль, який містить лише літери та/або словникові слова, які мають сенс, можна вважати дуже слабким і легко зламати. Надійні паролі повинні містити літери, цифри, розділові знаки та мати довжину не менше 16 символів. Найбільш безпечними паролями є паролі, створені програмами, розробленими для

цієї мети. Надійні паролі зазвичай важко запам’ятати. Можливо і ефективно налаштувати двофакторну аутентифікацію (2FA) або багатофакторну аутентифікацію (MFA), щоб забезпечити більш надійний доступ до криптовалютного гаманця. Використання безпечних мереж Інтернету є одним із факторів безпечного використання гаманців. Здійснюючи транзакції криптовалют, необхідно використовувати лише безпечне інтернет-з’єднання та не використовувати публічні мережі Wi-Fi.

Навіть під час доступу до домашньої мережі використовуйте VPN для додаткової безпеки. VPN змінює вашу IP-адресу та місцезнаходження, захищаючи вашу онлайн-безпеку безпечно та конфіденційно від загроз для гравців. Оскільки немає обмежень на створення гаманців, ви можете на кілька біт диверсифікувати свої інвестиції в криптовалюти.

Використовуйте один гаманець для повсякденних операцій, а решту зберігайте в окремому гаманці. Це захистить та мінімізує втрати при будь-якому зломі криптовалюти. Багато гаманців особливо важливі, коли у вас є велика кількість криптовалюти. [10]

У цьому розділі будуть наведені конкретні заходи та правила, які необхідні для збільшення безпеки користувачів під час використання електронних криптогаманців.

3.2. Принципи забезпечення безпеки

На основі усього вищенаведеного, виділимо три основні принципи, яким вони мають відповідати:

— захист особистих даних;

— безпечна поведінка;

— програмне забезпечення з надійних джерел.

3.3. Рекомендації та обґрунтування

Отже, конкретизуємо та визначимо точні кроки для того, щоб використовувати гаманці безпечно:

— приватні ключі мають бути в автономному режимі;

Цей захід попереджає від втрати даних як випадково, так і в результаті атаки на мережу, в якій користувач знаходиться. Як було показано раніше, мережі WiFi можуть стати небезпечними для використання гаманців, якщо вони піддаються атаці «людина посередині». Також публічні мережі вразливі до децентралізації. Хоча ця атака і дуже складна в реалізації, це може бути небезпекою.

— гаманці мають бути відключені від мережі за відсутності необхідності;

Якщо гаманці передають інформацію більше часу, ніж це необхідно, є ризик, знову, дістати дані через «подвійну» підставну мережу і запити з неї.

Також є небезпека сніффінгу пакетів.

— регулярно оновлювати додатки лише з довірених джерел;

Багато гаманців, випущених для Android, відмовляють в обслуговуванні за умови, якщо користувач має нестандартну користувацьку прошивку телефона. Це розумно, бо, як ми змогли побачити, зміни не тільки у самому додатку, а ще й у клавіатурі чи буфері обміну можуть спричинити до викрадення даних, що вводяться, копіюються і вставляються. Також ці дані можуть бути модифіковані під час роботи додатків. Довірені джерела мають служити гарантом штатного роботи навіть таких простих функцій.

Не варто, проте, забувати про нагальну необхідність оновлювати сам гаманець із довіреного джерела. На додатки часто випускають патчі, без яких вони ставали б набагато менш безпечними з часом. Критично важливо їх мати, бо самі додатки також можливо атакувати.

— зберігати приватні ключі таємно від інших людей;

Незважаючи на високу розвиненість технологій, соціальна інженерія усе ще є однією із найбільш небезпечних галузей. До цієї рекомендації відноситься не

надавати дані для входу третім особам та не ставати жертвами шахраїв, які намагаються отримати дані особисто.

— використовувати складні паролі;

Паролі, які використовуються, мають бути складними, адже короткі паролі легко зламати грубою силою. Необхідно пам’ятати, що кожен символ доданий до пароля, підвищує час на його перебір у близько 89 разів (26 символів * 2 регістри + 10 цифр + 27 спецсимволів як варіанти). Слова, які є у словниках, за допомогою сучасних модифікацій алгоритму знаходяться набагато швидше. Проте це дійсно важливо запам’ятати.

— пам’ятати пароль;

За різними оцінками, 3.7-4.2 мільйона BitCoin було втрачено назавжди лише через те. що користувачі забули свої токени. Наразі існують гаманці, які дозволяють відновити пароль, проте інші – ні. Необхідно завжди пам’ятати дані, необхідні для отримання доступу до гаманця.

— налаштувати двохфакторну автентифікацію;

Збільшення кількості питань та складності паролів в рази підвищує рівень забезпечення конфіденційності інформації. Необхідно, щоб для будь-яких операцій до гаманця мав доступ лише його господар.

— використовувати лише безпечні підключення до Інтернету;

Відкриті мережі мають ризик створення «подвійної» мережі, а також надсилання через неї пакетів-запитів до гаманця. Це може статися навіть із надійними мережами, адже завжди може підключитися злочинець. Є ризик сніфінгу пакетів, адже вони усі проходять через мережу.

— використання декількох гаманців;

Використання декількох гаманців для розділення суми, що зберігається, на частини, є гарною ідеєю для випадків, коли ризик втратити малу частину надходжень із більшою імовірністю є кращим, ніж втратити все із меншою імовірністю. Незважаючи на це, необхідно пам’ятати про безпечні джерела, із яких беруться самі гаманці. Завжди необхідно упевнятися у тому, що джерело безпечне.

— не використовувати буфер для зберігання паролів, а вводити його самостійно;

Атаки на буфер, як було представлено вище, досить небезпечні і порушують конфіденційність даних, що були скопійовані в буфер обміну. Із буфера ці дані можуть бути підхоплені іншою злочинною програмою і передані злочинцям. Хоча це і складна для проведення атака, рекомендується вводити пароль самотужки.

— завжди використовувати програми та прошивки;

Неліцензійна клавіатура на телефоні може записувати точку, до якої доторкається людина при введенні пароля. Менеджери паролів безпосередньо мають багато конфіденційної інформації. Гаманці завжди мають бути ліцензійними через ризик атак. Інші не довірені додатки можуть скоювати атаки та підміняти частину інформації у виключних випадках. Це досить небезпечні атаки, які часто стають успішними.

— не надавати стороннім додаткам права, що не є критичними;

Надання прав додаткам може зумовити використання цих прав не за призначенням. Задля слушного функціонування гаманців та їхньої взаємодії з іншими частинами телефону необхідно упевнитися, що нічого не намагається викрасти інформацію чи змінити її.

— використовувати надійні гаманці;

Усі гаманці мають бути не тільки ліцензованими і постійно оновлюватися. Вони мають серйозно ставитися до своєї безпеки. На різні гаманці можуть надходити сотні атак одночасно. Команда безпеки, що працює із цим, має бути професійною та швидко реагувати на інциденти.

— захищати джерела резервного копіювання.

Оскільки під час аварійного виключення додатку створюється резервна копія, вона може бути використана іншими девайсами чи програмами для вилучення особистих даних.

Отже, було надано кроки, які вважаються в роботі базовими для забезпечення безпеки під час використання онлайн-гаманців.

За загальною моделлю функціонування онлайн-гаманців, яка є досить розповсюдженою та надійною, в роботі розроблено та запропоновано схему рекомендацій для попередження зловживання вразливостями на усіх етапах використання гаманця користувачем. Це проілюстровано на рисунку 8.

Рисунок 8 – Схема рекомендацій щодо використання гаманців залежно від функцій, що піддаються вразливостям

Висновки за розділом 3

У цьому розділі було розроблено та представлено самі рекомендації щодо використання електронних гаманців. Було узагальнено три основні принципи, що рекомендуються цією роботою до дотримання задля більш безпечного використання гаманців. Пояснено причини вибору саме цих рекомендацій.

ВИСНОВКИ

У першому розділі цієї роботи було досліджено та проаналізовано законодавчу врегульованість та визначення криптогаманців в Україні. У тому ж розділі було проаналізовано класифікацію гаманців за принципом роботи, було візуалізовано схему класифікації різних криптогаманців. Було визначено функції криптогаманців.

У другому розділі бакалаврської роботи було досліджено та проаналізовано випадки зламу гаманців, їхні особливості; випадки зламу та зловживань електронними гаманцями залежно від їхньої будови; найрозповсюдженіші способи зламу. Також було визначено та класифіковано вразливості у гаманцях із точки зору користувача, у тому числі тих, які характерні для певних гаманців.

У третьому розділі роботи було безпосередньо розроблено рекомендації щодо безпечного використання гаманців користувачами. Було узагальнено три основні принципи, що рекомендуються цією роботою до дотримання задля більш безпечного використання гаманців. Пояснено причини вибору саме цих рекомендацій.

Отже, було досліджено загрози та атаки на криптогаманці. Було розроблено рекомендації щодо використання електронних криптогаманців користувачами. Було також досліджено базу, необхідну для розробки таких рекомендацій. Було досліджено загрози та їхні причини, а також атаки на криптогаманці. Було розроблено рекомендації щодо дотримання безпеки криптогаманців з боку користувачів. Було візуалізовано схему рекомендацій та пов’язано її із функціями криптогаманців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Верховна Рада України. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового ураження [Електронний ресурс] / Верховна Рада України. – 2022. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/361-20#Text. (дата звернення 17.05.2022).

2. Верховна Рада України. Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами [Електронний ресурс] / Верховна Рада України. – 2019. – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423. (дата звернення 17.05.2022).

3. Кісіль А. Правовий статус криптовалют в Україні [Електронний ресурс] / А. Кісіль, В. Пряміцин. – 2021. – Режим доступу до ресурсу: https://doi.org/10.32837/pyuv.v0i1.722 (Дата звернення 17.05.2022)

4. Агентство США з міжнародного розвитку. / Агентство США з міжнародного розвитку // Криптовалюти в Україні: технологія, ринок, регулювання / Агентство США з міжнародного розвитку., 2018. – С. 8–50.

5. The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon [Електронний ресурс] // Chainalysis. – 2020. – Режим доступу до ресурсу: https://blog.chainalysis.com/reports/2020-global-cryptocurrency-adoption-index-2020/.

6. Ісмайлов К. Ю. Використання знань про особливості криптовалют у протидії злочинності / К. Ю. Ісмайлов, Т. А. Бедрій, С. В. Медведенко. // Одеський державний університет внутрішніх справ «Кібербезпека в Україні: правові та організаційні питання». – 2018. – С. 140–149.

7. Бистрова Б. В. Безпечний криптовалютний гаманець / Б. В. Бистрова, Н. С. Вишневська, К. О. Тараненко. // Збірник тез наукових доповідей «Стан та

удосконалення безпеки інформаційно-телекомунікаційних систем». – 2021. – С. 66–68.

8. Дорош Ю. О. Дослідження автоматизованої системи для накопичення криптовалюти : кваліфікаційна робота магістра за спеціальністю «151 — автоматизація та комп’ютерно-інтегровані технології» / Ю. О. Дорош. — Тернопіль: ТНТУ, 2021.

9. Suratkar S. Cryptocurrency Wallet: A Review / S. Suratkar, M. Shirole, S. Bhirud. // 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP). – 2020. – №4. –P. 1–7.

10. Місюра А. В. Криптовалютні гаманці та їх характеристики: курсова робота за спеціальністю «Комп’ютерні науки» 122 / А. В. Місюра – Київ: НАУКМА, 2021.

11. Albayati H. A study on the use of cryptocurrency wallets from a userexperience perspective / H. Albayati, S. K. Kim, J. J. Rho. // Human Behavior and Emerging Technologies. – 2021. – №3. – P. 720–738.

12. Bitcoin Abuse Database [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.bitcoinabuse.com/.

13. Phishing attacks on modern android / A.Aonzo, G. Merlo, G. Tavella, Y. Fratantonio. // Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS ’18). – 2018. – №25. – P. 15–19.

14. Android-based Cryptocurrency Wallets: Attacks and Countermeasures / [C. Li, D. He, S. Li та ін.]. // 2020 IEEE International Conference on Blockchain (Blockchain). – 2020. – P. 9–16.

15. Security Threats from Bitcoin Wallet Smartphone Applications: Vulnerabilities, Attacks, and Countermeasures / [Y. Hu, S. Wang, G. Tu та ін.]. // CODASPY '21, April 26–28, 2021, Virtual Event, USA. – 2021. – P. 89–100.

16. A Structured Overview of Attacks on Blockchain Systems / T.Guggenberger, V. Schlatt, J. Schmid, N. Urbach. // Twenty-fifth Pacific Asia Conference on Information Systems. – 2021. – №25. – P. 1–14.

17. Bulut Y., Sertkaya I. Security Problem Definition and Security Objectives of Cryptocurrency Wallets in Common Criteria / Y. Bulut, I. Sertkaya. // Bilişim Teknolojileri Dergisi – 2020. – №13. – P. 157-165

18. Zindros D. Hours of Horus: Keyless Cryptocurrency Wallets [Електронний ресурс] / Dionysis Zindros. – 2021. – Режим доступу до ресурсу: https://eprint.iacr.org/2021/715.pdf.

19. Diedrich H. Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations / Henning Diedrich., 2016. – 360 с.

20. Evers S. Trügerische Sicherheit: Aus diesen Gründen bleibt Ransomware weiterhin eine Gefahr / Evers. // Digitale Welt. – 2022. – №1. – P. 34–37.

21. Herschel M. Bitcoin Sicherheit [Електронний ресурс] / Herschel. – 2021. – Режим доступу до ресурсу: https://herschel.io/assets/pub/Bitcoin_Sicherheit.pdf.

22. Приходько Е. Е. Аналіз вразливостей та засобів захисту криптовалют / Е. Е. Приходько, Є. О. Севастєєв. // 75-а науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів. – 2020. – С. 140–143.

23. Мельник Д. С. Забезпечення нормативно-правового регулювання обігу криптовалют в Україні як основа протидії їх протиправному використанню / Д. С. Мельник, О. С. Петрова. // International scientific conference, Łódź, the Republic of Poland. – 2021. – С. 131–135.

24. Pravdiuk M. International experience of cryptocurrency regulation / Pravdiuk. // Norwegian Journal of Development of the International Science. – 2021. – №53. – P. 31–37.

25. Jorgensen K. Universal Wallets / K. Jorgensen, R. Beck. // Bus Inf Syst Eng. – 2022. – №64. – С. 115–125.

26. N’Gumah J. Evaluating Security in Cr aluating Security in Cryptocurrency Wallets / Judith Mozoun N’Gumah. – St. Cloud, 2021. – 96 p.

27. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions / B.Bhushan, P. Sinha, K. Sagayam, A. J. // Computers & Electrical Engineering. – 2021. – №90.

28. Multiple-Layer Security Threats on the Ethereum Blockchain and Their Countermeasures / L.Duan, Y. Sun, K. Zhang, Y. Ding. // Hindawi. – 2021.

29. Blockchain Technology: Concept, Applications, Challenges, and Security Threats / C.Gandhi, N. Shukla, G. Kaur, K. Yadav. // Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing. – 2021. – P. 77–104.

30. Soonduck Y. Research on Security Threats Emerging from Blockchain-based Services / Yoo Soonduck. // International Journal of Internet, Broadcasting and Communication. – 2021. – №13. – P. 1–10.

31. Блотницька Д. В. Вразливості у використанні криптогаманців в криптовалютній індустрії / Д. В. Блотницька, А. О. Фесенко. // Міжнародна науково-практична конференція «Інтеграція інформаційних систем і інтелектуальних технологій в умовах трансформації інформаційного суспільства»,. – 2021.

ДОДАТОК А
ВРАЗЛИВОСТІ ДОДАТКІВ ДЛЯ СМАРТФОНІВ БІТКОЙН-ГАМАНЦІВ ЗА МЕРЕЖАМИ, В ЯКИХ ВОНИ МОЖЛИВІ

Категорія	Атака	Тип мережі жертви	Опис загрози	Основні вразливості
Витік особистих даних	Атака деанонімізації	Wi-Fi	Зловмисник використовує вразливі місця бібліотек, які використовуються програмами гаманця, щоб створити унікальний відбиток гаманця, і пов’язує його з ідентичністю користувача для подальшого відстеження користувачів.	Витік біткойн-адрес гаманців.
Спам	Віддзеркалення та посилення біткойн спам-атаки	Мобільна мережа	Зловмисник використовує вразливі місця реалізації програм і елементи загальнодоступної мережі біткойн для створення безперервного трафіку біткойн-спаму, що йде до жертв; ця атака спричиняє збільшення рахунку за послуги мобільного передавання даних жертви та скорочення терміну служби акумулятора	Відсутність захисту від спаму при транзакціях з біткойнами.

			смартфона жертви.	
Фінансові втрати	Шахрайство із мобільними біткойн-гаманцями	Wi-Fi або мобільна мережа	Зловмисник використовує неправильне розуміння користувачів інтерфейсу гаманця для розробки та просування їхніх програм серед жертв; Таким чином, жертви зазнають матеріальних збитків.	Порушена децентралізація служби гаманців біткоїну.

ДОДАТОК Б

СХЕМА РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ ГАМАНЦІВ ЗАЛЕЖНО ВІД ФУНКЦІЙ, ЩО ПІДДАЮТЬСЯ ВРАЗЛИВОСТЯМ

ДОДАТОК В
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИПЛОМУ

Тези наукових доповідей

1. Блотницька Д. В. Вразливості у використанні криптогаманців в криптовалютній індустрії / Д. В. Блотницька, А. О. Фесенко. // Міжнародна науково-практична конференція «Інтеграція інформаційних систем і інтелектуальних технологій в умовах трансформації інформаційного суспільства»,. – 2021.