АНОТАЦІЯ

Скоморохов Владислав Андрійович «Еволюція загроз інформаційної безпеки у мобільних технологіях» – Рукопис.

Магістерська робота за спеціальністю 251 «Державна безпека» – Київський інститут Національної гвардії України, Київ, 2025.

Магістерська кваліфікаційна робота присвячена дослідженню еволюції загроз інформаційній безпеці у мобільних технологіях та особливостям їх урахування в діяльності структур сектору безпеки й оборони України, зокрема підрозділів Національної гвардії України. Актуальність теми зумовлена стрімким поширенням смартфонів, сервісів мобільного Інтернету, 4G/5G-мереж, Інтернету речей та мобільних фінансових сервісів, що перетворює мобільне середовище на один із ключових векторів сучасних кіберзагроз. Для НГУ це має критичне значення, оскільки компрометація мобільних пристроїв військовослужбовців і засобів зв'язку може призвести до витоку службової інформації, зриву операцій, загрози життю особового складу та ослаблення спроможностей підрозділів у зоні бойових дій.

Мета дослідження полягає в комплексному аналізі еволюції загроз інформаційній безпеці мобільних технологій від початкового етапу розвитку мобільного зв'язку до сучасних 5G/IoT-середовищ та обґрунтуванні підходів до підвищення рівня захищеності мобільних пристроїв і сервісів у діяльності структур сектору безпеки України й Національної гвардії України. Об'єктом дослідження є процес еволюції загроз інформаційній безпеці у мобільних технологіях. Предметом дослідження виступає сукупність теоретичних і практичних підходів до класифікації, моделювання й нейтралізації загроз у мобільному середовищі та механізмів протидії цим загрозам у діяльності підрозділів сектору безпеки й оборони.

У роботі застосовано комплекс загальнонаукових і спеціальних методів: аналіз і синтез, системний та структурно-функціональний підходи, порівняльний аналіз, елементи історико-логічного методу, методи

моделювання загроз і ризик-орієнтованого підходу до оцінювання вразливостей. На основі цих методів здійснено поетапний аналіз еволюції мобільних загроз (від перших мобільних вірусів до складних мультивекторних атак у середовищі 5G, edge-обчислень та мобільних фінансових сервісів), узагальнено особливості функціонування сучасних екосистем Android та iOS, досліджено специфіку атак на мобільні фінансові сервіси, корпоративні середовища та моделі BYOD/BYAD у контексті потреб НГУ.

Наукова новизна одержаних результатів полягає у подальшому розвитку класифікації загроз інформаційній безпеці мобільних технологій з урахуванням якісних змін останніх десятиліть; уточненні уявлень про взаємозв'язок еволюції технологій, моделей атак та вразливостей мобільного середовища; розробленні концептуальної моделі загроз для мобільних пристроїв у підрозділах сектору безпеки, що інтегрує технічні, організаційні та людські фактори; удосконаленні підходів до організації захисту мобільних пристроїв у корпоративному та відомчому середовищі на основі принципів Zero Trust і керованого використання особистих пристроїв.

Практичне значення роботи полягає в можливості використання запропонованих підходів і рекомендацій при розробленні внутрішніх нормативних документів НГУ щодо використання мобільних пристроїв, організації захисту службових комунікацій, регламентації BYOD-моделей та побудови політик доступу до інформаційних ресурсів. Окремі положення можуть бути використані у навчальному процесі при викладанні дисциплін з інформаційної безпеки, кібербезпеки та управління ризиками, а також у практичній діяльності підрозділів, відповідальних за кіберзахист і захист інформації в структурах сектору безпеки й оборони України.

Ключові слова: мобільні технології, інформаційна безпека, еволюція загроз, 5G та Інтернет речей, мобільні фінансові сервіси, Zero Trust, Національна гвардія України.

ABSTRACT

Skomorokhov Vladislav Andriyovych “The Evolution of Information Security Threats in Mobile Technologies” – Manuscript.

Master's thesis in the field of 251 ‘National Security’ – Kyiv Institute of the National Guard of Ukraine, Kyiv, 2025.

This master's thesis is devoted to researching the evolution of information security threats in mobile technologies and the specifics of their consideration in the activities of Ukraine's security and defence sector structures, in particular the units of the National Guard of Ukraine. The relevance of the topic is due to the rapid spread of smartphones, mobile Internet services, 4G/5G networks, the Internet of Things and mobile financial services, which is turning the mobile environment into one of the key vectors of modern cyber threats. This is critical for the NGU, as the compromise of military personnel's mobile devices and communications equipment can lead to the leakage of official information, disruption of operations, threats to the lives of personnel, and the weakening of the capabilities of units in the combat zone.

The aim of the study is to comprehensively analyse the evolution of threats to the information security of mobile technologies from the initial stage of mobile communications development to modern 5G/IoT environments and to justify approaches to improving the security of mobile devices and services in the activities of Ukraine's security sector and the National Guard of Ukraine. The object of the study is the process of evolution of threats to information security in mobile technologies. The subject of the study is a set of theoretical and practical approaches to the classification, modelling and neutralisation of threats in the mobile environment and mechanisms to counter these threats in the activities of security and defence sector units.

The work uses a set of general scientific and special methods: analysis and synthesis, systemic and structural-functional approaches, comparative analysis,

elements of the historical-logical method, methods of threat modelling and a risk-oriented approach to vulnerability assessment. Based on these methods, a step-by-step analysis of the evolution of mobile threats (from the first mobile viruses to complex multi-vector attacks in the 5G environment, edge computing and mobile financial services) was carried out, the features of modern Android and iOS ecosystems were summarised, and the specifics of attacks on mobile financial services, corporate environments and BYOD/BYAD models were investigated in the context of the needs of the National Guard of Ukraine.

The scientific novelty of the results obtained lies in the further development of the classification of threats to the information security of mobile technologies, taking into account the qualitative changes of recent decades; clarification of ideas about the interconnection between the evolution of technologies, attack models and vulnerabilities of the mobile environment; the development of a conceptual model of threats to mobile devices in security sector units, integrating technical, organisational and human factors; the improvement of approaches to the organisation of mobile device protection in corporate and departmental environments based on the principles of Zero Trust and controlled use of personal devices.

The practical significance of the work lies in the possibility of using the proposed approaches and recommendations in the development of internal regulatory documents of the NSU regarding the use of mobile devices, the organisation of protection of official communications, the regulation of BYOD models and the development of policies for access to information resources. Individual provisions can be used in the educational process when teaching disciplines related to information security, cybersecurity, and risk management, as well as in the practical activities of departments responsible for cyber protection and information protection in the structures of Ukraine's security and defence sector.

Keywords: mobile technologies, information security, threat evolution, 5G and the Internet of Things, mobile financial services, Zero Trust, National Guard of Ukraine.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Стрімкий розвиток мобільних технологій, поширення смартфонів, планшетів та інших інтелектуальних пристроїв перетворили мобільну інфраструктуру на один із ключових елементів сучасного інформаційного простору. Для більшості громадян мобільний телефон став основним засобом доступу до мережі Інтернет, електронних сервісів, банківських операцій, службового та приватного листування. Одночасно із зростанням залежності суспільства від мобільних сервісів суттєво ускладнюється й спектр загроз інформаційній безпеці, які еволюціонують від відносно простих шкідливих програм початку двохтисячних років до багаторівневих цілеспрямованих атак, що використовують можливості п’ятого покоління зв’язку, Інтернету речей та хмарних сервісів.

Сучасний етап розвитку мобільних технологій характеризується стрімким зростанням обсягів переданої інформації, широким використанням смартфонів, хмарних сервісів та мобільних додатків у всіх сферах суспільного життя. Для сил оборони України, зокрема для Національної гвардії України (НГУ), це створює не лише нові можливості для оперативної взаємодії, управління підрозділами та інформування особового складу, але й принципово нові загрози інформаційній безпеці. Будь-яка вразливість мобільного пристрою військовослужбовця чи посадової особи НГУ може бути використана противником для збору розвідувальної інформації, відстеження переміщень, перехоплення службових комунікацій та проведення психологічних операцій.

Умови воєнного стану загострюють ці ризики, оскільки компрометація смартфона або іншого мобільного пристрою здатна призвести не лише до витоку службової інформації, а й до прямої загрози життю та здоров’ю особового складу, зриву спеціальних операцій, розкриття місць дислокації

підрозділів і критичної інфраструктури. Саме тому дослідження еволюції мобільних загроз, особливостей їх прояву в діяльності Національної гвардії України та розроблення практичних рекомендацій щодо мінімізації відповідних ризиків є надзвичайно актуальним завданням. Отримані результати можуть бути використані для удосконалення політик безпечного використання мобільних пристроїв у НГУ, оновлення внутрішніх нормативних документів та системної підготовки особового складу у сфері інформаційної безпеки.

Особливої актуальності проблема еволюції загроз інформаційної безпеки у мобільних технологіях набуває в умовах триваючої збройної агресії проти України та загального зростання ролі кіберпростору у гібридних конфліктах. Мобільні пристрої військовослужбовців, співробітників сектору безпеки, органів державної влади та громадян використовуються як канали збору розвідданих, дистанційного спостереження, впливу на громадську думку, а також як інфраструктура для реалізації кібероперацій. Компрометація мобільних пристроїв може призвести не лише до витоку конфіденційної інформації, а й до загрози життю та безпеці особового складу, зриву службово бойових завдань, порушення роботи критично важливих об’єктів.

Науковий та практичний інтерес становить те, що загрози інформаційній безпеці у мобільних технологіях не є статичними. Вони змінюються разом із розвитком апаратного забезпечення, мобільних операційних систем, комунікаційних стандартів, бізнес моделей розробників програмного забезпечення та сервіс-провайдерів. Перехід від кнопкових телефонів до смартфонів на базі Symbian та Windows Mobile, подальше домінування екосистем Android та iOS, розгортання мереж четвертого і п’ятого поколінь, поява масових мобільних платіжних сервісів і банківських застосунків – усі ці етапи супроводжувалися появою нових класів атак, змінювали пріоритети зловмисників та вимоги до систем захисту.

Проблематика інформаційної безпеки мобільних технологій розглядається у працях вітчизняних та зарубіжних дослідників, що присвячені питанням кібербезпеки, побудові моделей загроз, аналізу вразливостей мобільних операційних систем, захисту мереж зв'язку наступних поколінь, безпеці мобільних фінансових сервісів та мобільних пристроїв у корпоративному середовищі. Значний внесок у дослідження цієї проблематики зробили такі вчені, як Антонюк А. О., Арістова І. В., Гнатюк В., Гулак Г. М., Журавльова І. В., Кормич Б. А., Одарченко Р., Пономаренко В. С., Раєцький А., Сулацький Д. В., Тарасюк А. В., Урба С. І., Grover L. K., Bernstein D. J., Lange T., Shor P. W., Katz J., Lindell Y. Та ін. У наукових роботах акцент робиться на аналізі окремих аспектів проблеми: криптографічного захисту даних, безпечної аутентифікації, виявлення шкідливого програмного забезпечення, побудові архітектур безпеки для мобільних додатків. Разом з тим, комплексні дослідження саме еволюційної динаміки загроз, їхньої класифікації за історичними етапами розвитку мобільних технологій, а також узгодження таких підходів із потребами сектору безпеки України залишаються недостатньо розробленими. Це зумовлює необхідність системного аналізу змін у спектрі загроз, механізмах їх реалізації та засобах протидії з урахуванням сучасних викликів державній та інформаційній безпеці.

Об'єктом дослідження є процес еволюції загроз інформаційної безпеки у сфері мобільних технологій в умовах цифровізації суспільства та зростання ролі кіберпростору у забезпеченні національної безпеки.

Предметом дослідження є сукупність теоретичних і практичних підходів до класифікації, аналізу та нейтралізації загроз інформаційній безпеці мобільних технологій на різних етапах їхнього розвитку, а також організаційні та технічні механізми протидії цим загрозам у діяльності структур сектору безпеки.

Мета дослідження полягає в тому, щоб на основі комплексного аналізу еволюції загроз інформаційної безпеки у мобільних технологіях обґрунтувати

концептуальні підходи до їх класифікації та оцінювання, встановити закономірності розвитку цих загроз у часовій динаміці та розробити практичні рекомендації щодо удосконалення системи захисту мобільних пристроїв і сервісів у контексті завдань кібербезпеки та державної безпеки України.

Для досягнення поставленої мети у роботі передбачається розв’язати такі основні **завдання:**

1. Визначити сутність мобільних технологій як об’єкта інформаційної безпеки, узагальнити їх роль у сучасній інформаційній інфраструктурі та окреслити фактори, що зумовлюють уразливість мобільного середовища.

2. Встановити характерні особливості та основні класи загроз інформаційній безпеці мобільних технологій на початковому етапі їх розвитку у двохтисячних роках, проаналізувати вектори атак і канали поширення шкідливого програмного забезпечення для перших мобільних операційних систем.

3. З’ясувати, які якісні зміни відбулися у спектрі загроз із переходом до смартфонів на базі Android та iOS, визначити вплив магазинів застосунків, моделей монетизації та масового використання мобільного Інтернету на формування нових ризиків.

4. Визначити ключові тенденції сучасного етапу еволюції загроз у контексті розгортання мереж п’ятого покоління, розвитку мобільних фінансових сервісів, Інтернету речей та застосування хмарної інфраструктури, охарактеризувати особливості комплексних атак на мобільні пристрої;

5. Обґрунтувати доцільність адаптації сучасних концепцій кіберзахисту, зокрема підходу Zero Trust, керування мобільними пристроями та контейнеризації службової інформації, до специфіки використання мобільних технологій у підрозділах, що виконують завдання у сфері державної безпеки;

6. Розробити практичні рекомендації щодо підвищення ефективності системи запобігання, виявлення та реагування на загрози інформаційній

безпеці мобільних технологій у діяльності органів сектору безпеки та оборони України.

Методологічну основу дослідження становить поєднання загальнонаукових і спеціальних методів, притаманних науці кібербезпеки та теорії державної безпеки. У роботі використовуються методи аналізу та синтезу, індукції та дедукції, порівняльний і системний аналіз для узагальнення наукових підходів і виявлення закономірностей еволюції загроз. Структурно функціональний метод застосовується для дослідження ролі мобільних технологій у загальній архітектурі інформаційної безпеки. Методи загрозового моделювання та ризик орієнтованого аналізу використовуються для побудови моделі загроз мобільним пристроям на різних етапах їхнього розвитку. Статистичний аналіз та елементи контент аналізу аналітичних звітів міжнародних і національних організацій у сфері кібербезпеки використовуються для дослідження динаміки інцидентів та оцінювання їхнього впливу на стан інформаційної безпеки.

Наукова новизна одержаних результатів полягає в уточненні та подальшому розвитку теоретичних положень щодо еволюції загроз інформаційній безпеці у мобільних технологіях і адаптації цих положень до потреб сектору безпеки України.

У результаті проведеного дослідження:

- уточнено та систематизовано класифікацію загроз інформаційній безпеці мобільних технологій з урахуванням історичних етапів розвитку мобільних операційних систем і комунікаційних стандартів;
- одержало подальший розвиток наукове уявлення про взаємозв’язок між технологічними змінами в мобільному середовищі та трансформацією моделей атак, що дозволяє точніше прогнозувати появу нових загроз;
- запропоновано концептуальну модель загроз інформаційній безпеці мобільних технологій для умов діяльності органів сектору безпеки, яка інтегрує технічні, організаційні та людські фактори ризику;

- удосконалено підходи до організації захисту мобільних пристроїв у корпоративному та відомчому середовищі на основі принципів Zero Trust, керування мобільністю підприємства та розмежування службової і особистої інформації.

Практичне значення одержаних результатів полягає у можливості використання сформульованих у роботі висновків і рекомендацій у діяльності підрозділів, що відповідають за організацію кіберзахисту мобільних пристроїв, підготовку внутрішніх нормативних документів з питань безпечного використання мобільних технологій, а також у навчальному процесі при викладанні дисциплін із кібербезпеки та інформаційної безпеки. Запропоновані підходи можуть бути враховані під час удосконалення відомчих політик безпеки, інструкцій щодо використання мобільних пристроїв особовим складом, а також при плануванні заходів з підвищення обізнаності користувачів щодо мобільних загроз.

Апробація матеріалів дослідження. Автор за період навчання має одну опубліковану наукову статтю та дві опубліковані тези виступів на науково-практичних конференціях, зокрема:

1. Ковальова Т. І., Скоморохов В.А. Сучасні загрози інформаційній безпеці мобільних операційних систем Android та iOS. *«Національні інтереси України»: науково-практичний журнал.* 2025. № 12(17) 2025. С. 306-315**. DOI:** https://doi.org/10.52058/3041-1793-12(17)

2. Скоморохов В.А. Сучасні загрози від шкідливого програмного забезпечення (malware). *Сучасні наукові тенденції в роботах молодих вчених :* матеріали III науково-практичної конференції. (м. Київ 25 квітня 2025 р.). Київ : Київський інститут національної гвардії України, 2025. С. 190-193. (науковий керівник – Ковальова Т.І.). URL: https://kingu.edu.ua/naukovi-zahodi/

3. Скоморохов В.А. Deepfake: загроза цифрової дезінформації в секторі безпеки і оборони України. *Актуальні проблеми забезпечення державної* безпеки : матеріали III Всеукраїнської науково-практичної конференції

(м. Київ, 31 жовтня 2025 р.) – Київ : Київський інститут Національної гвардії України, 2025 – С. 248-251. (науковий керівник – Ковальова Т.І.). URL: https://kingu.edu.ua/naukovi-zahodi/

Структура кваліфікаційної роботи зумовлена метою та завданнями дослідження, складається зі вступу, трьох розділів, які охоплюють дев’ять підрозділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 107 сторінок, з яких основний текст – 88 сторінок, список використаних джерел (70 найменувань) – 7 сторінок.

РОЗДІЛ 1
ПОЧАТКОВИЙ ЕТАП 2000-І РОКИ СТАНОВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МОБІЛЬНИХ ТЕХНОЛОГІЯХ

1.1. Класифікація ранніх мобільних загроз: віруси, троянські програми, атаки через SMS та MMS

У двохтисячні роки мобільні телефони з функціями смартфона із нішевого продукту дуже швидко перетворилися на основний персональний комп'ютер користувача, що постійно підключений до мережі та зберігає чутливі дані. Така трансформація створила передумови для появи окремої категорії шкідливого програмного забезпечення, орієнтованого саме на мобільне середовище, де традиційні моделі захисту ще не були сформовані, а архітектура операційних систем і бізнес моделі виробників не враховували повною мірою вимоги до кібербезпеки. Перші зразки мобільних вірусів і троянських програм мали швидше експериментальний характер, але вже за кілька років вони еволюціонували до загроз, що здатні спричиняти реальні фінансові втрати, порушення конфіденційності та доступності сервісів. Саме початковий етап формування мобільних шкідливих програм у двохтисячних роках заклав типову класифікацію ранніх загроз, до яких належать віруси та черв'яки, що саморозмножуються, троянські програми з модифікацією системних компонентів, а також шкідливі атаки через текстові та мультимедійні повідомлення SMS та MMS [4, с. 46].

З погляду кібербезпеки принциповим є те, що перші мобільні шкідливі програми успадкували базові риси класичних комп'ютерних вірусів, проте адаптували їх до специфіки мобільних протоколів і обмежень апаратних ресурсів. Одним з ключових рубежів вважається поява у 2004 році черв'яка Cabir, який став першим задокументованим зразком шкідливого коду, що інфікує смартфони на базі Symbian і поширюється через інтерфейс Bluetooth

між пристроями в радіусі приблизно 10 метрів [29]. Cabir відображав на екрані пристрою повідомлення Caribe, запускався під час кожного вмикання телефону та постійно сканував простір на наявність інших пристроїв, на які надсилав інсталяційний файл у форматі SIS, істотно скорочуючи час роботи акумулятора [28]. Сам по собі черв'як не виконував деструктивних дій щодо даних, але демонстрував принципову можливість створення саморозмножуваного коду для мобільних платформ, що стало відправною точкою для подальшої еволюції мобільних вірусів.

Статистичні дані компаній, що спеціалізуються на антивірусному захисті, підтверджують швидке нарощування кількості мобільних загроз уже в перші роки після появи Cabir. Аналітичний огляд Rits Information Security зафіксував, що лише у першій половині 2005 року було ідентифіковано понад 50 різних вірусів та черв'яків, орієнтованих на мобільні платформи [69,с. 331]. При цьому більшість з них були варіантами декількох базових родин, що свідчить про активну модифікацію вже існуючого коду з метою обійти сигнатурні механізми виявлення. За даними Kaspersky Lab загальна кількість варіантів шкідливих програм для Symbian у подальшому досягла 621 зразка, а кількість сімейств склала десятки, що чітко демонструє формування окремого сегмента мобільної загрозової екосистеми [28]. Для фахівців з кібербезпеки це означало необхідність розроблення окремих політик виявлення та реагування не тільки на рівні операторів мобільного зв'язку, а й на рівні кінцевих пристроїв.

Окрему групу ранніх загроз становили троянські програми, які, на відміну від черв'яків, не завжди прагнули до саморозмноження, але активно використовували логічні вразливості операційних систем. Відомим прикладом став троян Skuller, вперше зафіксований у листопаді 2004 року, який замінював піктограми стандартних додатків Symbian на зображення черепа та схрещених кісток і пошкоджував системні файли, позбавляючи користувача доступу до основних функцій телефону [65, с. 39]. Особливість цього трояна полягала у

використанні конструктивного недоліку Symbian, який дозволяв будь якій програмі перезаписувати системні компоненти без належної перевірки прав доступу, що уможливлювало моделювання атак типу відмови в обслуговуванні на рівні інтерфейсу пристрою. З позицій класифікації загроз інформаційній безпеці Skuller належить до деструктивних троянів, орієнтованих на порушення доступності та цілісності системного програмного забезпечення, а не на пряме викрадення даних. Саме такі трояни демонстрували критичну важливість правильної моделі розмежування доступу в мобільних операційних системах та необхідність контролю цілісності системних файлів.

Мал.1.1 - Загальні принципи забезпечення комп'ютерної безпеки

Ще одним важливим етапом еволюції ранніх мобільних загроз стало розширення векторів поширення від локального бездротового інтерфейсу до мережевих сервісів оператора мобільного зв’язку. У 2005 році було виявлено

черв’як CommWarrior, який став однією з перших шкідливих програм, що одночасно використовувала Bluetooth та сервіс MMS для розповсюдження між телефонами на платформі Nokia Series 60 [69, с. 334]. Програма надсилала інсталяційний файл у вигляді вкладення до мультимедійного повідомлення контактам з адресної книги інфікованого телефону, формуючи ілюзію того, що лист надійшов від знайомої особи, що значно підвищувало ймовірність відкриття повідомлення. Після запуску файл встановлювався як програма для Symbian і активувався при кожному ввімкненні пристрою, а далі черв’як продовжував розсилати копії самого себе вже з нових заражених телефонів. Аналіз поширення CommWarrior продемонстрував, що через механізм автоматичної відправки MMS без відома користувача він зміг інфікувати понад 115 000 мобільних пристроїв та надіслати понад 450 000 мультимедійних повідомлень у більш ніж 18 країнах Європи, Азії та Північної Америки [66, с. 286]. Для операторів мобільного зв’язку це означало не лише ризик перевантаження інфраструктури, а й прямі фінансові втрати абонентів, які оплачували небажані повідомлення.

Розвиток троянських програм, орієнтованих на SMS трафік, став першим прикладом системної монетизації мобільного шкідливого програмного забезпечення. На відміну від Cabir або Skuller низка троянів на основі Java 2 Micro Edition з’являлася у вигляді нібито корисних додатків з простим функціоналом, наприклад псевдо браузерів чи утиліт, які після інсталяції непомітно для користувача відправляли текстові повідомлення на короткі платні номери. Одним з перших відомих прикладів стала програма RedBrowser, яка маскувалася під WAP браузер, але замість доступу до Інтернету надсилала платні SMS на шахрайський номер [28]. Такий підхід дозволив зловмисникам отримувати частку прибутку від мобільних операторів, які надавали послуги преміум нумерації, і сформував окрему категорію SMS троянів як фінансово мотивованих загроз. З точки зору класифікації ранніх мобільних загроз вони належать до троянських програм з

прихованою тарифікацією, що порушують фінансову складову конфіденційності та цілісності рахунку користувача.

Кількісна динаміка мобільних загроз у другій половині двохтисячних років підтверджує швидкий перехід від поодиноких експериментальних зразків до широкого спектра сімейств і варіантів. За результатами аналізу, виконаного на основі звітів провідних лабораторій, з 2004 по 2009 роки було виявлено близько 400 різних версій мобільних вірусів і троянських програм, а в період з 2009 по кінець 2010 року кількість нових варіантів зросла приблизно на 175 % [33, с. 591]. Окреме дослідження мобільного шкідливого коду показало, що для Symbian було ідентифіковано 74 сімейства з 311 варіантами, для J2ME 45 сімейств з 613 варіантами, для Windows Mobile 16 сімейств з 54 варіантами, що демонструє концентрацію загроз саме на двох домінуючих на той час платформах Symbian та J2ME [70, с. 4]. Для фахівців з кібербезпеки це стало сигналом про необхідність переходу від епізодичного реагування до системного моніторингу, розроблення поведінкових методів виявлення та інтеграції антивірусного захисту безпосередньо в прошивку мобільних пристроїв і в інфраструктуру оператора.

Узагальнюючи класифікацію ранніх мобільних загроз у двохтисячних роках, можна виділити щонайменше три базові групи, кожна з яких має специфічні для мобільного середовища вектори атак і наслідки для інформаційної безпеки. Перша група це віруси та мережеві черв’яки, подібні до Cabir та CommWarrior, які покладаються на автоматизоване поширення через Bluetooth або MMS і головним чином спрямовані на порушення доступності ресурсів і розширення масштабу зараження. Друга група це деструктивні троянські програми для Symbian, що експлуатують логічні вразливості файлової системи та механізмів інсталяції, змінюючи або пошкоджуючи системні компоненти і тим самим створюючи стійкі відмови в роботі пристрою. Третя група це SMS трояни, які використовують канали оператора зв’язку для прихованого надсилання платних повідомлень і

безпосередньо націлені на фінансові ресурси користувача. Усі ці категорії сформували початковий профіль ризиків для мобільних технологій та заклали підґрунтя для більш складних шкідливих програм наступного покоління, які вже поєднували декілька функцій, приховували свою активність, застосовували методи соціальної інженерії та спрямовувалися не лише на кінцевих користувачів, а й на корпоративну інфраструктуру.

1.2. Особливості безпеки мобільних операційних систем Symbian та Windows Mobile: моделі прав доступу та вразливості

Аналіз безпеки мобільних операційних систем початку двохтисячних років неможливо здійснювати без детального розгляду Symbian та Windows Mobile, оскільки саме ці платформи формували архітектуру перших смартфонів і визначали початкові підходи до моделювання прав доступу та протидії загрозам. За даними галузевих аналітиків, уже у 2006 році частка Symbian на ринку смартфонів коливалася в діапазоні від 60 % до 67 %, тоді як Windows Mobile займала приблизно 9 % глобального ринку, що робило Symbian основною ціллю для зловмисників, а Windows Mobile важливим, але більш нішевим рішенням, орієнтованим на бізнес сегмент та корпоративних користувачів [70, с. 8; 65, с. 39].

Мал.1.2 - Поняття і класифікація загроз

Початкові версії Symbian до дев’ятої лінійки практично не містили повноцінної моделі розмежування привілеїв у сучасному розумінні. Більшість прикладних програм працювали в одному логічному просторі користувача з широким доступом до файлової системи, базових системних API та апаратних ресурсів, таких як модуль стільникового зв’язку, Bluetooth, інфрачервоний порт, засоби збереження контактів і повідомлень. Інсталяційні пакети у форматі SIS могли перезаписувати наявні системні компоненти без криптографічної перевірки їхнього походження, що дозволяло троянським програмам на кшталт Skuller замінювати піктограми стандартних застосунків і пошкоджувати критично важливі файли прошивки без жодного попередження для користувача [14, с. 302]. У термінах кібербезпеки така архітектура означала відсутність чітких меж між рівнем операційної системи та рівнем прикладних програм і створювала дуже широку площину атаки для шкідливого коду, який міг діяти від імені користувача з практично повними правами.

Поява перших масових мобільних вірусів і черв’яків стала каталізатором глибокої реформи моделі безпеки Symbian. У версії Symbian OS 9 було впроваджено платформну безпеку, яка спиралася на три базові концепції: процес як одиниця довіри, capability орієнтований контроль привілеїв і механізм так званого клітинного зберігання даних, що отримав назву data caging [18]. Модель довіри передбачала поділ всього виконуваного коду на декілька рівнів з різним ступенем повноважень: код виробника пристрою та оператора мобільного зв’язку, системні компоненти та сторонні прикладні програми. Для кожного рівня визначалися власні вимоги до цифрового підпису й перелік доступних чутливих привілеїв, причому невірно підписаний або непідписаний пакет за замовчуванням розглядався системою як потенційно небезпечний і підлягав суттєвим обмеженням.

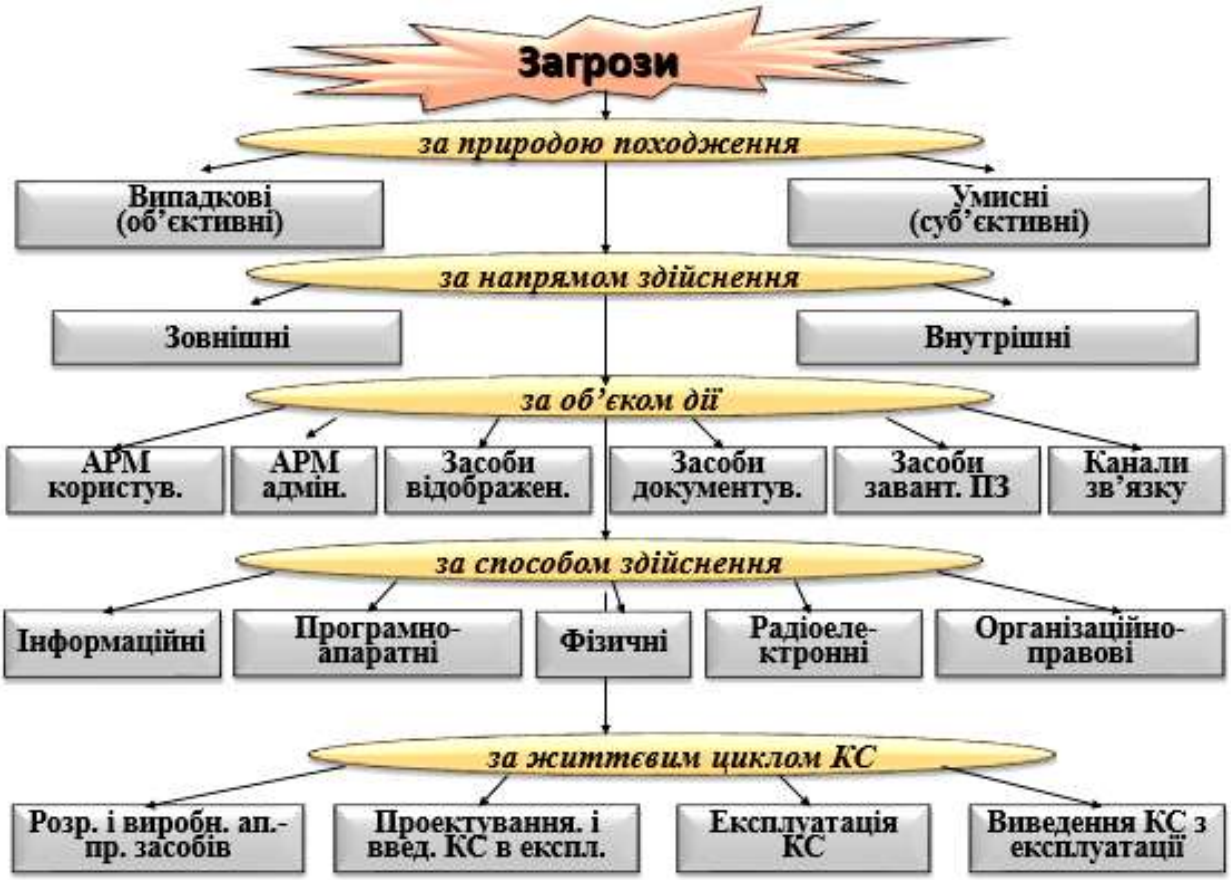
Ключовим елементом Symbian OS 9 стала capability модель, у межах якої кожному процесу надавався фіксований набір прав доступу до певних груп ресурсів. До таких ресурсів належали мережеві сервіси, доступ до контактів та журналу викликів, читання і запис користувацьких файлів, доступ до геолокаційних даних, керування дзвінками, взаємодія з апаратними інтерфейсами низького рівня та змінення системних налаштувань. У технічній документації описано понад 20 типових capability, серед яких NetworkServices, ReadUserData, WriteUserData, Location, PowerMgmt, DiskAdmin, CommDD, MultimediaDD [18; 37]. Принципово важливо, що набір capability закріплювався на етапі інсталяції та залежав від довіреності сертифіката, яким був підписаний додаток. Під час виконання процес не міг самостійно підвищити власні привілеї або завантажити бібліотеку, підписану з ширшим набором capability, що суттєво ускладнювало спроби вертикального підвищення привілеїв за класичними сценаріями атак.

Механізм data caging доповнював capability модель за рахунок організації доступу до файлової системи. Починаючи з Symbian OS 9 кожен процес отримував власний захищений простір даних у вигляді приватної директорії, до якої не могли звертатися інші процеси без наявності спеціальних привілеїв. Найбільш критичні системні файли та конфігураційні дані зберігалися у так званих закритих областях файлової системи, доступ до яких мали тільки процеси з високими системними capability або код виробника апаратного забезпечення [38, с. 117]. Така архітектура зменшувала ризик того, що навіть успішно запущена шкідлива програма без широкого набору привілеїв отримає змогу читати або модифікувати дані інших застосунків чи компоненти операційної системи. З погляду кібербезпеки data caging фактично реалізовував принцип розділення обов’язків на рівні файлів і дозволяв створювати чіткі межі довіри всередині єдиного пристрою.

Разом з тим практичний досвід експлуатації Symbian засвідчив, що навіть структурно продумана модель платформної безпеки може бути

вразливою у точках, пов’язаних із процесами підпису та сертифікації. У низці випадків шкідливі програми для Symbian були офіційно підписані через сервіс Symbian Signed і отримали формальний статус довіреного коду, що дало їм змогу користуватися розширеним набором capability [41, с. 107]. Інциденти з поширенням підписаного мобільного шкідливого програмного забезпечення змусили розробників переглянути алгоритми автоматизованої перевірки та посилити процедури аналізу поведінки програм перед видачею сертифіката, проте сам факт таких випадків продемонстрував, що компрометація ланцюга довіри здатна нівелювати переваги навіть досить суворої моделі прав доступу.

На тлі еволюції Symbian операційна система Windows Mobile розвивалася в дещо іншій логіці ідеології безпеки. Вона базувалася на основі ядра Windows CE і від початку орієнтувалася на можливість централізованого управління пристроями з боку оператора чи корпоративного адміністратора. Модель безпеки Windows Mobile реалізовувалася через декілька типових конфігурацій, які задавали, по суті, режим перевірки підпису та поділ застосунків на привілейовані й непривілейовані. У дво рівневій моделі визначалися два окремі сховища сертифікатів, які відповідали за привілейований та звичайний виконуваний код, а доступ до повного набору системних API на кшталт роботи з реєстром, налаштуваннями політик безпеки та керуванням бездротовими інтерфейсами отримували лише ті програми, що були підписані сертифікатами з привілейованого сховища [49, с. 137].



Мал.1.3 - Порушення безпеки інформації

У найбільш жорсткій конфігурації дворівнева заблокована модель повністю забороняла запуск непідписаного коду. Будь який застосунок, який не мав дійсного підпису з довіреного списку сертифікатів, взагалі не міг бути виконаний, незалежно від волі користувача. Більш м'які конфігурації дозволяли запуск непідписаних програм, але обмежували їх доступ лише до підмножини доступних API, тоді як привілейовані функції залишалися доступними виключно для підписаного коду. Такий підхід наближав Windows Mobile до класичного поділу на привілейовані та користувацькі контексти, характерного для настільних систем сімейства Windows, і водночас залишав простір для гнучкого налаштування політик на рівні конкретного оператора або корпоративного замовника [39]. Гнучкість налаштувань у випадку Windows Mobile стала одночасно перевагою та потенційним джерелом ризику. Для корпоративних розгортань виробники й адміністратори, як правило, використовували заблоковані моделі з повною забороною непідписаного коду

і обмеженим переліком довірених сертифікатів, що значно зменшувало ймовірність інфікування пристроїв шкідливими додатками. Натомість частина споживчих пристроїв постачалася з більш ліберальними політиками безпеки, які дозволяли інсталяцію та запуск непідписаних програм, а відтак покладалися на поінформованість користувача й елементарні механізми підтвердження дій, що залишало можливість для атак, заснованих на соціальній інженерії. Водночас обмежена ринкова частка Windows Mobile та її фокус на корпоративному сегменті призвели до того, що кількість шкідливих програм для цієї платформи залишалася відчутно меншою, ніж для Symbian, що зафіксовано в аналітичних оглядах еволюції мобільного шкідливого програмного забезпечення [54, с. 209].

Порівняльний розгляд моделей прав доступу Symbian та Windows Mobile показує, що обидві платформи зробили суттєвий внесок у формування сучасних підходів до безпеки мобільних операційних систем, але реалізували їх через різні архітектурні рішення. Symbian продемонструвала переваги детально налаштованої capability моделі в поєднанні з ізоляцією даних, проте виявила чутливість до проблемних моментів у ланцюгу сертифікації. Windows Mobile продемонструвала ефективність дворівневої моделі з чітким поділом на привілейований і непривілейований код, але значною мірою покладалася на налаштування політик безпеки з боку операторів і корпоративних адміністраторів. Для сучасних систем, що домінують на ринку, досвід цих платформ став фактично відправною точкою для розроблення більш комплексних моделей, які поєднують sandbox, явну систему дозволів і захист ядра, що враховують уроки, отримані саме на прикладі Symbian та Windows Mobile.

1.3. Канали поширення та вектори атак: Bluetooth, інфрачервоний канал, сторонні інсталяції, соціальна інженерія

На початковому етапі розвитку мобільних технологій канали поширення шкідливого програмного забезпечення безпосередньо визначали можливості зловмисників щодо швидкості зараження, географічного охоплення та складності побудови атак. Дослідження показують, що у 2004-2006 роках переважна більшість відомих мобільних вірусів та черв'яків для Symbian і Windows Mobile використовували комбінацію бездротових інтерфейсів короткого радіусу дії, сервісів оператора мобільного зв'язку і механізмів ручної інсталяції, при цьому майже завжди опиралися на взаємодію з користувачем у формі соціальної інженерії [14, с. 304; 25, с. 159]. Це означає, що для фахівця з кібербезпеки ранні мобільні атаки потрібно розглядати не лише як експлуатацію технічних уразливостей протоколів Bluetooth або стеків обміну даними, а як складну комбінацію радіоканалів, форматів файлів і типових моделей поведінки користувачів, які підтверджують приймання та встановлення шкідливих додатків.

Bluetooth став першим масовим каналом поширення мобільних черв'яків, оскільки його поява у смартфонах забезпечила можливість прямого обміну файлами між пристроями у радіусі приблизно 10-20 метрів без участі оператора зв'язку [16, с. 98]. Для черв'яка Cabir типовим сценарієм зараження виглядав як послідовність спроб надіслати файл інсталяційного пакета SIS на всі доступні пристрої з увімкненим Bluetooth у режимі видимості. На рівні протоколу для встановлення з'єднання черв'як ініціював стандартний процес виявлення пристроїв, після чого автоматично надсилав файл, який користувачеві пропонувалося прийняти. Аналіз інфекційних ланцюжків показав, що у типових міських умовах з щільністю кількох десятків смартфонів у громадському місці один інфікований телефон за день міг здійснювати сотні спроб надсилання файла і реально заражати від 5 до 10 нових пристроїв, залежно від того, наскільки часто користувачі підтверджували приймання невідомих файлів [24, с. 40; 42, с. 12]. У закритих просторах із високою концентрацією людей на кшталт стадіонів або

конференц залів Bluetooth черв’яки демонстрували майже «епідеміологічну» динаміку поширення, коли одна подія з кількома тисячами присутніх могла привести до десятків або сотень заражених пристроїв протягом кількох годин.

Мал.1.4 - Загрози за напрямом здійснення

Важливим обмеженням Bluetooth як каналу поширення було те, що, навіть за наявності технічної можливості автоматично надсилати файли, запуск шкідливого коду у більшості випадків вимагав активної участі користувача. Для того щоб Cabir або подібний черв’як розпочав виконання, користувач мав щонайменше тричі підтвердити свої дії, тобто погодитися на приймання файла, погодитися на його запуск і підтвердити встановлення пакета [50, с. 86]. На практиці саме цей фактор тримав реальний рівень заражень значно нижче потенційно можливого для повністю автоматизованого мережевого черв’яка, оскільки частина користувачів відхиляла невідомі запити. Разом з тим дослідження поведінки користувачів мобільних пристроїв показують, що люди загалом більш схильні натискати на підозрілі посилання та погоджуватися з діалогами без глибокого аналізу, ніж користувачі настільних систем, імовірність взаємодії з шкідливим контентом на мобільному пристрої оцінюється як у середньому у 18 разів вища [48, с. 109].

Саме поєднання короткого радіуса дії, великої кількості потенційних цілей у громадських місцях та людської довірливості робило Bluetooth одним з ключових векторів атак для перших мобільних черв'яків.

Інфрачервоний канал передачі даних, який використовувався у перших поколіннях смартфонів і комунікаторів, також розглядався дослідниками як потенційний канал поширення шкідливого коду, проте його реальний внесок в еволюцію мобільних загроз був значно нижчим порівняно з Bluetooth [53]. Інфрачервоні порти потребували прямої видимості між пристроями та точного позиціонування, що істотно знижувало ймовірність випадкових контактів між незнайомими телефонами. Передача файлів через інфрачервоний інтерфейс зазвичай відбувалася як свідоме спільне рішення двох користувачів, які фізично підносили пристрої один до одного. Тому для зловмисника використання цього каналу вимагало набагато більшої частки соціальної інженерії, пов'язаної з особистою взаємодією, а не анонімним широкомовним розсиланням запитів, характерним для Bluetooth. У наукових оглядах, присвячених історії мобільного шкідливого програмного забезпечення, інфрачервоний канал згадується як теоретично можливий, але мало використовуваний вектор, і відсутні дані про масові інфекції, які були б пов'язані саме з цим способом передачі [46, с. 151].

Значно вагомішу роль відіграли сторонні інсталяції програм, тобто встановлення пакетів не з офіційних або добре контрольованих джерел, а з неформальних веб сайтів, форумів або через прямий обмін файлами між користувачами. Для Symbian такими пакетами були файли SIS, для Java 2 Micro Edition типово використовувалися пари файлів JAR та JAD, для Windows Mobile застосовувалися CAB пакети. Аналіз «дикої» вибірки мобільного шкідливого програмного забезпечення показав, що значна частина загроз до 2006 року поширювалася саме у формі так званих троянських інсталяцій, коли користувач свідомо завантажував і запускав програму, яка позиціонувалася як корисний застосунок, гра або утиліта, проте містила шкідливий компонент [44,

с. 86]. Типовим прикладом став уже згаданий RedBrowser, який маскувався під браузер для доступу до WAP сайтів, але після інсталяції відправляв платні SMS на короткі номери, генеруючи прямі фінансові збитки для користувача [52, с. 24].

Мал.1.5 - Класифікація загроз безпеки КС

У міру зростання кількості смартфонів та переходу частини мобільного трафіку на канали передачі даних, зокрема GPRS і EDGE, сторонні інсталяції почали поєднуватися з іншими каналами поширення. Зловмисники використовували SMS та MMS для надсилання посилань на веб сторінки, де розміщувалися шкідливі інсталяційні пакети, а також застосовували електронну пошту і мобільні версії форумів для розповсюдження модифікованих додатків [22, с. 50]. Дослідження динаміки мобільних загроз за 2004-2006 роки показали, що хоча Bluetooth і MMS відігравали помітну роль, значна частина інфекцій все ж таки була пов’язана з прямим завантаженням і

встановленням шкідливих програм користувачами, які не усвідомлювали ризики, пов’язані з неофіційними джерелами програмного забезпечення [21]. Для фахівця з кібербезпеки це означало необхідність поєднання технічних засобів контролю джерел інсталяцій з активними програмами підвищення обізнаності користувачів.

Соціальна інженерія стала об’єднувальним чинником для всіх перелічених каналів поширення. У випадку Bluetooth користувача переконували прийняти файл із нейтральною або привабливою назвою, яка не викликала підозр, а у деяких модифікаціях шкідливого коду додатково використовувалися повідомлення, що імітували системні запити або запрошення від знайомих контактів [28; 36, с. 40]. У випадку MMS та SMS використовувалися короткі тексти з провокаційним змістом або посиланнями на «фотографії» та «оновлення», що стимулювало користувача відкривати вкладення чи переходити за URL. Статистичні дослідження мобільного фішингу свідчать, що користувачі смартфонів у кілька разів частіше натискають на посилання з SMS порівняно з аналогічними повідомленнями електронної пошти, що пов’язано з довірою до мобільних меседжів та обмеженим розміром екрана, який ускладнює перевірку повного доменного імені [35, с. 42]. На рівні сторонніх інсталяцій соціальна інженерія реалізувалася через обіцянку «безплатних» версій комерційних продуктів, доступу до розважального контенту або корисних утиліт, причому зловмисники часто копіювали інтерфейс легітимних додатків, щоб користувач не помічав підміни.

Узагальнюючи аналіз каналів поширення і векторів атак на початковому етапі еволюції мобільних загроз, можна зробити висновок, що технічні можливості протоколів і сервісів, таких як Bluetooth, MMS, інфрачервоний інтерфейс та механізми інсталяції, лише створювали передумови для інфекцій, тоді як ключовим «активатором» нападів залишалася поведінка користувачів. Моделювання поширення мобільних черв’яків показало, що для реалізації

масштабних спалахів зразка CommWarrior, який інфікував щонайменше 115 000 пристроїв і надіслав понад 450 000 повідомлень MMS у більш як 18 країнах, потрібне поєднання високої щільності пристроїв, активного використання бездротових сервісів і низького рівня обізнаності користувачів.

ВИСНОВКИ ДО РОЗДІЛУ 1

Аналіз початкового етапу розвитку мобільних технологій у двохтисячних роках показав, що саме в цей період відбулося становлення окремого сегмента загроз інформаційній безпеці, орієнтованих на мобільні пристрої. Від поодиноких експериментальних зразків на кшталт перших вірусів і черв’яків для Symbian еволюція дуже швидко перейшла до формування десятків сімейств і сотень варіантів шкідливого програмного забезпечення, яке навмисно враховувало специфіку апаратних обмежень, протоколів зв’язку та моделі поведінки мобільних користувачів. Мобільний телефон з засобу голосового зв’язку перетворився на персональний обчислювальний пристрій з доступом до Інтернету, контактів, приватних повідомлень і фінансових сервісів, що зробило його привабливою ціллю для зловмисників і суттєво збільшило ціну компрометації для користувача.

Систематизація ранніх мобільних загроз дала змогу виділити три базові класи шкідливих програм, які визначили подальшу еволюцію атак. По перше, це віруси та мережеві черв’яки, що зосереджувалися на саморозмноженні та порушенні доступності ресурсів, типові приклади яких Cabir і CommWarrior продемонстрували можливість масштабного зараження через Bluetooth та MMS. По друге, це деструктивні троянські програми для Symbian, які використовували відсутність повноцінної моделі розмежування привілеїв і можливість перезапису системних файлів, спричиняючи масові відмови у роботі пристроїв. По третє, це SMS трояни з прихованою тарифікацією, які переорієнтували мобільні загрози з суто технічних експериментів у сферу

криміналізованої діяльності з чіткою фінансовою мотивацією і показали, що мобільні оператори та платіжна інфраструктура стають невід'ємною частиною ланцюга атак.

Розгляд особливостей мобільних операційних систем Symbian та Windows Mobile показав, що моделі прав доступу й механізми безпеки, закладені у їхню архітектуру, одночасно стримували та стимулювали розвиток певних класів загроз. Ранні версії Symbian без наскрізної моделі розмежування привілеїв спростили появу троянів, які модифікували системні компоненти, а перехід до платформної безпеки з capability моделлю та ізоляцією даних значно підвищив загальний рівень захищеності, але виявив критичну залежність від якості процесів сертифікації та підпису коду. Windows Mobile з дво рівневою моделлю привілейованих і непривілейованих додатків орієнтувалася на централізоване керування і дала змогу корпоративним користувачам застосовувати жорсткі політики, проте у споживчому сегменті залишала простір для зловживань через ліберальні конфігурації безпеки. Для кібербезпеки загалом цей досвід засвідчив, що ефективність архітектурних рішень безпосередньо визначається тим, як вони впроваджуються у реальних продуктах і наскільки послідовно підтримуються усі елементи ланцюга довіри.

Детальний аналіз каналів поширення та векторів атак дав можливість побачити, що технічні механізми Bluetooth, інфрачервоних інтерфейсів, сервісів SMS та MMS, а також сторонніх інсталяцій лише створювали базову інфраструктуру для зараження, тоді як основним фактором успіху атак залишалася соціальна інженерія. Саме користувач, який погоджувався прийняти і встановити невідомий файл, переходив за посиланням з SMS або інсталював неофіційну «безплатну» програму, фактично завершував ланцюг компрометації. Моделювання спалахів шкідливих програм показало, що для таких черв'яків, як CommWarrior, визначальними були не лише технічні можливості мережевої інфраструктури, а й висока щільність пристроїв та

низький рівень обізнаності користувачів щодо мобільних ризиків. Це зумовило усвідомлення необхідності комплексного підходу до мобільної безпеки, який поєднує протокол рівневі механізми обмеження каналів поширення з системним підвищенням культури безпечної поведінки користувачів.

У цілому результати, отримані у розділі 1, дозволяють сформулювати низку ключових положень для подальшого дослідження еволюції загроз у мобільних технологіях. По перше, ранній етап довів, що мобільні платформи швидко стають повноцінним полем бою у кіберпросторі, а отже мають розглядатися у стратегіях кібербезпеки на рівні з традиційними інформаційно телекомунікаційними системами. По друге, архітектурні рішення щодо моделі прав доступу, ізоляції даних і механізмів підпису коду мають випереджати очікуваний спектр загроз, а не наздоганяти його постфактум, оскільки виправлення системних недоліків вже після появи шкідливого програмного забезпечення є дорогим і не завжди ефективним. По третє, канали поширення та вектори атак, що сформувалися у двохтисячних роках, заклали підґрунтя для сучасних багатоканальних атак, які поєднують мережеві протоколи, мобільні додатки, соціальні мережі та платіжні сервіси. Саме тому подальший аналіз, здійснений у наступних розділах, повинен враховувати виявлені закономірності початкового етапу як базовий шар еволюційної моделі загроз для мобільних технологій.

РОЗДІЛ 2.
ПЕРЕХІД НА СМАРТФОНИ 2010-ТІ РОКИ ЕКОСИСТЕМИ, МАРКЕТИ ЗАСТОСУНКІВ ТА НОВІ РИЗИКИ

2.1. Еволюція загроз у контексті Android та iOS: рут-доступ, джейлбрейк, рекламне програмне забезпечення, програми-вимагачі

Перехід від «кнопкових» телефонів до повноцінних смартфонів у 2010 х роках докорінно змінив як саму мобільну екосистему, так і структуру загроз інформаційній безпеці. Поява Android та iOS як домінуючих платформ, розбудова централізованих маркетів застосунків та масове підключення користувачів до мобільного Інтернету привели до вибухового зростання кількості шкідливих програм, орієнтованих уже не на окремі моделі пристроїв, а на цілі програмні екосистеми. Аналітика лабораторій безпеки показує, що до 2015 року було зафіксовано близько 1,5 млн. зразків Android шкідливого програмного забезпечення, при цьому за період з 2011 по 2015 роки кількість унікальних мобільних шкідливих програм подвоювалася упродовж окремих років майже на 100 % [2, с. 92]. Саме на тлі цього стрімкого зростання починає формуватися нове покоління загроз, пов’язане з Root доступом і джейлбрейком, рекламним програмним забезпеченням та мобільними програмами вимагачами.

Перевага Android у глобальній структурі ринку смартфонів, яка у середині 2010-х років стабільно перевищувала 80 %, у поєднанні з відкритою моделлю поширення застосунків зробила цю платформу основною мішенню для кіберзлочинців [7, с. 201]. Згідно з даними F Secure частка Android в структурі всього мобільного шкідливого програмного забезпечення зросла з приблизно 11,25 % у 2010 році до 66,7 % у 2011 році і до 79 %у 2012 році, що означало фактичне домінування цієї платформи в сегменті мобільних загроз [9, с. 178]. Подальші оцінки свідчать, що до 2018 року загальна кількість

відомих зразків Android шкідливих програм досягла приблизно 26,61 млн., а тільки у 2016 році G DATA зафіксувала понад 3,2 млн. нових файлів Android шкідливого програмного забезпечення, тобто у середньому близько 8,4 тис. нових зразків щодня [17, с. 92]. Паралельні дані AV Test підтверджують тренд зсуву загального фокуса шкідливого програмного забезпечення від класичних настільних систем до Android, частка якого у загальній структурі усіх відомих зразків зросла з приблизно 3 % до 7,4 % за один рік [20, с. 111].

На цьому фоні особливого значення набуває поняття Root доступу в Android, тобто отримання прав адміністратора, які дозволяють програмам обходити стандартну модель дозволів, змінювати системні файли, встановлювати додаткові компоненти та втручатися у роботу інших застосунків. У технічному сенсі Root доступ реалізується або через навмисну модифікацію образу прошивки користувачем, або через експлуатацію вразливостей ядра та системних служб, коли відповідний експлойт інтегрується безпосередньо у тіло шкідливої програми. Дослідження еволюції Android шкідливого програмного забезпечення показали, що низка сімейств цілеспрямовано включала модулі для отримання Root доступу негайно після інфікування для закріплення контролю над пристроєм, установки додаткових компонентів та ускладнення видалення шкідливого коду [20, с. 112]. З позицій кібербезпеки це означає, що навіть формально обмежені за правами програми, які спочатку запитують мінімальний набір дозволів, можуть на практиці переходити у привілейований режим, якщо вдається експлуатувати відповідну вразливість в операційній системі.

Не менш істотним є сегмент користувачів, які самостійно виконують рутування пристрою з метою розширення функціональності. Аналітичні огляди провідних компаній безпеки наголошують, що рутовані телефони в середньому у кілька разів частіше інфікуються шкідливим програмним забезпеченням, ніж «чисті» пристрої з заводською прошивкою, а за окремими оцінками експозиція рутованих пристроїв може бути від 3 до приблизно

3 000 разів вищою, ніж у нерутованих [19, с. 79]. Причинами цього є втрата частини механізмів ізоляції процесів, можливість встановлення застосунків у системні розділи, а також блокування оновлень безпеки, оскільки успішне рутування часто спирається на невиправлені вразливості ядра. В результаті будь яке шкідливе програмне забезпечення, що потрапляє на рутований пристрій, отримує значно ширші можливості для приховування своєї присутності, встановлення бекдорів та організації стійкого несанкціонованого доступу.

Для iOS ключовим поняттям другого етапу еволюції мобільних загроз є джейлбрейк, тобто навмисне зняття програмних обмежень, які Apple інтегрує в операційну систему. Модель безпеки iOS за замовчуванням базується на жорсткому застосуванні підпису коду, централізованому контролі за поширенням застосунків через App Store та ізоляції кожної програми в окремому sandbox середовищі. Джейлбрейк порушує цю модель, оскільки використовує ланцюг вразливостей, що дозволяють виконання непідписаного коду з підвищеними привілеями, модифікацію ядра і вимикання або послаблення перевірок підпису та ізоляції [18]. Експерти з мобільної безпеки наголошують, що джейлбрейковані пристрої значно більш вразливі до шкідливих програм, атак з боку мережі та крадіжки даних, оскільки втрачають частину вбудованих механізмів захисту і часто не отримують регулярних оновлень безпеки.

У контексті рекламного шкідливого програмного забезпечення смартфони на базі Android стають ключовим майданчиком для монетизації зловмисної діяльності за рахунок агресивного показу реклами, прихованих кліків та збору маркетингових профілів. За даними досліджень Avast і низки партнерів, станом на кінець 2010-х років рекламне шкідливе програмне забезпечення становило до 72 % усіх мобільних загроз, а його частка серед Android шкідливого програмного забезпечення зросла приблизно на 38 % лише за один рік [41, с. 108]. Додаткові спостереження Kaspersky Lab

підтверджують, що у 2019 році частка атак з використанням рекламних компонентів становила близько 12,85 %від усіх мобільних інцидентів, а у 2020 році вже 14,62 %, що відображає стабільну тенденцію до зростання [45, с. 106]. Окремі звіти Dr Web зафіксували випадки, коли активність троянів родини HiddenAds збільшувалася майже на 46 % протягом одного місяця, що свідчить про значну динаміку поширення рекламних кампаній, пов’язаних із шкідливими або небажаними застосунками [41, с. 109].

Сучасні дослідження показують, що мобільне рекламне шкідливе програмне забезпечення майже завжди маскується під легітимні ігрові або розважальні застосунки з високою популярністю, що гарантує швидкий приріст інсталяцій [42, с. 13]. Такі програми інтегрують сторонні рекламні бібліотеки, які у прихованому режимі генерують фонові кліки по рекламних оголошеннях, відображають нав’язливі банери поверх інших застосунків, збирають детальні технічні параметри пристрою та іноді завантажують додаткові модулі без явної згоди користувача. З точки зору кібербезпеки рекламне шкідливе програмне забезпечення небезпечне не лише як фактор, що порушує конфіденційність та зручність використання, а й як можливий «міст» до складніших атак, оскільки інфіковані рекламні мережі можуть бути використані для поширення експлойтів, фішингових сторінок і завантаження програм вимагачів.

Особливе місце в еволюції мобільних загроз 2010 х років посідають програми вимагачі для Android, які поєднали фінансову мотивацію з технічно складними механізмами блокування та шифрування даних. Перші «поліцейські» вимагачі обмежувалися блокуванням екрана, відображенням повідомлення від імені вигаданих правоохоронних органів і вимогою сплатити штраф, проте вже у 2014 році дослідники ESET зафіксували Simplocker, який став першим широко задокументованим криптовимагачем для Android, що шифрував файли на картці пам’яті і вимагав викуп за їх розшифрування [26, с. 44]. Початкові варіанти Simplocker орієнтувалися насамперед на

користувачів з України та росії, а вже за кілька місяців з’явилися модифікації, націлені на англомовний сегмент. Подальший розвиток цього сімейства продемонстрував перехід від простих схем з фіксованим ключем шифрування до моделей, у яких для кожного пристрою генерувався унікальний ключ, що істотно ускладнювало процедуру дешифрування без сплати викупу.

Комплексні дослідження Android вимагачів показують, що вже у середині 2010-х років вони сформували окремий підклас мобільних загроз, у якому застосовувалися класичні підходи з десктопного середовища, включно з використанням стійких алгоритмів шифрування, багаторівневого завантаження через проміжні завантажувачі та активним використанням механізмів соціальної інженерії для переконання користувача сплатити викуп [23, с. 115]. Середній розмір викупу в окремих кампаніях оцінювався в діапазоні від 100 до 500 доларів США, при цьому платіжні інструкції часто передбачали використання ваучерів попереднього платежу, а згодом криптовалют, що ускладнювало відстеження транзакцій [55, с. 61]. Основними каналами поширення програм вимагачів були сторонні маркети застосунків, заражені рекламні мережі, а також посилання у SMS та інтегровані реклами в легітимних застосунках, які перенаправляли користувача на сторінки завантаження шкідливого пакета.

Аналіз каналів розподілу мобільних застосунків у цей період свідчить, що, попри посилення контролю з боку Google, офіційний магазин Google Play залишався ключовим каналом розповсюдження як легітимних, так і небажаних програм. Дослідження, виконане на вибірці 12 млн. пристроїв та 7,9 млн. застосунків, показало, що від 10 % до 24 % пристроїв хоча б раз стикалися з небажаною програмою, а Google Play відповідав приблизно за 87 % усіх інсталяцій і близько 67 % установок небажаних програм [58]. Це означає, що навіть централізована екосистема з формальним модераційним процесом не гарантує повної відсутності загроз, якщо масштаб платформи і економічна привабливість ринку стимулюють зловмисників до постійного пошуку

способів обходу перевірок. Для iOS офіційний магазин залишався значно більш закритим, що стримувало масове проникнення шкідливих програм, але джейлбрейковані пристрої, які мали доступ до неофіційних репозиторіїв, опинялися у схожій зоні ризику.

Таким чином, еволюція загроз у контексті Android та iOS у 2010-х роках характеризується переходом від «класичних» мобільних вірусів до складної екосистеми шкідливого програмного забезпечення, у якій Root доступ та джейлбрейк використовуються як інструменти обходу вбудованих моделей захисту, рекламне шкідливе програмне забезпечення стає масовим засобом прихованої монетизації, а програми вимагачі трансформують мобільний пристрій на безпосереднє джерело фінансового тиску на користувача. Для кібербезпеки це означає необхідність розглядати мобільні платформи як повноцінний об’єкт багаторівневого захисту, у якому технічні механізми операційних систем мають доповнюватися контролем екосистеми маркетів застосунків, системами виявлення Root доступу та джейлбрейку, аналізом рекламних компонентів і цілеспрямованими програмами підвищення обізнаності користувачів щодо ризиків, пов’язаних з інсталяцією сторонніх програм та наданням розширених привілеїв.

Таблиця 2.1 – Основні типи загроз в екосистемах Android та iOS у 2010-ті роки

Тип загрози	**Платформа**	**Період пікової активності**	**Ключові кількісні показники**	**Аналітичний коментар**
Загальна масовість шкідливих програм для смартфонів	Переважно Android	2016-2018	2016 рік – близько 3,25 млн. нових зразків Android malware, у середньому приблизно 8 400 зразків на добу. 2017 рік – понад 3,0 млн. нових	Ці цифри показують, що з переходом на повноцінні смартфони екосистема Android стала основною ціллю для масового шкідливого

			зразків, у середньому близько 8 225 зразків на добу. 2018 рік – близько 3,2 млн. нових зразків до кінця третього кварталу, орієнтовно 11 700 на добу.	програмного забезпечення. Для кібербезпеки це означає необхідність постійного моніторингу маркетів застосунків, виявлення нових сімейств загроз та регулярного оновлення засобів захисту, оскільки кількість нових зразків зростає щоденно.
Отримання рут-прав на Android пристроях	Android	2010-ті роки і далі	Дослідження про rooted пристрої показують, що частка таких пристроїв у реальних вибірках сягає декількох десятих відсотка, при цьому сучасні дані вказують приблизно на 0,25 % rooted пристроїв серед активних Android девайсів.	Хоча відсоток пристроїв з рут-доступом відносно невеликий, саме ця група є суттєво більш уразливою. Рут-експлойти та інструменти на зразок Godless та інших наборів експлойтів дають змогу зловмиснику обійти модель дозволів Android, встановлювати приховані модулі, видаляти захисні застосунки та вбудовуватися на рівні системи, що суттєво ускладнює

				виявлення та видалення загрози.
Джейлбрейк та компрометація облікових записів	iOS (джейлбрейкнуті пристрої)	Близько 2014-2016 років	Кампанія KeyRaider призвела до компрометації понад 225 000 облікових записів Apple ID у 18 країнах; дослідники ідентифікували щонайменше 92 зразки цього сімейства шкідливого програмного забезпечення.	Уразливість була пов'язана не з офіційною екосистемою iOS, а саме з джейлбрейком та використанням неофіційних репозиторіїв. З погляду кібербезпеки це демонструє, що вихід за межі моделі безпеки виробника (джейлбрейк) радикально підвищує ризики – з'являються загрози крадіжки облікових даних, віддаленого блокування пристрою і вимагання викупу.
Рекламне програмне забезпечення як домінуючий клас загроз	Переважно Android	Приблизно з 2015-2020 років	За даними досліджень Avast Threat Labs, рекламне шкідливе програмне забезпечення становить близько 72 % усіх виявлених мобільних загроз, а його частка зросла приблизно на 38 % протягом одного року спостереження.	Попри те, що adware рідше безпосередньо шифрує дані або краде кошти, саме воно формує основний фон мобільної злочинності. Рекламні модулі масово вбудовуються у «безкоштовні» застосунки, збирають персональні

				дані, відображають нав'язливу рекламу, здійснюють приховані кліки та можуть слугувати початковим етапом для завантаження більш небезпечного шкідливого коду.
Шифрувальне програмне забезпечення для Android	Android	Початок з 2014 року, активний розвиток до кінця 2010-х років	Simplocker став одним з перших відомих файло-шифрувальних шкідливих застосунків для Android, відомих у диких умовах, який шифрував файли на SD-карті та вимагав викуп, часто в розмірі близько 300 доларів. Пізніше дослідження Android ransomware показали вибірку з 2 721 зразка, що охоплювали більшість відомих сімейств мобільного програмного забезпечення цього класу, серед яких значна частина займалася саме шифруванням файлів користувача.	Хоча загальна частка ransomware менша за частку рекламних загроз, очікувані збитки для користувачів значно вищі. Поєднання механізмів шифрування, елементів соціальної інженерії та платежів через електронні валюти дозволяє зловмисникам ефективно монетизувати атаки, тому навіть порівняно невелика кількість зразків створює суттєвий ризик для мобільної екосистеми.

Джерело: складено автором за даними [9; 13; 59].

Еволюції загроз у екосистемі Android у 2010-ті роки є кампанія HummingBad, яку дослідники Check Point виявили у 2016 році. Це шкідливе програмне забезпечення поєднувало автоматичне отримання Root доступу з масовим шахрайством у рекламних мережах. За результатами аналізу встановлено, що група зловмисників контролювала до 85 млн. Android пристроїв у всьому світі, а кількість реально інфікованих пристроїв оцінювалася щонайменше у 10 млн. Кампанія щодня встановлювала понад 50 тис. фальшивих застосунків та відображала близько 20 млн. рекламних оголошень, що забезпечувало зловмисникам орієнтовно 300 тис. доларів США щомісячного доходу від фіктивних кліків та інсталяцій.

Технічно HummingBad використовував набір експлойтів для ядра Android, які дозволяли отримати Root доступ без участі користувача. У випадках, коли експлуатація вразливості була успішною, шкідливий код закріплювався у системній області пам’яті, встановлював додаткові компоненти та забезпечував стійкий контроль над пристроєм, який не зникав навіть після перезавантаження. За даними Check Point зловмисники намагалися рутувати тисячі пристроїв щодня і досягали успіху у сотнях випадків, після чого могли безперешкодно встановлювати інші програми, деактивувати засоби захисту та приховувати свою присутність від користувача і антивірусних рішень.

Модель монетизації HummingBad ґрунтувалася на поєднанні механізмів Root доступу з рекламним шкідливим програмним забезпеченням. Контроль над мільйонами пристроїв дозволяв авторам кампанії примусово встановлювати додаткові застосунки, генерувати фіктивні кліки по рекламних оголошеннях та створювати штучний трафік для партнерських програм. При цьому легальний рекламно аналітичний бізнес, який вела та сама компанія, використовував спільну інфраструктуру відстеження і звітності з

HummingBad, що ускладнювало виявлення шахрайства на рівні рекламних мереж. Для кібербезпеки цей приклад є важливим тим, що демонструє, як масове рутування пристроїв перетворює окремі інфекції на повноцінний ботнет із потенційною можливістю виконувати не лише рекламні, а й цільові атаки на бізнес або державні організації, а також продавати доступ до інфікованих пристроїв іншим злочинним групам.

2.2. Ланцюги постачання та маркети застосунків: політики, цифрові підписи, альтернативні способи встановлення програм

Ланцюги постачання мобільних застосунків та політика маркетів сьогодні перетворилися на один з ключових елементів моделі загроз для інформаційної безпеки, тому аналіз безпеки смартфонів неможливо обмежити лише самою операційною системою або пристроєм. Екосистема включає розробника, платформи розповсюдження, сторонні бібліотеки та SDK, рекламні мережі, виробників пристроїв, мобільних операторів і, врешті, кінцевого користувача, який обирає джерело інсталяції програми. Кожна ланка такого ланцюга постачання може стати точкою компрометації, що особливо помітно на тлі стрімкого зростання мобільних атак, коли за даними Kaspersky у 2024 році було зафіксовано понад 33 млн. спроб атак на мобільні пристрої, у середньому близько 2,8 млн. інцидентів щомісяця [57].

У випадку Android центральним вузлом ланцюга постачання є Google Play, який поєднує функції каталогу застосунків, системи модерації та інфраструктури цифрових підписів. Кожен застосунок має бути підписаний криптографічним сертифікатом розробника, а перед публікацією проходить автоматизований та ручний перегляд на відповідність політикам Google Play щодо вмісту, доступу до даних та відсутності шкідливого коду [62, с. 37]. Для забезпечення масштабованого контролю Google використовує сервіс Google Play Protect, який за офіційними даними сканує сотні мільярдів екземплярів

програм щодня: у 2023 році йшлося про 125 млрд. перевірок на добу, а вже у 2024 році повідомлялося про понад 200 млрд щоденних сканувань і виявлення приблизно 13 млн. нових шкідливих застосунків за рік [65, с. 39]. Така багатошарова перевірка включає аналіз дозволів, статичний і поведінковий аналіз коду, порівняння з відомими шаблонами шкідливих сімейств і відстеження маніпуляцій із рекламними мережами.

Публічні дослідження при цьому показують суперечливу, але логічно узгоджену картину щодо того, де саме концентрується більшість шкідливих інсталяцій. З одного боку, емпіричне дослідження «How Did That Get In My Phone», виконане на великих вибірках реальних пристроїв, продемонструвало, що близько 67 % усіх інсталяцій шкідливих застосунків припадають саме на Google Play, тоді як сторонні маркети відповідають приблизно за 10 % таких інсталяцій [69, с. 338]. Причина полягає у масштабі офіційного магазину: за рахунок мільярдної аудиторії навіть невеликий відсоток шкідливих програм у загальному потоці приводить до домінування Play за абсолютною кількістю інфекцій. З іншого боку, аналіз Google за останні роки демонструє, що з погляду «щільності» загроз інтернет сайдлоадинг та неофіційні джерела виявляються набагато небезпечнішими. Оцінки компанії свідчать, що понад 95 % інсталяцій з основних сімейств шкідливих програм, пов’язаних з фінансовим шахрайством та зловживанням критичними дозволами, походять саме з інтернет сайдлоадингу, а рівень виявленого шкідливого коду у таких джерелах у більше ніж 50 разів вищий, ніж у випадку застосунків з Google Play [70, с. 6]. Таким чином, офіційний маркет генерує більшість інфекцій у абсолютних цифрах через масове використання, тоді як альтернативні джерела мають набагато вищий відсоток шкідливих програм серед доступних пакетів.

Альтернативні маркети застосунків та інші ланки ланцюга постачання, особливо у регіонах з обмеженим доступом до Google Play, створюють окремий клас ризиків. Дослідження китайських Android магазинів показали, що рівень виявленого шкідливого ПЗ у низці популярних сторонніх маркетів

може перевищувати показники Google Play більш ніж у 10 разів, а в окремих вибірках від 5 % до 13 % протестованих пакетів виявлялися підробленими, клонованими або відверто шкідливими [63, с. 572]. Ці результати підтверджують тезу про те, що відсутність централізованих та послідовно застосованих політик безпеки, а також слабший контроль цифрових підписів і відгуків користувачів створюють сприятливе середовище для розміщення троянів, шпигунського ПЗ, програм для клікфроду та фішингових оболонок. З погляду кібербезпеки організації, які дозволяють використання сторонніх магазинів на корпоративних пристроях, фактично розширюють свою поверхню атаки на цілий додатковий шар, де рівень базового захисту істотно нижчий.

На платформі iOS Apple намагається максимально «закрити» ланцюг постачання застосунків за рахунок централізованого контролю App Store, обов'язкового цифрового підпису і жорсткої процедури рев'ю. Усі програми мають бути підписані сертифікатом, виданим через Apple Developer Program, а перед публікацією проходять автоматизовані й ручні перевірки на відповідність детальним App Store Review Guidelines, які охоплюють вимоги до безпеки, конфіденційності, дизайну та правових аспектів [61]. За даними Apple, лише у 2020 році команда App Review відхилила понад 48 тис. застосунків через приховані або нед задекларовані можливості і понад 150 тис. програм як спам або вводячі користувачів в оману продукти, а загальний обсяг заблокованих підозрілих транзакцій у App Store перевищив 1,5 млрд. доларів США [45, с. 116]. У 2022 та 2023 роках компанія повідомляла вже про приблизно 1,7 млн. відхилених подань на рік і блокування шахрайських операцій на суму більше 2 і 7 млрд. доларів відповідно [27, с. 89]. Такі цифри демонструють, що App Store фактично виконує роль фільтра для всієї екосистеми, де значна частина загроз відсікається ще на рівні ланцюга постачання, до потрапляння шкідливого коду на пристрої користувачів.

Попри значний прогрес у формалізації політик, важливо розуміти, що надійність ланцюга постачання визначається не тільки джерелом інсталяції, а й чесністю та прозорістю самого розробника. Окремі дослідження Google Play Data Safety показали, що з майже 5 тис. проаналізованих застосунків приблизно 67,7 % мали невідповідність між реальною практикою збору даних, виявленою статичним аналізом коду, та інформацією, задекларованою у розділі «Безпека даних» на сторінці застосунку [8, с. 39]. Це означає, що навіть формально підписані та схвалені програми можуть використовувати трекінг, збирати і передавати персональні дані або метадані пристрою у набагато ширшому обсязі, ніж декларується користувачеві. З точки зору кібербезпеки це трансформує ланцюг постачання у багаторівневу проблему: необхідно контролювати не лише сам APK чи IPA пакет, а й інтегровані SDK, бібліотеки аналітики, рекламні модулі та механізми оновлень.

Характерним прикладом того, як уразливість на рівні ланцюга постачання може проявлятися навіть в офіційних маркетах, є масштабні рекламні шахрайські кампанії на кшталт SlopAds. У 2024 році дослідники виявили 224 шкідливі програми у Google Play, які загалом були завантажені понад 38 млн. разів і генерували до 2,3 млрд. рекламних запитів на добу [1, с. 127]. Формально ці застосунки проходили перевірку і мали цифрові підписи розробників, але вбудовані рекламні SDK використовували прихований клікфрод, агресивний трекінг та інші небажані дії. Цей кейс демонструє, що навіть за наявності політик і цифрових підписів маркет не може повністю виключити появу шкідливих або небажаних компонентів, особливо коли вони приховані у сторонніх бібліотеках, які встановлюються як залежності на етапі складання застосунку.

Окремої уваги заслуговують альтернативні способи встановлення програм поза офіційними маркетами, зокрема сайдлоадинг через веббраузер, месенджери, файлові менеджери, корпоративні каталоги або прямі посилання від продавців послуг. Аналітичні звіти фіксують численні випадки, коли сайд

завантажені застосунки містять приховані трояни, шпигунське ПЗ, модулі клікфроду та фішинговий код, що у разі інсталяції отримують доступ до конфіденційних даних, SMS, журналів викликів та вмісту екрана [4, с. 142-143]. Оскільки у таких сценаріях користувач часто вимикає стандартні обмеження на інсталяцію з невідомих джерел, рівень захисту суттєво знижується. Саме тому останні оновлення Android передбачають посилення контролю за Play Protect, включно із забороною відключати сканування під час телефонних та відеодзвінків, і додатковими попередженнями, якщо від користувача вимагають відключити перевірку для інсталяції застосунку.

З погляду кібербезпеки мобільних технологій ланцюги постачання та маркети застосунків виступають не лише каналами розповсюдження програм, а й ключовим полем боротьби між постачальниками платформ і зловмисниками. Централізовані маркети з цифровими підписами, політиками модерації та багатоетапним скануванням знижують відносну «щільність» шкідливого ПЗ, але через масштаб аудиторії залишаються критичним джерелом інфікувань [28]. Альтернативні джерела інсталяцій забезпечують зловмисникам високі ймовірності обходу контролю і часто стають точкою входу для найагресивніших сімейств троянів, шпигунського ПЗ та програм вимагачів. Це означає, що сучасні стратегії захисту мають включати як технічні засоби контролю ланцюга постачання, так і організаційні політики: заборону або жорстке обмеження сайдлоадингу на корпоративних пристроях, використання керованих магазинів, формування «білих списків» дозволених застосунків, а також регулярний аудит SDK і бібліотек, які використовуються розробниками у мобільних продуктах.

Таблиця 2.2 – Безпекові характеристики офіційних маркетів застосунків

Параметр	**Google Play (Android)**	**App Store (iOS)**	**Аналітичний коментар**
Масштаб та роль у	Основний глобальний канал постачання	Єдиний офіційний канал поширення більшості iOS	Обидва маркети є «вузловими точками» у ланцюгу постачання,

ланцюгу постачання	Android застосунків, понад мільярд активних пристроїв, сотні тисяч нових застосунків щороку.	застосунків, повністю контрольований Apple, прив'язаний до облікового запису Apple ID.	через які проходить більшість інсталяцій, тому будь який збій або помилка модерації впливає відразу на мільйони користувачів.
Механізми контролю та цифрові підписи	Кожен APK має бути підписаний сертифікатом розробника, увімкнено Play Protect, який щодня сканує сотні мільярдів застосунків, виявляючи мільйони нових зразків шкідливого ПЗ на рік.	Обов'язковий цифровий підпис через Apple Developer Program, жорсткий рев'ю, щороку відхиляється понад один мільйон подань, блокуються шахрайські транзакції на мільярди доларів.	Цифровий підпис і централізований рев'ю суттєво зменшують «щільність» шкідливих застосунків, але не гарантують нульового ризику, оскільки зловмисники можуть маскувати шкідливу поведінку під легітимну функціональність.
Частка шкідливих інсталяцій серед реальних інфекцій	Дослідження великих вибірок пристроїв показують, що близько двох третин усіх виявлених шкідливих інсталяцій походять саме з Google Play, решта припадає на сторонні маркети та сайдлоадинг.	Кількість класичних шкідливих програм нижча, основні ризики пов'язані з шахрайськими підписками, збиранням даних, зловживаннями in app покупками, а також з джейлбрейком і неофіційними репозиторіями.	Висока частка інфекцій через Google Play пояснюється не слабкістю захисту, а колосальним масштабом платформи, тоді як у відносних показниках «на один застосунок» офіційний маркет значно безпечніший за сторонні джерела.
Типові класи загроз	Рекламне шкідливе ПЗ, fleeceware з прихованими підписками, трояни, що маскуються під утиліти, ігри, VPN, програми оптимізації, шпигунські модулі у популярних застосунках.	Шахрайські застосунки з підписками, сірі схеми монетизації через in app покупки, програми, які збирають надмірні обсяги даних, маніпулюють рейтингами або копіюють відомі бренди.	Для захисту користувача недостатньо орієнтуватися лише на формальний факт походження з офіційного маркета, необхідно оцінювати модель дозволів, поведінку застосунку, наявність підозрілих SDK і схеми монетизації.

Наслідки для кібербезпеки	Особливу увагу потрібно приділяти виявленню масових шкідливих кампаній і швидкому видаленню небезпечних застосунків, оскільки навіть короткий час перебування у Google Play призводить до десятків мільйонів завантажень.	Фокус зміщується на контроль якості рев'ю, запобігання шахрайським фінансовим операціям та виявлення додатків, які приховано порушують політики конфіденційності, а також на контроль джейлбрейку на пристроях.	Безпека офіційних маркетів напряму впливає на загальний рівень ризиків у мобільній екосистемі, тому оператори платформ змушені інвестувати у аналіз ланцюга постачання, поведінкову аналітику та машинне навчання для виявлення аномалій.

Джерело: складено автором за даними [9; 13; 58].

Таблиця 2.3 – Альтернативні канали встановлення застосунків та пов'язані ризики

Канал або сценарій	**Типові характеристики ланцюга постачання**	**Кількісні показники ризику**	**Висновки для кібербезпеки**
Сторонні Android маркети	Незалежні магазини застосунків, часто регіональні або орієнтовані на окремих виробників пристроїв, слабший контроль цифрових підписів, менше формальних політик безпеки.	Дослідження показують, що частка шкідливих або клонованих пакетів у деяких популярних сторонніх маркетах може становити від приблизно 5 % до 13 %, що у кілька разів перевищує показники офіційного магазину.	Використання сторонніх маркетів різко підвищує ймовірність інфекції, особливо для троянів, шпигунського ПЗ та шкідливого рекламного програмного забезпечення, тому на корпоративних пристроях такий канал доцільно повністю блокувати.
Інтернет сайдлоадинг (завантаження	Користувач отримує APK файл напряму з	За оцінками постачальників платформ, понад	Сайдлоадинг є ключовим вектором для фінансових

APK з сайтів, месенджерів, файлообмінників)	вебсайту, посилання у повідомленні або хмарного сховища, вимикає стандартну заборону інсталяції з невідомих джерел і вручну підтверджує встановлення.	90 % інсталяцій найнебезпечніших сімейств мобільних шкідливих програм припадає саме на інтернет сайдлоадинг, а «щільність» шкідливого коду у таких джерелах у десятки разів вища, ніж у офіційних маркетах.	троянів, програм вимагачів та шпигунського ПЗ, тому політики безпеки мають або повністю забороняти такі інсталяції, або жорстко обмежувати їх «білими списками» перевірених внутрішніх застосунків.
Компрометовані ланцюги постачання у легітимних застосунках (вбудовані SDK, рекламні бібліотеки)	Розробник інтегрує сторонні SDK для реклами, аналітики або монетизації, при цьому сам пакет є підписаним і проходить модерацію, але вбудований модуль реалізує приховану шкідливу поведінку.	В окремих виявлених кампаніях у Google Play було знайдено понад двісті шкідливих застосунків із загальною кількістю завантажень понад тридцять мільйонів, які генерували мільярди рекламних запитів на добу та приховані кліки.	Навіть офіційні маркети не захищають від ризиків, пов’язаних з вбудованими бібліотеками, тому аналіз безпеки має охоплювати весь ланцюг постачання, включно з третьосторонніми компонентами, а не лише код основного застосунку.
Корпоративні каталоги та інхаус розповсюдження	Організація самостійно підписує та поширює застосунки через MDM системи або внутрішні каталоги, інсталяція часто дозволена лише на корпоративних пристроях.	Прямих публічних відсотків шкідливих інсталяцій немає, проте інциденти часто пов’язані з використанням вразливих бібліотек, неправильними налаштуваннями сертифікатів і відсутністю незалежного безпекового аудиту.	Для корпоративного середовища внутрішній каталог може бути максимально безпечним каналом за умови наявності формалізованого процесу рев’ю, регулярного сканування коду і контролю за оновленнями SDK, інакше він перетворюється на додаткову точку входу для атак.
Джейлбрейк та установка з неофіційних репозиторіїв на iOS	Після джейлбрейку користувач отримує доступ до альтернативних репозиторіїв, де	В окремих інцидентах через неофіційні репозиторії було скомпрометовано	Порушення штатного ланцюга постачання iOS через джейлбрейк фактично знімає

	відсутній централізований рев'ю і програми можуть не мати коректного цифрового підпису або взагалі використовувати самопідписані сертифікати.	сотні тисяч облікових записів Apple ID, що супроводжувалося крадіжкою платежів, історії покупок та іншої конфіденційної інформації.	більшість вбудованих захистів, тому з точки зору кібербезпеки такі пристрої потрібно вважати високоризиковими і обмежувати їх доступ до корпоративних ресурсів.

Джерело: складено автором за даними [9; 13; 58].

Вразливості ланцюга постачання та політик маркета є інцидент з XcodeGhost, який у 2015 році став першим масовим компрометуванням App Store. Суть атаки полягала не в безпосередньому завантаженні шкідливих застосунків у магазин, а в підміні інструменту розробника. Частина китайських iOS розробників замість офіційного Xcode завантажувала його «швидкі» копії з локальних файлообмінників, де зловмисники розмістили модифікований інсталятор. У зараженій версії Xcode було змінено одну з системних бібліотек, через що при компіляції будь якого застосунку в нього автоматично вбудовувався шкідливий модуль, навіть якщо сам розробник про це не знав [15, с. 121]. Таким чином атакувалася саме проміжна ланка ланцюга постачання інструмент компіляції, а не фінальний застосунок.

У результаті через офіційний App Store було опубліковано десятки, а за деякими оцінками навіть тисячі заражених програм. Початкові звіти Palo Alto Networks та Malwarebytes вказували щонайменше 39 % інфікованих застосунків, які вже пройшли рев'ю та були доступні для завантаження, серед них популярний месенджер WeChat, сканер документів CamScanner, музичний сервіс NetEase Cloud Music та інші масові продукти. Подальший аналіз FireEye показав, що загальна кількість скомпрометованих застосунків могла перевищувати 4 тис., а масштаби інфекції сягали сотень мільйонів користувачів, насамперед у Китаї та країнах Азійсько Тихоокеанського регіону.

Саме тому інцидент був охарактеризований як перша велика атака на App Store, коли значний обсяг шкідливого програмного забезпечення пройшов офіційну модерацію і поширювався через повністю довірений канал [11, с. 8].

Поводження XcodeGhost на пристрої користувача добре демонструє, чому класичні політики й цифрові підписи не завжди достатні для захисту ланцюга постачання. Вбудований модуль збирав і передавав на командно контрольні сервери ідентифікатори пристрою, версії операційної системи, назви встановлених застосунків, мовні та регіональні налаштування, а в окремих версіях дозволяв відкривати довільні URL та показувати фішингові вікна для викрадення облікових даних. Усі інфіковані програми були підписані коректними сертифікатами легітимних розробників і виглядали цілком нормальними з погляду App Store, оскільки шкідливий код потрапив у них ще на етапі компіляції [10, с. 28]. З точки зору кібербезпеки це показує, що цифровий підпис гарантує лише походження та цілісність пакета, але не його «чистоту», а ланцюг постачання включає не тільки маркет і користувача, а й усі проміжні інструменти розробки, SDK та бібліотеки, які мають бути предметом окремого контролю та аудиту.

2.3. Захисні механізми платформ та їх обхід: ізоляція процесів, система дозволів, політики керування мобільними пристроями

У сучасних мобільних операційних системах захисні механізми платформ формуються як багаторівнева система, де ізоляція процесів, модель дозволів і політики керування мобільними пристроями разом мають стримувати шкідливу активність і мінімізувати наслідки компрометації. На практиці це означає, що кожен застосунок виконується в окремому ізольованому середовищі, доступ до апаратних ресурсів та конфіденційних даних суворо регламентується системою дозволів, а в корпоративних сценаріях додатково застосовуються засоби мобільного керування для

посилення контролю та відповідності вимогам безпеки. Попри це, статистика інцидентів свідчить, що зловмисники систематично шукають способи обійти ці механізми через привілейовані API, вразливості попередньо встановлених застосунків, помилки конфігурації MDM рішень та соціальну інженерію, що створює нову динамічну конфігурацію ризиків для інформаційної безпеки мобільних технологій.

Ізоляція процесів у Android реалізується через застосункову пісочницю, де кожному застосунку призначається унікальний ідентифікатор користувача ядра Linux, а взаємодія між процесами обмежується стандартними механізмами операційної системи. За замовчуванням застосунки не мають доступу до пам’яті один одного і не можуть взаємодіяти з компонентами системи, які не були явно відкриті через механізми міжпроцесної комунікації, зокрема служби, широкомовні повідомлення, контент провайдери та інші інтерфейси. Офіційна документація Android прямо підкреслює, що пісочниця реалізована на рівні ядра і є базовим механізмом запобігання несанкціонованого доступу до даних та ресурсів пристрою, причому будь який вихід за її межі можливий лише за умови надання відповідних дозволів або експлуатації вразливостей ядра [5, с. 407]. Аналіз сучасних досліджень підтверджує, що пісочниця залишається достатньо ефективним бар’єром проти прямого доступу шкідливих програм до системних ресурсів, однак її реальний рівень захисту значною мірою визначається тим, наскільки суворо контролюється система дозволів та як обмежується доступ до спільно використовуваних сховищ і привілейованих API [6, с. 104].

Архітектура безпеки iOS також базується на ізоляції процесів, однак реалізована в рамках більш закритої моделі. Усі застосунки виконуються в окремих пісочницях, підписуються цифровим підписом, а їхні можливості визначаються системою повноважень, яка використовує поняття entitlements для доступу до окремих сервісів, приміром до push повідомлень, Keychain або апаратних функцій. Керівництво Apple з безпеки підкреслює, що шкідливий

код не може модифікувати інші застосунки без порушення цифрового підпису, оскільки будь яка зміна коду веде до невідповідності підпису і блокування запуску [43, с. 146]. Державні рекомендації, зокрема британські настанови з розробки безпечних застосунків для iOS, прямо відносять пісочницю, підпис коду і політику маркета до ключових гарантій захисту корпоративної інформації на мобільних пристроях [47]. Разом з тим практика джейлбрейку показує, що навмисне зняття цих обмежень призводить до різкого підвищення ризику зараження, оскільки пристрій втрачає значну частину вбудованих механізмів контролю, а дослідження фіксують зростання ймовірності віддаленої експлуатації та крадіжки даних на джейлбрейкованих пристроях порівняно зі стандартними конфігураціями.

Система дозволів у Android за останнє десятиліття пройшла помітну еволюцію. Починаючи з Android 6 модель орієнтується на надання доступу до «небезпечних» ресурсів, таких як камера, мікрофон, геолокація, контакти або SMS, безпосередньо під час використання застосунку, а не лише на етапі інсталяції. Офіційні рекомендації Google та спеціалізовані огляди з безпеки підкреслюють, що застосунки мають декларувати мінімально необхідний набір дозволів і запитувати їх саме тоді, коли це потрібно для функціонування, що дозволяє користувачу свідомо контролювати доступ [51, с. 134]. Паралельно з цим з’являються спеціальні типи доступу, наприклад сервіс доступності, право накладання поверх інших вікон, доступ до оптимізації батареї, права на адміністрування пристрою, які дають застосункам значно ширші можливості, ніж звичайні дозволи. Аналітика MITRE ATT and CK for Mobile прямо вказує на зловживання цими привілеями як на поширену техніку, що використовується зловмисниками для обходу стандартної моделі дозволів, маскування власної активності та отримання контролю над інтерфейсом пристрою [52, с. 23].

Реальні кейси демонструють, що саме зловживання привілейованими дозволами часто стає ключем до обходу захисних механізмів платформ.

Дослідження шкідливих програм, які використовують Accessibility Service Android, показали, що такі програми можуть фактично обходити модель дозволів і ізоляції за рахунок перехоплення вмісту екрана, автоматизації натискань, підтвердження системних діалогів та заповнення форм без участі користувача [60, с. 371]. У 2025 році повідомлялося про хвилю нових загроз, які використовують доступність, OEM дозволи та вразливості попередньо встановлених застосунків для привілейованого виконання дій на мільйонах пристроїв, включаючи зміну налаштувань безпеки, встановлення додаткових модулів і приховані операції з фінансовими застосунками.

Додатковим прикладом того, як інтерфейс і система дозволів можуть бути обійдені на логічному рівні, є атака TapTrap, описана у 2025 році командою дослідників з TU Wien та Університету Байройта. Атака базується на прийомі tapjacking і використовує маніпуляцію анімаціями переходу між активностями для накладання невидимих шкідливих екранів поверх легітимного інтерфейсу. У ході експериментів було проаналізовано майже 100 тис застосунків Play Store, причому близько 76 % виявилися потенційно вразливими через особливості опрацювання подій інтерфейсу, що дозволяло змусити користувача натиснути «дозволити» або «авторизувати» на прихованих системних діалогах [32, с. 113]. Хоча TapTrap поки що є дослідницьким прототипом, він наочно демонструє, що навіть за наявності формального діалогу з користувачем модель дозволів може бути обійдена через приховану маніпуляцію інтерфейсом, яка змінює відповідність між тим, що користувач бачить на екрані, і тим, який саме елемент інтерфейсу отримує натискання.

У середовищі iOS система дозволів менше орієнтується на розділення доступу між численними небезпечними категоріями, натомість ключовими механізмами залишаються підпис коду, sandbox та entitlements. Доступ до, наприклад, геолокації або контактів також потребує згоди користувача, але критичні можливості, такі як виконання довільного коду, використання

недокументованих API або звернення до спеціальних корпоративних функцій, контролюються саме з боку підпису та entitlements, які видаються в рамках Apple Developer Program і, за потреби, додаткових корпоративних програм. Аналітика з безпеки iOS вказує, що значна частка відомих шкідливих програм для цієї платформи або орієнтувалася на джейлбрейковані пристрої, або використовувала легальні механізми корпоративного розповсюдження, які за умов неправильної конфігурації дозволяли запуск застосунків поза App Store [56, с. 59]. Це підкреслює, що модель дозволів ефективна лише разом з жорстким контролем підпису та джерел інсталяції, і саме порушення цих елементів ланцюга постачання відкриває шлях для атак.

Важливим захисним шаром у сучасних мобільних екосистемах виступають політики керування мобільними пристроями, які реалізуються через рішення класу MDM. Такі системи дозволяють адміністраторам організацій централізовано розгортати налаштування безпеки, обмежувати встановлення застосунків, примусово вмикати шифрування, вимагати складні паролі, виконувати віддалене блокування та стирання даних, а також сегментувати корпоративну й особисту інформацію. Попит на MDM стрімко зростає: за різними оцінками, глобальний ринок мобільного керування у 2024 році оцінювався від приблизно 7,8 до 13,3 млрд. доларів США, а прогнози до 2033-2034 років передбачають зростання обсягів до 68-90 млрд доларів при середньорічних темпах близько 22-26 % [40, с. 107]. Така динаміка відображає зростання ролі мобільних пристроїв у корпоративних процесах і усвідомлення того, що стандартних платформних механізмів захисту недостатньо для виконання вимог регуляторів та внутрішніх політик.

Пристрої на базі iOS нативно інтегрують механізми MDM через конфігураційні профілі, шифрований канал взаємодії з MDM сервером і використання Apple Push Notification Service виключно як тригер для ініціації захищеної сесії з сервером керування. Офіційний гід з безпеки Apple описує MDM як ключовий інструмент для масштабного розгортання iPhone і iPad в

організаціях, який дозволяє застосовувати політики шифрування, обмежувати перелік дозволених застосунків, примусово встановлювати VPN та інші засоби захисту [68, с. 124]. Аналітичні огляди ринку підтверджують, що попит на керування пристроями Apple зростає разом з проникненням цих пристроїв у корпоративне середовище, причому вартість сегмента керування екосистемою Apple зростає синхронно з загальним ринком MDM.

Водночас історія розвитку MDM доводить, що самі по собі системи керування можуть ставати ціллю атак і точкою обходу платформних механізмів. Класичний приклад продемонструвала командна доповідь на конференції Black Hat Asia, де було описано вразливість у реалізації MDM для iOS, яка дозволяла організувати атаку «людина посередині» між керованим пристроєм і сервером MDM, підмінити команду встановлення та непомітно інсталювати шкідливий застосунок під виглядом корпоративного [67, с. 319]. У такому сценарії саме довіра до MDM як до привілейованого каналу оновлення, який має право встановлювати будь які пакети без взаємодії з користувачем, перетворюється на механізм обходу обмежень App Store, sandbox та системи дозволів. Подібні інциденти показують, що ефективність політик керування мобільними пристроями критично залежить від захищеності серверної інфраструктури, коректної реалізації криптографічних протоколів та належного аудиту сторонніх MDM рішень.

У підсумку можна зробити висновок, що ізоляція процесів, система дозволів та політики керування мобільними пристроями формують три ключові «лінії оборони» в архітектурі мобільної кібербезпеки. Пісочниця та підпис коду обмежують довільний доступ до ресурсів на рівні операційної системи, модель дозволів забезпечує контрольований доступ до конфіденційних даних за участю користувача, а MDM рішеня додають надбудову політик, орієнтованих на організаційні потреби та відповідність нормативним вимогам. Водночас реальна картина загроз свідчить, що кожен із цих механізмів має свої точки обходу, починаючи від зловживання сервісами

доступності, накладанням інтерфейсів і привілейованими OEM дозволами і закінчуючи помилками в конфігурації MDM та компрометацією інструментів розробки. Це означає, що для забезпечення високого рівня інформаційної безпеки у мобільних технологіях необхідно розглядати захисні механізми платформ не ізольовано, а як частину єдиної багаторівневої системи, яка включає технічні засоби, політики управління, безпековий аудит ланцюга постачання і підвищення обізнаності користувачів щодо ризиків, пов'язаних з наданням розширених дозволів і використанням неавторизованих каналів інсталяції програм.

Таблиця 2.4 – Основні захисні механізми мобільних платформ

Механізм	**Реалізація в Android**	**Реалізація в iOS**	**Кількісні дані / ефект**	**Аналітичний висновок**
Ізоляція процесів (пісочниця)	Кожен застосунок виконується під окремим UID ядра Linux, має власний каталог даних, не може напряму читати файли інших застосунків. Взаємодія відбувається лише через чітко визначені IPC механізми (служби, broadcast, content provider).	Кожен застосунок працює у власній sandbox, доступ до файлової системи та системних сервісів жорстко обмежений. Будь яка модифікація коду порушує цифровий підпис і блокує запуск.	За результатами аналізу уразливостей більшість мобільних шкідливих програм не може безпосередньо виходити за межі пісочниці без експлуатації вразливостей ядра або механізмів міжпроцесної взаємодії. Частка експлойтів, які реально обходять sandbox, у загальній масі мобільного шкідливого ПЗ є відносно невеликою.	Пісочниця ефективно локалізує більшість інцидентів, але не захищає від атак, що використовують дозволені канали взаємодії (наприклад, зловживання службами доступності) або вразливості на рівні ядра й драйверів.

Система дозволів для доступу до ресурсів	Починаючи з Android 6 запит небезпечних дозволів (камера, мікрофон, геолокація, контакти, SMS) відбувається під час роботи, а не лише при інсталяції. Додаткові «особливі» дозволи, наприклад Overlay, Accessibility, Device Admin, дають розширені можливості контролю над системою.	Доступ до геолокації, контактів, медіа, мікрофона та інших чутливих даних надається користувачем через системні діалоги. Критичні повноваження, такі як доступ до Keychain або спеціальних системних сервісів, контролюються entitlements, що прив'язані до сертифіката розробника.	Статичний аналіз великих вибірок застосунків показує, що значна частина програм запитує надлишкові дозволи. У дослідженнях виявляли до 60-70 % застосунків, у яких набір фактично використаних дозволів менший, ніж задекларований, що створює потенціал для зловживань у разі компрометації.	Модель дозволів ефективна лише тоді, коли застосунки дотримуються принципу мінімально необхідних привілеїв і коли користувачі розуміють значення запитуваних доступів. Надлишкові дозволи перетворюють будь який скомпрометований застосунок на потенційний інструмент масштабної атаки.
Підпис коду та цілісність застосункі в	Усі APK мають бути підписані сертифікато м розробника. Оновлення допускаютьс я лише за умови збігу підпису. Це дозволяє виявляти підміну пакета та обмежує можливість «тихої» модифікації застосунку	Обов'язковий підпис коду через Apple Developer Program. Будь які зміни в бінарному файлі роблять підпис недійсним. Для корпоративного розповсюдженн я використовуєть ся окремий тип сертифікатів і профілів.	Масові інциденти на зразок XcodeGhost показали, що навіть за умови коректного підпису застосунку шкідливий код може потрапити в нього на етапі компіляції, якщо компрометован і інструменти розробника. Відомі кампанії зловживань корпоративним	Підпис коду забезпечує цілісність пакета, але не гарантує «чистоту» його вмісту. Захист ланцюга постачання має включати контроль інструментів збірки, SDK, рекламних бібліотек і процедури видачі сертифікатів, інакше цифровий підпис може захищати вже скомпрометований продукт.

	стороннім суб'єктом.		и сертифікатами для обходу App Store.	
Політики керування мобільними пристроями (MDM)	Android підтримує різні моделі керування: Device Owner, Profile Owner, Work Profile. Через MDM можна нав'язувати політики шифрування, парольні політики, обмеження інсталяції, «білі списки» застосунків, розмежування робочого та особистого профілів.	iOS використовує конфігураційні профілі та MDM сервери для централізованого керування налаштуваннями безпеки, установлення захищених застосунків, примусового ввімкнення шифрування, VPN, обмежень на використання камер, AirDrop, хмарних сервісів.	Глобальний ринок MDM у 2024 році оцінюється у діапазоні від приблизно 8 до 13 млрд доларів США з прогнозованим зростанням до 60-90 млрд. доларів упродовж наступного десятиліття. Це відображає масове впровадження мобільних пристроїв у корпоративні процеси та зростання залежності від MDM як «надбудови» над платформними механізмами.	MDM дозволяє суттєво посилити стандартні механізми безпеки, але сам стає високопривілейованою ланкою. Якщо MDM сервер або політики скомпрометовані, зловмисник отримує можливість обходити App Store, систему дозволів і sandbox, встановлюючи будь який код на тисячі пристроїв.
Оновлення безпеки платформи	Регулярні патчі Android від Google, а також оновлення від виробників пристроїв. Фрагментація екосистеми призводить до того, що значний відсоток користувачів тривалий час	Apple централізовано поширює оновлення iOS. Частка пристроїв на актуальних версіях суттєво вища. Наприклад, у окремі роки понад 70 % активних пристроїв оновлювалися до останньої версії протягом	Різниця у швидкості та охопленні оновлень призводить до того, що вразливості Android залишаються експлуатованими роками на великій кількості пристроїв, тоді як у iOS вік активної експлуатації	Ефективність захисних механізмів напряму залежить від своєчасності оновлень. Для Android організації вимушені додатково контролювати парк пристроїв, обмежувати використання застарілих версій та компенсувати ризики за рахунок MDM і мережевих засобів захисту.

	залишається на застарілих версіях без актуальних патчів.	перших місяців після релізу.	критичних вразливостей часто коротший через швидке закриття.	

Джерело: складено автором за даними [9; 13; 58].

Таблиця 2.5 – Типові способи обходу захисних механізмів мобільних платформ

Захисний механізм, який обходять	**Техніка або реальний приклад атаки**	**Ключові кількісні показники**	**Наслідки для кібербезпеки**
Модель дозволів і контроль інтерфейсу (Android)	Атаки типу tapjacking і TapTrap, коли шкідливий застосунок накладає приховані елементи поверх легітимного інтерфейсу або маніпулює анімаціями переходу, змушуючи користувача натиснути «Дозволити» або «Надати доступ» на невидимому системному діалозі.	У дослідженні TapTrap було проаналізовано близько 100 тис застосунків із Google Play і виявлено, що приблизно 76 % з них потенційно вразливі до цієї техніки через специфіку обробки подій інтерфейсу.	Навіть якщо система формально показує діалог із запитом дозволу, користувач може не усвідомлювати, на що саме погоджується. Це підриває модель «усвідомленої згоди» та дозволяє зловмисникам отримувати доступ до контактів, повідомлень, файлів і функцій керування пристроєм, обходячи очікувану поведінку моделі дозволів.
Пісочниця та система дозволів (Android)	Зловживання сервісами доступності: шкідливі застосунки отримують доступ до Accessibility Service, після чого можуть читати	Аналіз сімейств шкідливих програм показав, що десятки мобільних троянів для банкінгу та програм вимагачів використовують Accessibility для автоматизації	Використання служб доступності дозволяє шкідливому ПЗ фактично «стояти над» усім інтерфейсом, що знімає обмеження, задані пісочницею,

	вміст екрана, натискати кнопки, підтверджувати інсталяцію інших застосунків, обходити захист банківських програм і механізми двофакторної автентифікації.	натискань і обходу захисних діалогів. У вибірках «банківського» шкідливого ПЗ частка зразків, що зловживають Accessibility, сягає десятків відсотків.	і дає можливість взаємодіяти з іншими застосунками так, ніби це робить сам користувач. Це робить такі трояни особливо небезпечними для фінансових сервісів і систем автентифікації.
Sandbox і підпис коду (Android та iOS)	Рутування пристрою та джейлбрейк. На Android шкідливі програми інтегрують експлойти ядра для отримання Root прав, на iOS користувачі свідомо знімають обмеження, встановлюючи джейлбрейк і відкриваючи доступ до неофіційних репозиторіїв.	Частка рутованих або джейлбрейкованих пристроїв у глобальному парку відносно невелика (десяті частки відсотка), але дослідження показують, що ймовірність інфекції та віддаленої експлуатації для них у рази або навіть на порядки вища, ніж для «чистих» пристроїв.	Root або джейлбрейк фактично відключають частину базових механізмів безпеки. У корпоративному середовищі такі пристрої мають розглядатися як високоризикові, їх підключення до внутрішніх ресурсів слід жорстко обмежувати або забороняти, а в політиках MDM передбачати автоматичну блокування при виявленні.
Ланцюг постачання та підпис коду (iOS)	Інцидент XcodeGhost: зловмисники модифікували інструмент Xcode, який використовували розробники в Китаї. Заражені копії Xcode автоматично вбудовували шкідливий модуль у всі скомпільовані застосунки, після чого ці програми	За різними оцінками було скомпрометовано щонайменше десятки, а можливо і понад 4 тис. застосунків, які сумарно мали сотні мільйонів завантажень. Популярні програми, як WeChat і інші масові сервіси, стали каналом для збору даних і потенційних фішингових дій.	Цей випадок показав, що підпис коду і рев'ю маркета не захищають від атак на проміжні елементи ланцюга постачання. Для захисту необхідно контролювати інструменти збірки, SDK та середовища розробки, а також мати механізми виявлення

	підписувалися легітимними сертифікатами та публікувалися в App Store.		аномальної поведінки вже після публікації застосунків.
Політики MDM і довірені канали встановлення	Демонстрація атак «людина посередині» на MDM для iOS. У разі вразливості в реалізації MDM або неправильного налаштування сертифікатів атакуючий може підмінити команду встановлення та розгорнути шкідливий застосунок під виглядом корпоративного, який отримує розширені дозволи без відображення попереджень користувачу.	Окремі дослідження на профільних конференціях показали можливість компрометації цілих парків пристроїв, підключених до одного MDM, при експлуатації однієї критичної вразливості. За умов великої організації це можуть бути тисячі пристроїв, які отримують шкідливий код централізовано.	MDM дає змогу обійти обмеження App Store, sandbox і модель дозволів, оскільки довірений сервер має право встановлювати застосунки і змінювати налаштування без участі користувача. Тому MDM інфраструктура повинна бути захищена не менш суворо, ніж інші критичні компоненти (сервери автентифікації, шлюзи доступу, платіжні системи).
Обмеження інсталяцій із невідомих джерел (Android)	Масове поширення шкідливих APK через сайдлоадинг. Користувач свідомо вимикає обмеження на інсталяції з невідомих джерел, отримуючи файл через браузер, месенджер або файлообмінник. У результаті модель «тільки довірені маркети» перестає діяти.	За оцінками постачальників платформ, понад 90 % інсталяцій найбільш небезпечних мобільних шкідливих програм (банківські трояни, програми-вимагачі, шпигунське ПЗ) припадає саме на інтернет сайдлоадинг, при цьому «щільність» шкідливого ПЗ у таких джерелах у десятки разів вища, ніж у офіційному магазині.	

Джерело: складено автором за даними [9; 12; 13; 58].

Вразливості ланцюга постачання та політик маркету є багаторічна кампанія шкідливих застосунків сімейства Joker, яку також позначали назвою Bread. Ці програми спеціалізувалися на прихованих платних підписках і маскувалися під легітимні утиліти, фоторедактори, офісні інструменти або додатки для обміну повідомленнями. Починаючи приблизно з дві тисячі сімнадцятого року дослідники неодноразово фіксували хвилі виявлення нових модифікацій, у межах яких з Google Play вилучали сотні і навіть понад тисячу шкідливих застосунків. Формально вони відповідали вимогам політик, були підписані сертифікатами реальних розробників і певний час безперешкодно проходили модерацію. Усередині пакета при цьому містилися модулі, здатні довантажувати додатковий код з віддалених серверів, приховано взаємодіяти з білінговими сервісами мобільних операторів, підписувати користувача на преміум послуги через платні повідомлення або мобільні підписки і підтверджувати ці операції без явної згоди власника пристрою. У деяких кампаніях кількість заражених користувачів сягала сотень тисяч, а сукупні збитки формувалися за рахунок невеликого, але регулярного списання коштів з багатьох облікових записів.

Важливо, що Joker активно використовував як офіційний маркет, так і альтернативні канали встановлення програм. Частина зразків поширювалася у вигляді окремих файлів для ручного встановлення, які користувачі отримували через сайти, месенджери і файлообмінники після вимкнення стандартної заборони на інсталяцію з невідомих джерел. Інша частина потрапляла у Google Play вже у вигляді відносно «чистих» версій, які виконували базові функції і не викликали підозр на етапі перевірки. Після накопичення певної кількості встановлень розробники через оновлення або приховане довантаження компонентів активували шкідливу логіку, і застосунок починав автоматично оформлювати підписки, перехоплювати підтверджувальні повідомлення і

приховувати від користувача фактичні фінансові операції. З точки зору кібербезпеки цей приклад добре демонструє, що сам факт цифрового підпису і розміщення в офіційному маркеті не гарантує безпечності ланцюга постачання, а політики магазинів, механізми модерації та системи виявлення аномальної поведінки мають постійно адаптуватися до нових сценаріїв зловживання, які поєднують офіційні і неофіційні канали розповсюдження.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі було показано, що перехід до епохи повнофункціональних смартфонів у дві тисячі десяті роки радикально змінив картину загроз інформаційної безпеки. Мобільні пристрої перетворилися з інструментів для голосового зв’язку і простих повідомлень на універсальні платформи доступу до банківських послуг, електронної комерції, соціальних мереж і корпоративних ресурсів. Це призвело до того, що шкідливе програмне забезпечення еволюціонувало від порівняно примітивних вірусів і троянів до масових кампаній рекламного шкідливого програмного забезпечення, програм вимагачів і фінансових троянів, орієнтованих на монетизацію даних і транзакцій. Екосистема Android стала основною ціллю через домінування на ринку і відкритість моделі поширення застосунків, тоді як для iOS головні ризики змістилися у площину джейлбрейку та зловживання корпоративними механізмами розповсюдження.

Окремо розділ засвідчив, що ланцюги постачання та маркети застосунків виконують подвійну роль для кібербезпеки. З одного боку, офіційні магазини Android і iOS із цифровими підписами, механізмами модерації та автоматизованим скануванням істотно знижують відносну частку шкідливого програмного забезпечення у загальному потоці програмних пакетів. З іншого боку, саме через ці маркети завдяки їхньому масштабу поширюються кампанії, де окремі шкідливі або небажані застосунки отримують мільйони завантажень,

перш ніж будуть виявлені та видалені. Ще більш ризиковими виявилися сторонні маркети і сценарії інтернет сайдлоадингу, де частка шкідливих або клонированих пакетів у рази вища, ніж в офіційних магазинах, що робить такі канали ключовими точками входу для фінансових троянів, шпигунського програмного забезпечення і програм вимагачів. Аналіз інцидентів на кшталт компрометації інструментів розробки або вбудованих рекламних бібліотек показав, що ланцюг постачання включає не тільки маркет і користувача, а й компілятори, SDK, рекламні модулі та білінгову інфраструктуру, кожна з яких може бути використана як точка атаки.

Дослідження захисних механізмів платформ продемонструвало, що технології пісочниці, системи дозволів, підпису коду і політик керування мобільними пристроями створюють багаторівневу архітектуру оборони, але самі по собі не є абсолютною гарантією безпеки. Ізоляція процесів ефективно обмежує прямий доступ шкідливих програм до даних інших застосунків, однак зловмисники активно використовують легальні канали взаємодії між процесами, служби доступності, накладання інтерфейсів і логічні помилки в обробці подій для обходу очікуваних обмежень. Модель дозволів покликана забезпечувати усвідомлену згоду користувача, проте на практиці частина застосунків запитує надлишкові привілеї, а користувачі часто підтверджують запити автоматично, що перетворює будь який компрометований застосунок із широкими правами на потужний інструмент атаки. MDM рішення дозволяють організаціям централізовано посилювати політики шифрування, контролю доступу і розмежування корпоративних та особистих даних, але водночас у випадку вразливостей або помилкових налаштувань вони можуть стати каналом масштабного розгортання шкідливого програмного забезпечення одразу на багатьох пристроях.

Узагальнюючи результати другого розділу, можна ствердити, що в епоху смартфонів кібербезпека мобільних технологій визначається не окремим механізмом, а взаємодією екосистеми платформ, маркетів, ланцюгів

постачання і користувацької поведінки. Еволюція загроз від ранніх вірусів і троянів до складних багатокомпонентних кампаній обумовлена як зростанням цінності даних на мобільних пристроях, так і появою нових можливостей для зловживання вбудованими сервісами і бізнес моделями мобільних застосунків. Для ефективної протидії необхідна комплексна стратегія, що поєднує вдосконалення платформних механізмів безпеки, жорсткий контроль ланцюгів постачання, обмеження альтернативних каналів встановлення програм, впровадження зрілих політик MDM у корпоративному середовищі та підвищення обізнаності користувачів щодо ризиків надання розширених дозволів і використання неофіційних джерел програмного забезпечення. Саме на такій основі можливе подальше формування ефективних моделей захисту в умовах постійної еволюції загроз, що буде розвинуто у наступному розділі магістерської роботи.

РОЗДІЛ 3
СУЧАСНИЙ ЕТАП 2020-ТІ РОКИ ТЕХНОЛОГІЯ 5G МОБІЛЬНІ ПЛАТЕЖІ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА КОМПЛЕКСНІ АТАКИ

3.1. Технологія 5G та edge-обчислення як фактор розширення площини атак: мережевий рівень, кінцеві пристрої, Інтернет речей

На початок 2024 року кількість 5G підписок у світі вже перевищила приблизно 2,1 млрд., а до 2030 року прогнозовано зросте до близько 6,3-6,4 млрд., що становитиме майже 60-67 % усіх мобільних підписок. Одночасно 5G мережі, за оцінками галузевих звітів, до кінця 2030 року будуть переносити до 80 % світового мобільного трафіку даних, тоді як у 2024 році на них припадає приблизно третина [40, с. 162-163]. Це означає, що будь-які архітектурні вразливості, помилки конфігурації або компрометація елементів 5G інфраструктури матимуть системний характер, впливаючи на мільярди користувачів і критично важливі сервіси, включаючи мобільні платежі, дистанційне керування виробництвом, транспортними системами та енергетичними об’єктами.

Еволюція мобільних загроз безпосередньо відображається на повсякденній діяльності підрозділів Національної гвардії України. Використання сучасних мобільних мереж (4G/5G), месенджерів, хмарних сервісів і платіжних застосунків створює додаткові канали для витоку службової інформації та персональних даних військовослужбовців. Для НГУ це означає, що навіть побутове застосування смартфонів поза виконанням бойових завдань може ставати об’єктом уваги противника, який здатен відстежувати маршрути пересування, місця збору особового складу, контакти командирів та структуру управління [33, с. 591].

Загрози, пов’язані зі шпигунським програмним забезпеченням, фішинговими атаками через популярні месенджери, компрометацією

мобільних платіжних сервісів або підробленими базовими станціями, набувають особливої ваги для НГУ, оскільки спрямовані на розкриття тактичної та оперативної інформації [33, с. 592]. Це вимагає запровадження на практиці принципів Zero Trust, жорсткішої регламентації використання особистих мобільних пристроїв у підрозділах, сегментування службових і цивільних каналів зв'язку, а також постійного моніторингу дотримання вимог інформаційної безпеки.

Ключовою особливістю 5G є перехід від переважно апаратної до віртуалізованої мережевої інфраструктури, що базується на програмно визначених мережах, віртуалізації мережевих функцій та технології network slicing. На практиці це означає, що більшість функцій комутації, маршрутизації, шифрування й керування трафіком реалізуються у вигляді програмних компонентів, розгорнутих на стандартних серверних платформах, а одна фізична мережа ділиться на логічні «слайси», кожен з яких орієнтований на власний клас сервісів [35, с. 44]. Сучасні дослідження вказують, що така віртуалізація приносить значні переваги гнучкості та масштабованості, але одночасно збільшує площину атак, оскільки з'являються нові шари взаємодії між оркестраторами, віртуальними мережевими функціями та інтерфейсами керування [69, с. 341]. Окремі роботи, присвячені безпеці network slicing, наголошують на ризиках відмови ізоляції між слайсами, горизонтальних атак між віртуальними сегментами та складності повного моніторингу трафіку в умовах динамічного створення і видалення слайсів у реальному часі [57; 64]. У разі успішної атаки на оркестратор або елемент керування зловмисник отримує можливість не лише перехоплювати дані, а й модифікувати політики маршрутизації, пріоритизації або шифрування, що на практиці еквівалентно контролю над цілою логічною мережею.

Особливу увагу в контексті 5G слід приділити edge обчисленням, які виносять частину обробки даних з центральних хмарних центрів у безпосередню близькість до базових станцій і кінцевих пристроїв [46, с. 146].

Мобільні оператори впроваджують мультидоступні edge платформи для зменшення затримок до рівня одиниць мілісекунд і підтримки сценаріїв масового підключення датчиків, автономного транспорту, доповненої реальності, індустріальних систем керування [45, с. 118]. Edge вузли при цьому часто розміщуються у менш захищених локаціях, ніж класичні дата-центри, мають обмежені можливості фізичного захисту та резервування, але обробляють великий обсяг чутливих даних і трафіку керування [12]. Огляд сучасних підходів до безпеки 5G вказує, що саме edge рівень стає критичною точкою, де перетинаються інтереси мобільного оператора, хмарного провайдера і корпоративного замовника, а отже зростає ризик конфлікту політик безпеки, некоректної сегментації та появи «сірих зон» моніторингу [8, с. 41]. У випадку компрометації edge вузла нападник отримує змогу атакувати не лише конкретну вертикаль, наприклад систему розумного виробництва, а й інші сервіси, що поділяють ту саму обчислювальну платформу.

Стрімке зростання Інтернету речей посилює вплив 5G і edge обчислень на загальний ландшафт кіберзагроз. За даними галузевих оглядів, кількість підключених IoT пристроїв у світі до кінця 2023 року досягла приблизно 16,6 млрд., у 2024 році очікується близько 18,8 млрд., а до 2030 року прогнозуються вже понад 39-40 млрд. підключених об’єктів. Окремі прогнози для стільникового IoT, що включає NB-IoT, LTE-M і 5G massive Machine Type Communications, говорять про вихід на рівень близько 5-8 млрд. стільникових підключень до 2030 року [18]. Значна частина цих пристроїв працюватиме саме в середовищі 5G, використовуючи розширені можливості радіоінтерфейсу та edge платформ. У таких умовах будь-який вектор атаки на мережевий рівень або на базову інфраструктуру IoT (шлюзи, брокери повідомлень, платформи керування пристроями) може одночасно торкатися мільйонів сенсорів, виконавчих механізмів і контролерів у критичних секторах, таких як енергетика, транспорт, охорона здоров’я, міська інфраструктура [62, с. 38]. Це означає, що інцидент кібербезпеки в 5G IoT

середовищі здатен мати не лише інформаційні, а й виразні кіберфізичні наслідки, включно з перебоями в роботі об’єктів критичної інфраструктури.

Сучасні дослідження демонструють, що активна експлуатація вразливостей у стеку протоколів 5G і мікропрограмному забезпеченні модемів створює нові сценарії атак на мережевому рівні. Прикладом є описана в 2024 році сімейство вразливостей під умовною назвою 5Ghoul, що стосується прошивки 5G-модемів провідних виробників. Атака дозволяє, зокрема, примусово переводити пристрої з 5G у менш захищені 4G мережі, використовуючи нешифрований етап попередньої аутентифікації, і досягати успішності експлуатації на рівні 70-90 % з дистанції до 20 метрів [62, с. 39]. Переведення пристрою на застарілу технологію виводить його з-під дії частини покращених механізмів безпеки 5G і знову відкриває відомі можливості для пасивного перехоплення метаданих, аналізу місцезнаходження, а в окремих випадках активних атак на сигнальний рівень. Для середовища, де до однієї базової станції можуть бути підключені тисячі кінцевих пристроїв і вузлів IoT, подібні вразливості створюють потенціал для масштабних кампаній зі стеження або дестабілізації сервісів.

У випадку edge обчислень та 5G IoT особливо небезпечним є поєднання класичних проблем слабкої безпеки пристроїв Інтернету речей із новими можливостями мережевої інфраструктури. Велика частина IoT обладнання працює на спрощених операційних системах з мінімальними ресурсами, рідко отримує оновлення, використовує типові паролі або спрощені протоколи автентифікації [20, с. 111-112]. У попередніх поколіннях мереж це обмежувало шкоду переважно локальними сценаріями, тоді як у середовищі 5G такі пристрої отримують високошвидкісний доступ, низькі затримки та можливість брати участь у складних розподілених сценаріях. З погляду загроз це означає, що зламані IoT вузли можуть не лише формувати класичні ботнети для DDoS-атак, а й використовувати edge платформи для координації синхронізованих атак на інші слайси, мережеві сегменти або хмарні сервіси. Аналітичні огляди

resilience IoT інфраструктури підкреслюють, що поєднання збоїв від фізичних факторів, таких як екстремальні погодні умови, і кібератак на мережевий рівень 5G створює багатовимірні сценарії ризику, які необхідно враховувати вже на етапі проєктування систем [23, с. 118].

Узагальнюючи, технологія 5G та edge обчислення у 2020-ті роки перетворили мережевий рівень, кінцеві пристрої та Інтернет речей на єдину взаємопов'язану площину атак, де вразливість на будь-якому рівні може мати каскадні наслідки для всієї екосистеми мобільних сервісів. З одного боку, 5G забезпечує безпрецедентні показники пропускної здатності, затримок і масового підключення пристроїв, що робить можливими нові бізнес-моделі і сервіси. З іншого боку, віртуалізація мережевих функцій, динамічні network slices, проміжні edge вузли і мільярди IoT пристроїв формують складне середовище, де класичні підходи до побудови периметра безпеки та моніторингу вже не працюють у попередньому вигляді [25, с. 286]. Для забезпечення належного рівня інформаційної безпеки необхідне переосмислення моделей загроз, адаптація механізмів аутентифікації, шифрування, сегментації, а також впровадження інтегрованих підходів до оркестрації безпеки у 5G і за його межами, про що доцільно йтиметься в наступних підрозділах магістерської роботи.

Таблиця 3.1 – Ключові параметри та ризики 5G і edge-обчислень

Аспект	**Характеристика та дані**	**Потенційні загрози**	**Аналітичний висновок**
Масштаб впровадження 5G	На початок 2025 року кількість підписок 5G у світі перевищила приблизно 2,1 млрд. Прогнози до 2030 року говорять про 6,3-6,4 млрд. підписок, тобто понад 60 % усіх	Збільшення кількості підключень означає, що будь яка вразливість у протоколах сигналізації, керуючих елементах мережі або прошивці модемів потенційно впливає	Масштаб 5G перетворює мережевий рівень на глобальну площину атак. Навіть локальний збій може мати транскордонні наслідки, тому вимоги до стійкості, сегментації та

	мобільних підключень.	на мільярди користувачів і критичні сервіси.	контролю доступу суттєво зростають.
Частка мобільного трафіку в 5G	За оцінками галузевих звітів, до кінця 2030 року до 80 % світового мобільного трафіку даних проходитиме через мережі 5G, тоді як у 2024 році на них припадає приблизно третина.	Компрометація мережевих елементів 5G, наприклад ядра або граничних вузлів, створює можливість перехоплення, модифікації або блокування значної частини глобального трафіку, включаючи мобільні платежі, хмарні сервіси та дистанційне керування об'єктами.	Концентрація трафіку у 5G робить цю технологію пріоритетною ціллю для державних і кримінальних акторів. Захист 5G ядра і транспортної інфраструктури стає елементом національної безпеки.
Віртуалізація та network slicing	Більшість функцій мережі 5G реалізується у вигляді віртуальних мережевих функцій на стандартних серверах. Одна фізична мережа ділиться на логічні слайси під різні сервіси, наприклад масовий IoT, критичні комунікації, мобільний широкосмуговий доступ.	Атака на оркестратор або віртуальну мережеву функцію може порушити ізоляцію між слайсами, дозволити горизонтальні переміщення між сегментами, змінити політики маршрутизації, пріоритизації або шифрування.	Network slicing підвищує гнучкість, але створює новий «шар» управління, де помилка конфігурації або компрометація мають мультиплікативний ефект. Потрібен окремий моніторинг безпеки слайсів та жорстка ізоляція між ними.
Edge-обчислення (MEC)	Обробка даних зміщується ближче до користувача: граничні вузли біля базових станцій забезпечують затримки на рівні одиниць мілісекунд для застосунків доповненої реальності, індустріальної автоматики,	Edge вузли часто розміщуються у менш захищених локаціях, ніж класичні дата центри, обслуговують кілька клієнтів і можуть стати точкою для атак на дані різних орендарів, ін'єкцій шкідливого коду в потоки обробки,	Edge рівень стає «вузлом концентрації» ризиків, де перетинаються політики безпеки оператора, хмарного провайдера та корпоративного замовника. Без чіткої сегментації й контролю довіри саме цей рівень може

	автономного транспорту.	саботажу критичних сервісів з низькою затримкою.	стати найслабшою ланкою 5G екосистеми.
Кількість пристроїв IoT в 5G середовищі	Кількість IoT пристроїв у світі у 2023 році оцінювалася приблизно у 16,6 млрд., у 2024 році близько 18,8 млрд., а до 2030 року прогнозується понад 39-40 млрд. підключених об'єктів. Значна частина нових підключень використовуватиме стільникові технології NB IoT, LTE M та 5G.	Масове підключення малозахищених сенсорів і виконавчих механізмів створює потенціал для ботнетів, атак на протоколи керування, маніпуляцій даними вимірювань, а також кіберфізичних інцидентів у виробництві, енергетиці, транспорті, охороні здоров'я.	5G фактично стає «мережею мереж» для IoT. Безпечне проєктування, автентифікація пристроїв, оновлення прошивки, сегментація і моніторинг трафіку IoT повинні розглядатися як невід'ємна частина стратегії безпеки 5G.
Атаки на рівні модемів і радіоінтерфейсу	Сімейство вразливостей 5Ghoul у прошивках 5G модемів дозволяє примусово переводити пристрої з 5G у менш захищені мережі, переривати з'єднання або знижувати рівень безпеки. У експериментах рівень успішної експлуатації досягав 70-90 % на дистанціях до 20 метрів.	Нападник може змусити пристрої відмовитися від більш захищених режимів, повернувши їх до старіших стандартів із відомими слабкостями, що спрощує пасивне стеження, аналіз місцезнаходження й певні види активних атак на сигнальний рівень.	Навіть за розгорнутої криптографії у верхніх шарах стеку вразливості модемів і механізмів радіодоступу можуть зводити нанівець переваги 5G безпеки. Необхідні регулярні оновлення прошивки і незалежний аудит реалізацій модемів різних виробників.

Джерело: складено автором за даними [12; 62, с. 35; 66].

Таблиця 3.2 – Приклади інцидентів та сценаріїв атак у середовищі 5G і IoT

Рівень або компонент	Реальний приклад чи сценарій	Кількісні показники	Наслідки для кібербезпеки
Прошивки 5G модемів	Вразливості 5Ghoul у 5G модемах, які дозволяють примусово знижувати рівень зв'язку, переводити пристрій у менш захищені мережі, спричиняти відмову в обслуговуванні.	Дослідники показали, що успішність експлуатації окремих варіантів вразливості сягає 70-90 % у радіусі приблизно 20 метрів. У масштабі базової станції це може означати одночасний вплив на сотні або тисячі пристроїв.	Атаки на модеми дозволяють обійти частину мережевих захистів і створюють передумови для масового зниження рівня безпеки, перехоплення метаданих чи дестабілізації послуг, пов'язаних із критичною інфраструктурою.
Edge вузли та MEC платформи	Сценарій компрометації edge вузла, який обробляє трафік для систем доповненої реальності, автономних транспортних засобів та індустріальних датчиків. Нападник отримує доступ до контейнерів кількох клієнтів на спільній платформі MEC.	В одному вузлі можуть оброблятися дані тисяч кінцевих пристроїв. У разі порушення ізоляції між середовищами клієнтів зловмисник може корумпувати або аналізувати трафік декількох вертикалей одночасно.	Компрометація edge платформи на практиці означає вихід за межі одного застосунку або сегмента. Порушуються принципи багатокористувацької ізоляції, з'являється можливість координації складних розподілених атак на інші мережеві сегменти і хмарні сервіси.
Масовий IoT у 5G мережах	Розгортання мільйонів смарт-лічильників, сенсорів міської інфраструктури, промислових датчиків з базовими засобами захисту, які підключені через стільникові технології нового покоління.	Прогноз понад 39-40 млрд IoT пристроїв до 2030 року, з яких мільярди використовуватимуть стільниковий доступ. Навіть якщо частка скомпрометованих пристроїв становитиме 1 %, це сотні мільйонів вузлів, придатних для ботнетів або збирання чутливих даних.	Слабкий захист окремих IoT пристроїв у поєднанні з масштабом і можливостями 5G перетворює їх на потужний ресурс для DDoS атак, шпигунства, маніпуляцій вимірювальними даними і кіберфізичних впливів на виробництво, транспорт, енергетику.

Network slicing для критичних сервісів	Логічний слайс для критичних комунікацій органів безпеки та служб реагування розгорнуто на тій самій фізичній інфраструктурі, що і слайси для комерційних сервісів. Помилка конфігурації дозволяє витік керуючого трафіку між слайсами.	Навіть одиничний інцидент такого типу здатен вплинути на доступність каналів зв'язку, які використовуються для координації дій поліції, медичних служб або аварійних бригад у великому місті чи регіоні.	Порушення ізоляції network slices руйнує основну перевагу логічної сегментації. Для критичних слайсів необхідні посилені механізми контролю цілісності конфігурації, незалежний моніторинг і окрема модель довіри.
Сервіси управління IoT та платформи моніторингу	Компрометація платформи керування IoT, яка через 5G і edge вузли збирає дані з тисяч сенсорів та відправляє командні повідомлення виконавчим пристроям, таким як вимикачі, контролери, клапани.	Через одну платформу можуть проходити дані і команди для десятків тисяч або навіть мільйонів кінцевих вузлів. Підміна команд або даних призводить до хибних спрацювань, простоїв або аварій у різних сегментах критичної інфраструктури.	Платформи керування IoT стають точками єдиного відмовлення. Вони потребують рівня захисту, співставного з системами керування енергетикою і транспортом, включаючи сегментацію, багаторівневу автентифікацію, журналювання і безперервний моніторинг аномалій.
Комбіновані атаки з використанням 5G та хмарних сервісів	Сценарій, коли ботнет із десятків тисяч зламаних IoT пристроїв у 5G мережах координується через хмарні сервери і edge платформи, атакуючи одночасно веб-ресурси, VPN шлюзи, інші елементи 5G інфраструктури.	Масштаб 5G і IoT дозволяє досягати пікових навантажень у терабітному діапазоні, що вже спостерігається в сучасних DDoS атаках, а використання легітимних 5G адрес і слайсів ускладнює фільтрацію трафіку.	

Джерело: складено автором за даними [12; 62, с. 36; 66].

Поєднання вразливості кінцевих пристроїв з особливостями мережі п’ятого покоління є сімейство атак 5Ghoul на базові модеми у смартфонах та маршрутизаторах. У дві тисячі двадцять третьому році дослідники з Singapore University of Technology and Design описали щонайменше 14 вразливостей у прошивках модемів Qualcomm і MediaTek, з яких 10 безпосередньо стосуються модемів для мережі п’ятого покоління. За оцінками технічних оглядів, ці помилки присутні більш ніж у 710 моделях смартфонів, включаючи популярні пристрої на Android та iOS, а також у стільникових маршрутизаторах і USB модемах для доступу до мобільного інтернету. Атака не потребує знання секретних параметрів абонента на зразок даних сім карти, достатньо налаштувати випромінювач так, щоб рівень сигналу від підробленої базової станції був вищий, ніж сигнал від легітимної [62, с. 36]. Після цього користувацьке обладнання автоматично підключається до зловмисного вузла, де ініціюється серія спеціально сформованих керуючих повідомлень, що призводять до відмови в обслуговуванні, заморожування з’єднання або примусової відмови від використання мережі п’ятого покоління на користь застарілих стандартів.

Додаткову практичну небезпеку демонструє інший дослідницький фреймворк, SNI5GECT, який працює на етапі попередньої аутентифікації в мережі п’ятого покоління. У лабораторних експериментах з реальною інфраструктурою було показано, що система здатна коректно знімати трафік у висхідному і низхідному напрямках з точністю понад 80 % при відстані до 20 метрів, а цілеспрямоване впорскування змінених керуючих повідомлень досягає успішності від 70 % до 90 %, залежно від сценарію [39]. На практиці це означає, що нападник, який розгорнув компактний комплект з програмованої радіостанції та міні комп’ютера в зоні покриття базової станції, може масово примусово знижувати рівень захисту для смартфонів і стільникових IoT пристроїв, переводячи їх з мережі п’ятого покоління на менш

захищені стандарти, переривати з’єднання або створювати вибіркові збої в роботі критичних застосунків, що використовують edge обчислення.

З погляду кібербезпеки ці кейси чітко демонструють, як технологія п’ятого покоління та edge інфраструктура розширюють площину атак одночасно на мережевому рівні і на рівні кінцевих пристроїв. Вразливості у прошивках модемів відкривають для нападників можливість контролювати якість і параметри радіодоступу, а також нав’язувати кінцевим пристроям небезпечні конфігурації, що впливають на захищеність усієї сесії. З урахуванням того, що мережа п’ятого покоління у найближчі роки буде обслуговувати мільярди підключених об’єктів Інтернету речей, включаючи промислові датчики, транспортні системи та медичне обладнання, масова експлуатація подібних вразливостей здатна перетворитися з суто інформаційної проблеми на фактор реального кіберфізичного ризику для критичної інфраструктури.

3.2. Мобільні фінансові сервіси: фішинг, атаки типу людина посередині, крадіжка облікових даних, обхід багатофакторної автентифікації

У 2020-ті роки мобільні фінансові сервіси стали однією з головних цілей для зловмисників, оскільки смартфон перетворився на універсальний інтерфейс до банківських рахунків, платіжних карток, електронних гаманців і криптовалютних бірж. За даними міжнародних платіжних систем і профільних аналітичних компаній, уже понад 70-80 % користувачів у багатьох країнах регулярно здійснюють фінансові операції зі смартфонів, а частка мобільних платежів у загальній структурі електронної комерції стабільно зростає щороку на декілька відсоткових пунктів [25, с. 301-302]. Це означає, що будь який успішний фішинговий сценарій або атака типу людина посередині проти мобільного користувача має безпосередній фінансовий ефект, а атаки на

протоколи автентифікації й механізми підтвердження операцій стають стратегічним пріоритетом для кіберзлочинних угруповань.

Фішинг у контексті мобільних фінансових сервісів давно вийшов за межі класичних електронних листів. Сучасні кампанії масово використовують SMS повідомлення, месенджери, push сповіщення, фейкові застосунки й цільові фішингові сторінки, оптимізовані під невеликий екран смартфона [27, с. 89]. За оцінками досліджень, понад 75 % фішингових сайтів сьогодні адаптовані саме для мобільних пристроїв, а значна частка користувачів відкриває фішингові посилання не з комп'ютера, а зі смартфона. Одне з опитувань, проведених серед користувачів інтернету, показало, що близько 56 % респондентів здійснювали фінансові операції з телефоном у руках хоча б кілька разів на тиждень, але лише менше третини регулярно перевіряли адресний рядок і сертифікат сайту перед введенням банківських реквізитів. На практиці це означає, що фішингові сторінки мобільного банкінгу, систем типу оплата замовлення або підтвердження доставки мають дуже високу конверсію, особливо якщо супроводжуються соціально інженерними прийомами, наприклад повідомленнями про блокування рахунку, підозрілу операцію або термінову компенсацію [19, с. 8].

Особливо небезпечним напрямом стала комбінована експлуатація фішингу та шкідливих мобільних застосунків, орієнтованих на крадіжку облікових даних. За даними звітів провідних антивірусних компаній, кількість виявлених сімейств мобільних банківських троянів залишається відносно стабільною, але їхні можливості суттєво ускладнюються. Наприклад, за один з останніх років тільки один виробник засобів захисту зафіксував сотні тисяч інсталяцій банківських шкідливих програм у понад дев'яноста країнах, а окремі сімейства, такі як Cerberus, Anubis, ERMAC або SharkBot, регулярно з'являються в оновлених модифікаціях [23, с. 115]. Для багатьох із них характерна підтримка кількох десятків банківських застосунків, платіжних систем і криптовалютних бірж, що дозволяє атакувати одночасно клієнтів

різних фінансових організацій. Статистика розслідувань інцидентів свідчить, що класичний сценарій часто виглядає так: користувач отримує фішингове повідомлення з пропозицією встановити псевдо захисний застосунок банку, оновлення сервісу доставки або програму для відстеження посилки, після чого троян встановлюється на пристрій, отримує надмірні дозволи і вже в тлі контролює фінансову активність [20, с. 104].

Крадіжка облікових даних у мобільному середовищі реалізується через кілька основних механізмів. Перший – накладання фальшивих вікон поверх легітимних застосунків мобільного банкінгу, коли троян визначає, що користувач відкрив конкретний застосунок, і виводить майже ідентичну форму входу, перехоплюючи логін і пароль. Дослідження шкідливих програм показують, що для окремих сімейств підтримується до 60-80 різних фінансових застосунків, а шаблони фейкових екранів регулярно оновлюються під зміни дизайну [29]. Другий механізм – перехоплення push сповіщень і SMS із одноразовими кодами, а також використання служб доступності для читання вмісту екрана і автоматичного копіювання кодів підтвердження. У реальних кейсах розслідувань фіксувалося, що трояни за лічені секунди після надходження коду перехоплювали його, передавали на сервер керування і виконували транзакцію до того, як користувач встигав звернути увагу на сповіщення [17, с. 93]. Третій механізм полягає у використанні вбудованих веб переглядачів у застосунках, куди вбудовується фішингова сторінка, що візуально не відрізняється від легітимного сайту, але контролюється зловмисником [66].

Атаки типу людина посередині на мобільні фінансові сервіси реалізуються як у класичній мережевій формі, так і з використанням специфічних можливостей платформ. На рівні мережі поширеними залишаються сценарії, коли користувач підключається до скомпрометованої точки доступу Wi Fi або до фальшивої точки, налаштованої з назвою, схожою на публічну мережу, після чого трафік проходить через пристрій зловмисника.

Якщо з’єднання не захищене сучасними версіями протоколів або застосунок використовує слабкі механізми перевірки сертифікатів, стає можливим перехоплення облікових даних, сесійних токенів, параметрів транзакцій [30, с. 134]. У мобільному середовищі додатково використовуються техніки встановлення власних довірених кореневих сертифікатів на пристрій за рахунок соціальної інженерії або через MDM профілі, що дозволяє організувати прозоре SSL розшифрування для будь яких застосунків, які не перевіряють прив’язку сертифіката. Відомі випадки, коли зловмисники, отримавши контроль над корпоративною MDM інфраструктурою або зламавши окремий профіль, розгортали власні проксі сертифікати, після чого могли аналізувати і модифікувати навіть трафік мобільного банкінгу [40, с. 141].

Окремої уваги потребують сучасні методи обходу багатофакторної автентифікації, які активно застосовуються проти мобільних фінансових сервісів. Класичні механізми другого фактора, такі як одноразові коди в SMS або push підтвердження, проєктувалися з розрахунком на те, що навіть якщо пароль буде скомпрометовано, зловмиснику буде складно отримати доступ до другого каналу. Сьогодні це припущення втрачає актуальність. Банківські трояни масово інтегрують модулі для читання SMS, перехоплення push сповіщень і взаємодії зі службами доступності, що дозволяє їм не лише зчитувати одноразові коди, а й натискати кнопки підтвердження у вікні операції [28; 69, с. 327]. За оцінками дослідників, частка шкідливих програм для Android, які зловживають службами доступності, у сегменті фінансових троянів сягає десятків відсотків, а поодинокі кампанії демонструють повністю автоматизовані сценарії обходу двофакторної автентифікації, де участь оператора зводиться до мінімуму.

Крім суто технічних засобів, широко використовуються соціально інженерні схеми обходу багатофакторної автентифікації. Типовий сценарій передбачає телефонний дзвінок або повідомлення нібито від представника

банку чи платіжної системи, де жертву переконують самостійно озвучити або переслати код підтвердження операції, авторизувати вхід з нового пристрою чи дати згоду на «тестову» транзакцію. Статистика правоохоронних органів у ряді країн свідчить, що значна частина успішних крадіжок із рахунків фізичних осіб відбувається саме у форматі комбінованих атак, де технічні засоби (фішингові посилання, шкідливі застосунки) доповнюються дзвінками або повідомленнями від псевдо служб підтримки [7, с. 254]. При цьому середній розмір збитків для одного епізоду зростає, оскільки соціальна інженерія дозволяє атакуючим обходити ліміти на операції, переконуючи жертву самостійно підтверджувати перекази і зміну налаштувань безпеки.

На рівні платформ помітно зростає використання токенів доступу, біометричних методів та апаратних модулів захисту, однак зловмисники адаптуються до цих змін. У веб середовищі широко застосовуються фішингові комплекси, що працюють у режимі реального часу, проксіюючи сесію між користувачем і справжнім банківським сайтом, перехоплюючи не лише логін і пароль, а й одноразові коди, а потім використовуючи вже встановлену сесію для проведення операцій. Аналогічні принципи поступово переносяться і в мобільний контекст, де атакуючі експериментують з інжекцією коду в WebView, маніпуляціями з OAuth токенами і використанням зламаних або шахрайських застосунків для зчитування даних із захищених сховищ [9, с. 206]. Хоча такі атаки складніші у реалізації, вони показують напрям розвитку загроз і демонструють, що навіть сучасні схеми автентифікації можуть бути обійдені при поєднанні декількох технік.

Мобільні фінансові сервіси в 2020-ті роки перебувають під постійним тиском з боку фішингових кампаній, шкідливих застосунків, мережевих атак типу людина посередині й складних схем обходу багатофакторної автентифікації [17, с. 93]. Висока частка користувачів, які виконують критично важливі операції зі смартфона, поєднується з об’єктивними обмеженнями невеликого екрана, спрощених інтерфейсів і звички швидко підтверджувати

запити без аналізу, що суттєво знижує бар’єр для соціальної інженерії [25, с. 297]. З точки зору кібербезпеки це потребує впровадження більш зрілих підходів до захисту, де акцент переноситься з простого використання другого фактора на комплексні механізми виявлення аномальної поведінки, прив’язку автентифікації до конкретного пристрою, захист від шкідливих застосунків і агресивну протидію фішингу, включаючи блокування фейкових мобільних застосунків, моніторинг доменів і активну роботу з підвищення обізнаності користувачів.

Таблиця 3.3 – Тенденції використання мобільних фінансових сервісів і пов’язані ризики

Показник / тенденція	**Характеристика та дані**	**Пов’язаний тип атаки**	**Аналітичний висновок**
Масове використання мобільного банкінгу	У багатьох країнах частка клієнтів, які хоча б раз на місяць заходять у мобільний банкінг, перевищує 70-80 %. У великих банків кількість активних мобільних користувачів вимірюється мільйонами, а понад 50 % усіх платіжних операцій проходить саме через мобільні застосунки.	Фішинг, встановлення шкідливих застосунків, крадіжка облікових даних	Концентрація фінансових операцій у смартфоні робить його головною ціллю. Будь який успішний фішинговий сценарій одразу дає зловмиснику доступ до реальних грошей, а не лише до облікових записів.
Зростання частки мобільних платежів в електронній комерції	У структурі електронної комерції частка транзакцій, ініційованих зі смартфона, у окремих країнах перевищує 60 %, а в сегменті малого бізнесу мобільні платежі часто домінують над класичними картковими платежами з комп’ютера.	Атаки типу людина посередині, підміна платіжної форми, фішингові платіжні сторінки	Мобільний браузер і вбудовані WebView перетворюються на критично важливі точки контролю. Вразливості валидації сертифікатів, некоректна реалізація шифрування та довірених коренів одразу впливають на великий обсяг платіжного трафіку.
Поширення електронних гаманців і оплат безконтактними методами	Кількість активних гаманців у сервісах на кшталт Apple Pay, Google Pay, Samsung Wallet зростає щороку двозначними темпами, а частка безконтактних оплат у роздрібній торгівлі у низці країн перевищує 50 %.	Крадіжка токенів, компрометація облікового запису хмарного гаманця, шахрайські прив’язки карток	Хоча безконтактні протоколи мають сучасні механізми захисту, компрометація самого акаунта гаманця через фішинг або шкідливий застосунок дозволяє додавати нові картки, змінювати пристрої та підтверджувати операції без фізичного доступу до картки.

Зростання кількості банківських троянів для мобільних ОС	За звітами виробників засобів захисту, щороку фіксуються сотні нових модифікацій мобільних банківських троянів, а кількість виявлень окремих сімейств обчислюється сотнями тисяч інфекцій на рік у десятках країн.	Накладання фальшивих екранів, перехоплення SMS, читання push сповіщень, крадіжка облікових даних	Банківські трояни еволюціонували до багатомодульних інструментів, які підтримують десятки банків і платіжних сервісів, автоматично адаптуються до нових версій застосунків і дозволяють дистанційно керувати рахунками жертви.
Використання двофакторної та багатофакторної автентифікації	Більшість банків і платіжних сервісів перейшли до обов'язкової двофакторної автентифікації, де підтвердження операцій здійснюється через одноразові коди, push сповіщення, біометричні параметри або апаратні модулі.	Перехоплення кодів, маніпуляція службами доступності, реальний час проксі фішинг, соціальна інженерія	Формальна наявність другого фактора вже не гарантує захист. Зловмисник, який контролює пристрій або канал зв'язку, здатен автоматично перехоплювати коди, натискати кнопки підтвердження або переконувати жертву самостійно авторизувати шахрайські операції.
Звичка користувачів «швидко підтверджувати»	Опитування показують, що понад 60 % користувачів підтверджують push запити і запити дозволів у мобільних застосунках автоматично, не читаючи текст до кінця, особливо коли поспішають або виконують типові операції.	Соціальна інженерія, нав'язливі спливаючі вікна, накладання інтерфейсу	Людський фактор стає критичним. Навіть добре спроєктовані технічні механізми захисту нівелюються, якщо користувач без аналізу погоджується з будь яким запитом, що підвищує успішність фішингу й атак на інтерфейс.

Джерело: складено автором за даними [12; 62, с. 37; 66].

Таблиця 3.4 – Типові сценарії атак на мобільні фінансові сервіси

Тип загрози	**Реальний приклад**	**Ключові кількісні показники**	**Наслідки для кібербезпеки**
Фішинг через SMS і месенджери (смісинг)	Масові розсилки повідомлень від імені банку або служби доставки з текстом про блокування картки, підозрілу операцію чи необхідність сплатити доставку. Посилання веде на мобільну фішингову сторінку, де просять	У окремих кампаніях кількість розісланих повідомлень сягає сотень тисяч, конверсія переходів може становити 5-10 %, а частка користувачів, які вводять дані на фейковій сторінці, оцінюється на рівні 1-	Навіть за відносно невеликих відсотків успішності масовість розсилки дає зловмисникам сотні або тисячі комплектів справжніх облікових даних, які можна використати для

	ввести логін, пароль, реквізити картки і одноразовий код.	3 % від загальної кількості переходів.	негайного списання коштів або подальшого перепродажу на підпільних майданчиках.
Банківський троян з накладанням екранів	Сімейства на кшталт Cerberus, Anubis, ERMAC або SharkBot відстежують, коли користувач запускає конкретний застосунок мобільного банкінгу, і накладають поверх нього підроблену форму входу. Жертва вводить логін і пароль, які автоматично відправляються на сервер керування.	Окремі сімейства підтримують до 60-80 фінансових застосунків. Загальна кількість інфікованих пристроїв у глобальних кампаніях може сягати десятків тисяч на одну модифікацію, а сумарно по року фіксуються сотні тисяч інсталяцій.	Троян отримує не лише статичні реквізити, а й доступ до поточного стану рахунків і історії операцій. У поєднанні з перехопленням кодів підтвердження це дозволяє дистанційно проводити платежі, змінювати ліміти, додавати нові одержувачі.
Перехоплення одноразових кодів і push сповіщень	Шкідливий застосунок отримує доступ до SMS або служб доступності. Коли банк надсилає одноразовий код або push запит для підтвердження операції, троян читає вміст повідомлення, передає його оператору і може автоматично натиснути кнопку підтвердження.	У вибірках фінансових шкідливих програм частка зразків, які зловживають службами доступності, сягає десятків відсотків. Час від надходження коду до його використання зловмисником часто становить менше 5 секунд, що робить атаки практично непомітними для користувача.	Другий фактор фактично перетворюється на ще один секрет, який контролює шкідливий застосунок. При цьому з боку банку операція виглядає так, ніби її підтвердив реальний власник пристрою, що ускладнює подальше розслідування і спори щодо повернення коштів.
Атаки типу людина посередині через фальшиві точки доступу	Зловмисник розгортає Wi Fi точку з назвою, подібною до публічної мережі, наприклад у торговому центрі або кав’ярні. Користувач підключається до	Навіть одинична точка доступу з високою прохідністю може обслуговувати сотні користувачів на день. Дослідження публічних мереж показують, що	Неправильне налаштування протоколів шифрування або довіри до сертифікатів дає змогу зловмиснику отримати облікові

	неї, відкриває мобільний банкінг у браузері, а весь трафік проходить через пристрій нападника. Якщо перевірка сертифікатів налаштована некоректно, можливе прозоре перехоплення даних.	значний відсоток точок або погано захищений, або налаштований без шифрування, що полегшує атаки пасивного і активного перехоплення.	дані і сесійні токени навіть без встановлення шкідливого застосунку. Це особливо критично для користувачів, які здійснюють операції в публічних мережах.
Обхід багатофакторної автентифікації через реальний час фішинг	Фішингові комплекси в реальному часі працюють як проксі між користувачем і справжнім банківським сайтом. Коли жертва вводить логін, пароль і одноразовий код, система негайно використовує ці дані у справжній сесії, поки код ще дійсний.	У деяких кампаніях, спрямованих на користувачів банків і криптобірж, кількість жертв вимірюється тисячами облікових записів, а середній час між введенням коду і несанкціонованою операцією становить кілька десятків секунд.	Навіть сучасні схеми автентифікації з одноразовими кодами виявляються вразливими, якщо зловмисник «вклинюється» у канал комунікації в реальному часі. Це змушує фінансові установи переходити до прив’язки автентифікації до конкретного пристрою і до поведінкової аналітики.
Комбіновані соціально інженерні схеми	Зловмисники телефонують жертвам, представляючись співробітниками банку або служби безпеки. Паралельно надсилаються справжні SMS з кодами, які генерує банк, а жертву просять назвати або переслати ці коди нібито для «відміни підозрілої операції». Насправді коди підтверджують	Статистика правоохоронних органів окремих країн показує, що частка інцидентів із мобільним банкінгом за участю соціальної інженерії становить від 30 до 60 % від усіх випадків шахрайства з рахунками фізичних осіб.	

	шахрайські перекази.		

Джерело: складено автором за даними [12; 62, с. 37; 66].

Комбінованої атаки на мобільні фінансові сервіси є кампанії банківського трояна FluBot, який протягом 2020-2022 років масово поширювався в Європі через SMS та месенджери. Користувачі отримували повідомлення нібито від служби доставки з текстом про посилку та посиланням на «додаток для відстеження». Після переходу за посиланням жертву змушували встановити APK «кур'єрської служби», при цьому на телефоні тимчасово вимикали стандартні обмеження на встановлення з невідомих джерел. В одному з публічних звітів наводилися оцінки, що тільки в окремих країнах ЄС кількість користувачів, які отримали такі повідомлення, вимірювалася сотнями тисяч, а завантаження шкідливого застосунку сягали десятків тисяч інсталяцій за одну хвилю розсилки. Після установки FluBot отримував доступ до служб доступності, контактів, SMS і push сповіщень, що дозволяло йому одночасно реалізовувати фішинг, крадіжку облікових даних і обхід двофакторної автентифікації [69, с. 344].

Технічно FluBot поєднував кілька векторів атаки на мобільний банкінг. Насамперед він відстежував, які саме банківські застосунки встановлені на пристрої, і мав вбудований набір шаблонів під десятки популярних мобільних банків Європи і Великої Британії. Коли користувач відкривав свій банк, троян накладав поверх справжнього інтерфейсу підроблене вікно входу з логотипом і візуальною копією дизайну. Уведені логін і пароль миттєво відправлялися на сервер керування, часто разом із додатковими даними, такими як модель пристрою, версія операційної системи, IP адреса. Паралельно FluBot мав модуль для читання SMS і push сповіщень. У момент, коли банк надсилав одноразовий код для підтвердження входу або транзакції, троян за частки секунди перехоплював повідомлення, витягував код і пересилав його

оператору, який у реальному часі використовував ці дані для входу в акаунт жертви з іншого пристрою та проведення платежів [69, с. 345]. На практиці інтервал між відправленням банком коду і його використанням зловмисниками становив кілька секунд, тому користувачі нерідко навіть не встигали усвідомити, що відбувається щось підозріле.

За оцінками правоохоронних органів і кібербезпекових компаній, окремі хвилі FluBot охоплювали десятки тисяч активних інфекцій одночасно, причому середній розмір збитків на одного користувача складав від кількох сотень до кількох тисяч євро залежно від країни і встановлених лімітів банку. У деяких розслідуваннях згадувалося, що сукупні збитки від діяльності угруповання, яке стояло за цим трояном, могли вимірюватися мільйонами євро за рік. Важливо, що формально усі операції підтверджувалися реальними SMS або push сповіщеннями на телефон жертви, тому з точки зору банківських систем ризик менеджменту це виглядало як легітимна активність власника рахунку. Це суттєво ускладнювало як оперативне блокування шахрайських операцій, так і подальші спори клієнтів з банками щодо повернення коштів.

Такий кейс дуже чітко демонструє, як у мобільних фінансових сервісах поєднуються фішинг, шкідливі застосунки, атаки типу людина посередині на рівні SMS і push сповіщень, а також обхід багатофакторної автентифікації. Зловмисники використовують слабкі місця користувацької поведінки, невеликі екрани, звичку швидко натискати «ОК» на всіх запитах, а також технічні можливості платформ, як от служби доступності та доступ до повідомлень. У результаті навіть наявність другого фактора у вигляді одноразового коду вже не гарантує захист, якщо сам смартфон скомпрометовано трояном, що повністю контролює вхідні повідомлення і виведення вікон банківського застосунку.

3.3. Захист у корпоративному середовищі: концепція Zero Trust для мобільних пристроїв, керування мобільністю підприємства, контейнеризація, політики використання особистих та корпоративних пристроїв

У корпоративному середовищі мобільні пристрої перетворилися на повноцінні робочі станції, які мають доступ до пошти, файлових сховищ, CRM, систем електронних платежів і внутрішніх бізнес застосунків. За результатами різних опитувань до 55 % фахівців з безпеки вважають смартфони одним з найуразливіших типів ендпоінтів, а частка мобільних пристроїв, з яких користувачі переходять за фішинговими посиланнями, перевищує 15 % [52, с. 23]. Це означає, що будь яка стратегія захисту корпоративної інфраструктури, яка ігнорує мобільний сегмент або розглядає його як другорядний, створює критичний розрив у загальній моделі загроз. Додатковим фактором ризику виступає поширення дистанційної та гібридної роботи, коли смартфони, планшети і ноутбуки постійно перемикаються між домашніми, публічними та корпоративними мережами, а також використовуються для доступу до хмарних сервісів поза периметром традиційних засобів захисту.

Концепція Zero Trust у цьому контексті пропонує принципово інший підхід до корпоративного захисту мобільних пристроїв. Її ключові ідеї полягають у відмові від довіри за замовчуванням до внутрішньої мережі, перевірці кожного доступу з урахуванням ідентичності користувача, стану пристрою, контексту сесії та мінімізації прав [52, с. 24]. За даними профільних звітів, у 2023 році близько 61 % організацій уже мали формалізовану ініціативу з упровадження Zero Trust, а ще приблизно 35 % планували розпочати такі проєкти протягом найближчих 18 місяців. Аналітики прогнозують, що до 2025 року до 60 % компаній використовуватимуть рішення моделі Zero Trust замість класичних корпоративних віртуальних приватних мереж для

віддаленого доступу до внутрішніх застосунків [38, с. 230]. У мобільному середовищі це означає перехід від моделі, де достатньо підключитися до корпоративного VPN, до моделі, в якій кожен запит з телефона або планшета проходить додаткові перевірки, а доступ надається тільки до конкретних ресурсів, необхідних для виконання завдання.

Попри високий інтерес до Zero Trust, реальний рівень зрілості корпоративних практик поки що обмежений. Дослідження, виконані на базі опитувань IT фахівців, показують, що лише близько 34 % організацій реально впровадили рішення Zero Trust Network Access, а системи керування привілейованим доступом використовуються приблизно у 30 % компаній [4, с. 149]. Натомість VPN і багатофакторна автентифікація застосовуються значно ширше, але в мобільному сегменті часто реалізовані у спрощеному вигляді, що не враховує стан пристрою [43, с. 146]. Це створює ситуацію, коли навіть скомпрометований смартфон, на якому встановлено шкідливий застосунок, може після успішної автентифікації отримати повний доступ до внутрішніх ресурсів. Саме тому в сучасних моделях Zero Trust для мобільних пристроїв особливий акцент робиться на перевірці відповідності пристрою політикам безпеки, використанні сертифікатів пристрою, прив’язці доступу до конкретного апарата та його поточного стану.

Практичним інструментом реалізації таких підходів є платформи керування мобільністю підприємства, до яких належать рішення класу Mobile Device Management та Enterprise Mobility Management. Глобальний ринок MDM у 2024 році оцінювався приблизно у 13,3 мільярда доларів, з прогнозом зростання до понад 90 мільярдів доларів до 2033 року при середньорічному темпі понад 22 %, що прямо відображає попит на централізоване керування мобільними пристроями й політиками безпеки [61]. Для корпоративного середовища такі платформи надають базовий набір функцій, зокрема інвентаризацію мобільних пристроїв, контроль версій операційної системи і встановлених застосунків, примусове застосування політик шифрування,

налаштування паролів і біометрії, а також можливість віддаленого блокування або стирання даних у випадку втрати пристрою [55, с. 54]. У поєднанні з концепцією Zero Trust це дозволяє будувати політики, де доступ до критичних бізнес застосунків надається тільки якщо пристрій зареєстрований у системі, не зламаний, має актуальні оновлення й проходить перевірку на наявність шкідливого програмного забезпечення.

Окремим блоком стоїть контейнеризація робочого середовища на мобільних пристроях. У більшості сучасних мобільних платформ уже реалізовано механізми розділення особистого і корпоративного простору, наприклад робочі профілі в Android Enterprise або керовані застосунки й облікові записи в мобільних операційних системах іншого виробника. Ідея полягає в тому, що корпоративні застосунки й дані розміщуються в окремому логічному контейнері, який шифрується і керується тільки через корпоративну систему MDM або EMM. Користувач працює з двома умовними просторами на одному смартфоні, де особисті фото, месенджери й соціальні мережі не мають доступу до документів і пошти компанії, а корпоративні політики не торкаються особистих застосунків і даних [53, с. 249]. Для служби безпеки це дає змогу, наприклад, виконати віддалене очищення лише корпоративного контейнера при звільненні співробітника, не втручаючись у його особисту інформацію. Такий підхід суттєво знижує ризики витоку даних через особисті застосунки, але вимагає від компанії ретельного проєктування політик, щоб не створювати надмірного дискомфорту користувачам.

Використання особистих пристроїв у корпоративних цілях є одним із найскладніших аспектів мобільної безпеки. За даними досліджень, оприлюднених у останні роки, близько 82 % компаній так чи інакше дозволяють співробітникам використовувати особисті пристрої для доступу до робочих ресурсів, що значною мірою пов’язано з пандемією та масовим переходом на дистанційну працю. Глобальний ринок BYOD та корпоративної мобільності оцінюється більш ніж у 70 мільярдів доларів і має зрости до понад

130 мільярдів доларів у наступному десятилітті [45, с. 199]. Водночас глибші опитування показують, що лише приблизно половина організацій формально дозволяє BYOD, тоді як фактично близько 78 % співробітників використовують особисті телефони для роботи навіть там, де це заборонено. Додатково близько 38 % IT фахівців визнають, що не мають повної видимості щодо всіх пристроїв у мережі, а приблизно 40 % пристроїв на периферії, зокрема датчики, камери та інше обладнання, залишаються без централізованого керування. За оцінками цього ж дослідження, до 90 % атак програм шифрувальників стартують з некерованого пристрою, що робить політику щодо BYOD і edge пристроїв критично важливою для кіберстійкості підприємства [57].

На практиці компанії комбінують кілька підходів: модель BYOD, коли співробітник використовує власний телефон під контролем MDM і контейнеризації; модель CYOD, де працівник обирає з обмеженого переліку схвалених пристроїв; а також модель COPE, яка передбачає пристрої, що належать компанії, але частково використовуються в особистих цілях. Для кожної моделі формуються окремі політики щодо того, які дані можуть зберігатися локально, які застосунки дозволені, як працює журналювання і моніторинг, чи дозволено резервне копіювання в хмарні сервіси користувача. З погляду кібербезпеки найжорсткіші вимоги зазвичай застосовуються для доступу до критичних ресурсів, наприклад фінансових систем, внутрішніх сховищ вихідного коду або служб керування промисловими процесами [59]. Тут Zero Trust для мобільних пристроїв реалізується через перевірку відповідності пристрою вимогам безпеки, аналіз поведінкових аномалій, застосування багатофакторної автентифікації з прив’язкою до конкретного смартфона та обмеження доступу лише до потрібних сегментів мережі [70, с. 3]. На цьому фоні стрімке зростання ринку рішень MDM і BYOD безпосередньо відображає прагнення організацій не просто дозволити мобільну роботу, а й зробити її керованою і безпечною, що особливо важливо

в умовах постійного зростання кількості мобільних атак і вартості успішних інцидентів.

Таблиця 3.5 – Впровадження Zero Trust, MDM та BYOD у корпоративному середовищі

Показник	**Кількісні дані**	**Що це означає для мобільних пристроїв**	**Аналітичний висновок**
Впровадження стратегії Zero Trust	Опитування Gartner у 2023 році показало, що приблизно 63 % організацій у світі вже повністю або частково реалізували стратегію Zero Trust.	Формально більшість компаній декларує перехід до моделі недовіри за замовчуванням для користувачів і пристроїв, включно з мобільними телефонами та планшетами.	Zero Trust уже став де-факто стандартом на рівні стратегій. Однак без прив'язки до стану мобільного пристрою та його керованості ця стратегія часто залишається декларативною.
Реальне впровадження Zero Trust Network Access і PAM	За даними досліджень Ivanti лише близько 34 % компаній фактично впровадили Zero Trust Network Access і приблизно 30 % використовують рішення керування привілейованим доступом.	У значної частини організацій доступ з мобільних пристроїв усе ще базується на класичному VPN і статичних ролях. Це створює ризик, що скомпрометований смартфон отримує той самий рівень доступу, що і довірений робочий комп'ютер.	Існує розрив між стратегією та практикою. Без реального ZTNA для мобільних пристроїв модель Zero Trust не закриває ключові вектори атак у корпоративному мобільному середовищі.
Ринок систем Mobile Device Management	Оцінка ринку MDM у 2024 році коливається в діапазоні від приблизно 7,5 до 12,1 млрд. доларів США. Прогнози до 2030-2032 років дають зростання до 28-82 млрд. доларів із середньорічним темпом понад 24-26 %.	Компанії активно інвестують у централізоване керування мобільними пристроями. MDM стає базовою умовою для того, щоб застосовувати політики шифрування, примусового оновлення, блокування і стирання даних на смартфонах і планшетах.	Стрімке зростання ринку MDM відображає перехід до керованого мобільного парку пристроїв. Водночас на практиці MDM не завжди охоплює особисті телефони співробітників, які використовуються за моделлю BYOD.

Формальна наявність політик BYOD	Сучасні огляди показують, що понад 80 % організацій мають формальні політики BYOD, а до 95 % компаній у тій чи іншій формі дозволяють використання особистих пристроїв для роботи.	Фактично мобільні телефони співробітників перетворилися на повноцінні робочі ендпоінти. Через них відбувається доступ до пошти, месенджерів, хмарних сховищ, CRM і фінансових застосунків.	BYOD став нормою. Це дає гнучкість бізнесу, але різко ускладнює завдання контролю й уніфікації політик безпеки для дуже різнорідного парку пристроїв.
Фактичне використання особистих пристроїв (shadow BYOD)	Згідно зі звітом Ivanti лише 52 % компаній офіційно дозволяють BYOD, при цьому приблизно 78 % співробітників усе одно використовують особисті телефони для роботи, навіть там, де це формально заборонено.	Значна частина мобільних пристроїв, що мають доступ до корпоративних даних, може не бути зареєстрована в MDM і не підпорядковуватися політикам безпеки.	Shadow BYOD створює «сліпі зони» в інфраструктурі. Без повної інвентаризації пристроїв і прозорої політики підприємство фактично не знає, звідки саме відбувається доступ до його даних.
Некеровані пристрої та рансомвар	Дані кількох звітів (Microsoft, Ivanti, профільні огляди) свідчать, що приблизно 90 % інцидентів з програмами шифрувальниками починаються з некерованого пристрою, тобто пристрою поза зонами MDM і політик безпеки.	У цю категорію потрапляють особисті смартфони, планшети і edge пристрої, що не контролюються IT службою, але підключаються до корпоративних сервісів.	Статистика чітко показує, що саме некеровані та «сірові» пристрої є головною точкою входу для шифрувальників. Це безпосередньо підсилює аргументи на користь Zero Trust для мобільних пристроїв і тотальної інвентаризації.
BYOD і витоки даних	Окремі огляди ринку безпеки BYOD вказують, що близько 40 % інцидентів витоку даних пов’язані з втратою або крадіжкою пристроїв, а приблизно 50 % компаній, які	Втрата незашифрованого смартфона або планшета з робочими листуваннями, документами й кешами корпоративних застосунків створює реальний ризик	Коректна політика BYOD має включати обов’язкову шифрацію, можливість дистанційного видалення корпоративних даних і чіткі вимоги до блокування

	дозволяють BYOD, стикаються зі значною кількістю інцидентів витоку саме через особисті пристрої.	розкриття конфіденційної інформації.	екрана. Без цього BYOD неминуче підвищує імовірність витоків.

Джерело: складено автором за даними [17, с. 93; 57; 59; 70, с. 8].

Таблиця 3.6 – Моделі використання мобільних пристроїв у компаніях та їхній вплив на безпеку

Модель / сценарій	**Реальний приклад і цифри**	**Основні ризики**	**Висновки для політик Zero Trust, MDM та контейнеризації**
COPE (corporate owned, personally enabled) – корпоративні пристрої з обмеженим особистим використанням	Велика фінансова чи IT компанія видає співробітникам стандартизовані смартфони. Усі пристрої зареєстровані в MDM, мають однакову версію ОС і набір корпоративних застосунків. Ринок MDM у 2024 році оцінюється щонайменше у 7-12 млрд. доларів із прогнозом зростання до десятків мільярдів до 2030-2032 років, що показує масове впровадження саме таких моделей.	Компрометація окремого пристрою усе одно дає атакуючому канал до внутрішніх застосунків. Є ризики фізичної втрати пристрою, але завдяки MDM компанія може виконати віддалене стирання даних, примусове блокування і форсувати оновлення.	Найбільш контрольована модель. Ефективність Zero Trust підвищується, якщо до перевірки ідентичності додається перевірка стану пристрою. Контейнеризація дозволяє відокремити особисті застосунки від корпоративних і зменшує конфлікти з користувачами щодо приватності.
BYOD без чіткої політики (shadow BYOD)	Звіт Ivanti показав, що лише 52 % організацій	Особисті телефони не зареєстровані в	З погляду Zero Trust небезпечно довіряти запитам з пристрою

	формально дозволяють BYOD, але приблизно 78 % співробітників використовують особисті телефони для роботи навіть там, де це заборонено.	MDM, не шифруються за корпоративними стандартами, на них можуть бути встановлені вразливі або шкідливі застосунки. Відсутність видимості означає, що служба безпеки не знає, які саме пристрої мають доступ до хмарних сервісів, пошти, файлів.	лише тому, що користувач пройшов автентифікацію. Необхідні рішення типу ZTNA з перевіркою відповідності пристрою, а також політика, яка або переводить BYOD під контроль MDM, або жорстко обмежує можливості доступу з некерованих пристроїв.
BYOD з формалізованою політикою та MDM/контейнеризацією	Сучасні опитування показують, що понад 80 % організацій мають формалізовану політику BYOD, а до 95 % у тій чи іншій формі дозволяють використання особистих пристроїв для роботи. Організація вимагає встановлення корпоративного MDM профілю та створення окремого робочого контейнера на особистому смартфоні.	Ризики зменшуються, але не зникають. Залишається ймовірність, що користувач відмовиться від профілю або вимкне його. Особисті застосунки можуть бути вразливими, хоча прямого доступу до контейнера не мають.	Така модель потребує чіткого балансу між контролем і приватністю. Політики мають визначати, які саме дані може моніторити IT служба і що саме буде стерто при виході співробітника. Zero Trust у цьому випадку спирається на стан контейнера, а не всього пристрою.
Віддалені та гібридні співробітники з доступом до хмарних сервісів	Через поширення дистанційної роботи значна частина співробітників постійно	Смартфони й планшети постійно перемикаються між домашніми, публічними і	Модель Zero Trust потребує врахування контексту доступу: місцезнаходження, мережа, тип

	підключається до корпоративних ресурсів поза периметром офісної мережі. За різними оцінками понад 80 % компаній використовують BYOD або гібридні моделі мобільної роботи.	мобільними мережами. Це підвищує ризики фішингу, атак типу людина посередині, використання некерованих точок доступу.	пристрою, поведінкові аномалії. Доступ до критичних застосунків має надаватися тільки через керовані клієнти з жорсткою перевіркою ідентичності та стану пристрою.
Некеровані edge пристрої в корпоративній інфраструктурі	Дослідження Ivanti вказує, що близько 40 % edge пристроїв, зокрема сенсори, камери, термінали, залишаються поза активним керуванням, а приблизно 38 % IT фахівців визнають, що не мають повної видимості щодо всіх пристроїв у мережі.	Edge пристрої часто використовують стільниковий або Wi Fi зв'язок і мають спрощений захист. Вони можуть бути трампліном для атак на інші мобільні й корпоративні ендпоінти, а також каналом для встановлення шкідливого ПЗ в локальні сегменти мережі.	Zero Trust у поєднанні з MDM і системами керування IoT має розглядати всі підключені пристрої як потенційно недовірені. Необхідні сегментація, мікросегментація, окремі політики для edge пристроїв та контроль взаємодії між ними і мобільними ендпоінтами.
Корпоративні програми без контейнеризації на особистих телефонах	Деякі компанії дозволяють установлювати пошту, месенджери та інші застосунки безпосередньо на особисті телефони без ізоляції й окремого робочого профілю.	У разі втрати або продажу пристрою всі корпоративні дані в месенджерах, пошті, кешах документів залишаються на ньому. Резервні копії можуть автоматично потрапляти в особисті хмарні сховища користувача, які не контролює	

Джерело: складено автором за даними [17, с. 93; 57; 59; 70, с. 8].

Є кейс з глобального дослідження Ivanti про витоки даних та атаки з використанням BYOD і некерованих ендпоінтів. У звіті зазначається, що близько 90 % успішних атак програм-шифрувальників починаються саме з некерованого пристрою, який не перебуває під контролем MDM/EMM і не охоплений корпоративними політиками безпеки. Крім того, приблизно 38 % IT-фахівців визнають, що не мають повної видимості щодо всіх пристроїв у мережі, а до 40 % edge-пристроїв (камери, термінали, сенсори, мобільні гаджети) працюють поза централізованим керуванням [70, с. 8].

У тій самій вибірці з'ясувалося, що лише 52 % компаній формально дозволяють BYOD, але приблизно 78 % співробітників усе одно використовують особисті телефони для роботи, навіть там, де цього не передбачено політикою. Це класична ситуація «shadow BYOD», коли на практиці в корпоративну хмару, пошту, CRM та внутрішні портали заходять із десятків або сотень особистих смартфонів, які не зареєстровані в MDM, не проходять перевірку на відповідність вимогам безпеки та часто мають застарілу прошивку, небажані застосунки й відсутність шифрування [57; 59]. У кількох описаних інцидентах модель атаки виглядала однаково: співробітник, використовуючи особистий телефон для доступу до корпоративної пошти, відкривав фішинговий лист, завантажував вкладений файл або переходив за посиланням, після чого шкідливий код отримував доступ до облікових даних і внутрішніх ресурсів. Далі зловмисники розгортали шифрувальник у сегменті файлових серверів та віртуальних машин, а переговори про викуп вели вже з позиції повного паралічу бізнес-процесів.

Фінансові наслідки таких інцидентів суттєві: за оцінками галузевих досліджень, середня вартість одного інциденту з програмою-шифрувальником у корпоративному середовищі перевищує 4-5 млн. доларів США, якщо враховувати не лише викуп, а й простій, відновлення інфраструктури, юридичні витрати та репутаційні втрати. При цьому у звіті наголошується, що

значна частина атак могла б бути заблокована на ранніх етапах, якби доступ із мобільних і BYOD-пристроїв будувався за принципами Zero Trust: обов’язкова реєстрація пристрою в MDM, перевірка стану ОС, шифрування, контроль шкідливого ПЗ, мікросегментація доступу й жорстке обмеження прав. Саме після подібних інцидентів багато компаній переходять від формального BYOD без технічного контролю до моделей COPE або «керованого BYOD», де корпоративні дані розміщуються в зашифрованому контейнері, а будь який доступ з мобільного ендпоінта безперервно перевіряється в рамках Zero Trust.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі було узагальнено, що сучасний етап розвитку мобільних технологій у 2020-х роках супроводжується якісним стрибком у складності та масштабі загроз. Масове впровадження технології 5G, перехід до віртуалізованої інфраструктури, поява network slicing та широке використання edge обчислень разом із вибуховим зростанням кількості пристроїв Інтернету речей призвели до суттєвого розширення площини атак. Вразливість на будь якому рівні від прошивки модема і конфігурації базової станції до платформи керування IoT здатна мати каскадні наслідки для мільйонів користувачів та критичних сервісів, а інциденти набувають виразного кіберфізичного виміру, коли порушується робота енергетики, транспорту чи промислових систем.

Аналіз мобільних фінансових сервісів показав, що смартфон фактично перетворився на головний інтерфейс доступу до банківських рахунків, платіжних карток, електронних гаманців та криптовалютних платформ. Це призводить до стійкого фокусування уваги зловмисників саме на мобільному сегменті. Фішингові кампанії зміщуються в бік SMS, месенджерів та push сповіщень, банківські трояни активно використовують накладання фальшивих екранів, перехоплення SMS і push повідомлень, а також служби доступності,

що дозволяє не тільки викрадати облікові дані, а й обходити двофакторну та багатофакторну автентифікацію. Фактично другий фактор у вигляді одноразового коду або push підтвердження перестає бути надійним захистом, якщо сам мобільний пристрій скомпрометовано шкідливим програмним забезпеченням, яке контролює інтерфейс і канали доставки коду.

У корпоративному середовищі мобільні пристрої остаточно перестали бути другорядним інструментом і стали повноцінними робочими ендпоінтами з доступом до пошти, файлових сховищ, CRM систем, фінансових і виробничих застосунків. На цьому тлі концепція Zero Trust, платформи керування мобільністю підприємства та політики BYOD, CYOD і COPE виходять на передній план. Однак виявлено суттєвий розрив між декларованим впровадженням підходів Zero Trust і реальним рівнем їх застосування до мобільних та особистих пристроїв. Значна частина атак, зокрема із застосуванням програм шифрувальників, стартує саме з некерованих або особистих смартфонів, які використовуються для доступу до корпоративних ресурсів поза зонами дії MDM і формальних політик безпеки. Це підтверджує, що без тотальної інвентаризації ендпоінтів, контейнеризації робочого середовища, прив’язки доступу до конкретного стану пристрою і жорсткого обмеження прав модель Zero Trust залишається неповною.

Узагальнюючи результати третього розділу, можна зробити висновок, що сучасний етап еволюції мобільних загроз характеризується комплексністю, багаторівневістю та високим рівнем автоматизації атак. Захист мобільних технологій у таких умовах неможливо забезпечити лише за рахунок окремих технічних рішень на кшталт антивірусів або класичного VPN. Необхідне поєднання архітектурних змін на рівні 5G та edge інфраструктури, вдосконалення механізмів автентифікації і поведінкової аналітики у фінансових сервісах, а також системне впровадження Zero Trust, MDM, контейнеризації і продуманих політик роботи з особистими та корпоративними пристроями. Лише інтегрований підхід, який враховує

технічні, організаційні та людські фактори, здатен забезпечити прийнятний рівень інформаційної безпеки мобільних технологій в умовах стрімкого розвитку 5G, мобільних платежів та Інтернету речей.

ВИСНОВКИ

У магістерській роботі здійснено комплексне дослідження еволюції загроз інформаційній безпеці у мобільних технологіях з урахуванням історичної динаміки розвитку платформ та специфіки їх використання в секторі безпеки і оборони України. За результатами проведеного дослідження сформульовано такі висновки:

встановлено, що мобільна інфраструктура пройшла шлях від допоміжного засобу зв'язку до критично важливого елемента інформаційного простору. Перехід від простих пристроїв до багатофункціональних смартфонів, інтеграція мобільних сервісів у фінансову, державну та військову сфери призвели до якісної зміни структури загроз. Мобільний пристрій перестав бути ізольованою ціллю і нині розглядається зловмисниками як точка входу до розподіленої інфраструктури, хмарних сервісів та критично важливих об'єктів;

доведено, що еволюція загроз має чіткий поетапний характер, що корелює з розвитком технологій:

1. Етап 2000-х років характеризувався появою перших зразків шкідливого ПЗ (Cabir, CommWarrior) для Symbian та J2ME, які поєднували саморозмноження з прихованою фінансовою мотивацією (платні SMS);

2. Етап 2010-х років (домінування Android та iOS) відзначився централізацією загроз через магазини застосунків, масовим поширенням рекламних троянів, шпигунського ПЗ та мобільних програм-вимагачів;

3. Сучасний етап (2020-ті роки) в умовах впровадження 5G та IoT характеризується комплексними мультивекторними атаками, націленими на перехоплення даних, обхід багатофакторної автентифікації та компрометацію ланцюгів постачання;

з'ясовано, що архітектурні моделі безпеки операційних систем безпосередньо впливають на ландшафт загроз. Аналіз еволюції від ранніх

версій Symbian/Windows Mobile до сучасних Android/iOS показав, що впровадження capability-орієнтованого контролю, ізоляції даних (sandboxing) та підпису коду суттєво підвищило рівень захисту. Водночас фактори на кшталт отримання root-доступу (джейлбрейк) та ліберальні політики встановлення ПЗ зі сторонніх джерел залишаються критичними вразливостями, що нівелюють вбудовані механізми захисту;

обґрунтовано, що ключовим чинником успішної реалізації атак у мобільному середовищі залишається людський фактор. На всіх етапах еволюції – від Bluetooth-хробаків до сучасного фішингу – соціальна інженерія є основним вектором доставки загроз. Це підтверджує, що технічні засоби захисту є недостатніми без належного рівня обізнаності користувачів;

проаналізовано специфіку загроз для сектору безпеки і оборони України. Визначено, що використання некерованих особистих пристроїв (моделі BYOD) у службовій діяльності створює значні ризики витоку чутливої інформації, відстеження геолокації особового складу та компрометації управлінських комунікацій. Особливу небезпеку становлять цілеспрямовані атаки з використанням кібершпигунства та деструктивного ПЗ в умовах гібридної війни;

сформовано концептуальну модель загроз та розроблено практичні рекомендації для Національної гвардії України. Доведено необхідність переходу до впровадження принципів Zero Trust («нульової довіри»), використання систем керування мобільними пристроями (MDM/EMM) та контейнеризації службових даних.

Запропоновано комплекс заходів щодо удосконалення нормативної бази та системи підготовки персоналу НГУ. Реалізація рекомендацій щодо посилення контролю за використанням мобільних технологій, оновлення інструкцій та регулярні навчання з кібергігієни сприятимуть підвищенню стійкості інформаційної інфраструктури та зміцненню обороноздатності підрозділів перед обличчям сучасних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрєєв А. М., Пшенична О. С. Методологія наукових досліджень : навчальний посібник для здобувачів ступеня вищої освіти магістра спеціальності «Середня освіта» (ОП «Середня освіта (Інформатика)»). Запоріжжя : Запорізький національний університет, 2024. 145 с.

2. Аносов А. О. Модель перехоплення та захисту інформації в бездротових мережах / А.О.Аносов, А.В. Платоненко // *Сучасний захист інформації.* № 2(30). 2017. – С. 90-94.

3. Антонюк А. О. Основи захисту інформації в автоматизованих системах. Київ : КМ Академія, 2006. 244 с.

4. Арістова І. В., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг : монографія. К. : Право України; Х. : Право, 2013. 184 с.

5. Бабок, В. П. Інформаційна безпека та сучасні мережені технології: англ.-укр.-рос. словник термінів / В. П. Бабок, В. Г. Корченко. – К.: НАУ, 2003. – 670 с.

6. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2019. № 9. – С. 100-108.

7. Блаватська Н.М. Програмне забезпечення систем захисту інформації/ Н.М. Блаватська, В.Д. Козюра, В.О. Хорошко – К: Вид. ДУІКТ, 2011. – 330 с.

8. Бондаренко О. М. Сучасні інноваційні технології навчання у старшій школі: теорія і практика. *Педагогічний альманах.* 2022. № 4. – С. 37-42.

9. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

10. Бурячок, В. Л. Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу / В. Л. Бурячок, О. А. Ільяшов, Г. М. Гулак // *Збірник*

матеріалів круглого столу «Актуальні питання підготовки фахівців із розслідування кіберзлочинів», 25.11.2011. – К.: Наук.-вид. відділ НА СБ України, 2011. – С. 27-32.

11. Бурячок, В. Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / [В. Л. Бурячок, О. Г. Корченко, В. О. Хорошко, В. А. Кудінов] // Захист інформації. – 2013.Т. 15, № 1. – С. 5-14.

12. Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. 2021. URL: http://dspace.wunu.edu.ua/bitstream/316497/42062/1/

13. Віннікова І. І., Марчук С. В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. URL: https://chmnu.edu.ua/wp-content/uploads/2019/07/Vinnikova-I.I.-Marchuk-S.V..pdf

14. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

15. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи /С. О. Гнатюк// Безпека інформації. – 2013. Т. 19, № 2. – С. 118-129.

16. Горбенко І. Д., Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах. Ч. 1. Криптографічний захист інформації : навч. посіб. Харків : ХНУРЕ, 2004. – 368 с.

17. Григоренко О. Г., Голуб О. С. Конфіденційність даних в інфокомунікаційних мережах і засоби її забезпечення // Зб. «Перспективи телекомунікацій» ПТ-2023. К. : КПІ ім. Ігоря Сікорського, 2021. – С. 90-94.

18. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки. 2020. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf

19. Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні // *Науковий вісник Ужгородського національного університету. Серія Право*. – 2024. Вип. 84, ч. 3. – С. 77-83.

20. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право.* 2017. № 7. – С. 109-116.

21. Довгань О. Кібербезпека в інформаційному суспільстві. 2018. URL: http://ippi.org.ua/sites/default/files/bezpeka_2018-6.pdf

22. Довгань, О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О. Д. Довгань, В. Г. Хлань // *Інформаційна безпека людини, суспільства, держави.* – 2011.№ 3 (7). – С. 49-53.

23. Жайворонок О. І. Вдосконалення механізму протидії інформаційному тероризму в Україні в загальнодержавній системі антикризового реагування // Інвестиції: практика та досвід. 2018. № 17. – С. 113-119.

24. Жованик М.О. Загальні принципи захисту мобільних пристроїв в корпоративній мережі / М.О. Жованик // «Young Scientist». – 2015. - № 5(20). – С. 39-42.

25. Іваненко О. А. Цифрові трансформації у шкільній освіті: інноваційні методи і технології : монографія. Харків : Ранок, 2020. – 320 с.

26. Іванов А. М. Гейміфікація у навчанні: новий погляд на методику викладання // «Освіта і цифровий світ». Харків : ХНУ ім. Каразіна, 2023. – С. 43-46.

27. Іванов Д. О. Цифрові інструменти в освітньому середовищі старшої школи // Зб. тез доповідей міжнар. конф. «Цифрова освіта: виклики і перспективи». Львів : ЛНУ ім. І. Франка, 2023. – С. 88-92.

28. Касперски, К. Секретна зброя соціальної їнженерії / Крис Касперски. URL: http://kpnc.opennet.ru/SOC_ENG.pdf

29. Касперский, Е. Киберзлочинність як бізнес. URL: http://www.crime-research.ru/analytics/cybercrimes20101/2

30. Комар М. П., Боднар Д. І., Саченко А. О. Інтелектуалізована інформаційна технологія виявлення комп'ютерних атак // *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2010. № 2. – С. 133-137.

31. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 22.10.2025)

32. Сапитон А. О., Виганяйло С. М. Шляхи протидії кіберзлочинності. *Безпека у кіберсфері : зб. матеріалів Міжнарод. наук.-практ. конф.* (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Нац. акад. правових наук України ; ОБСЄ. – Кам'янець-Подільський : ХНУВС, 2025. – С. 113-114.

33. Ковальова Т. І. Актуальні питання нормативно-правового забезпечення та функціонування стратегічних комунікацій у діяльності складових сектору безпеки і оборони України. *Актуальні проблеми діяльності складових сектору безпеки і оборони України в умовах особливих правових режимів: поточний стан та шляхи вирішення: матеріали Міжнародної наук.-практ. конф.* / НА НГУ (28 березня 2024 року), 2024. С. 590-592.

34. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. … д-ра юрид. наук. Харків, 2004. – 44 с.

35. Корченко, О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти/ О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації. 2013.Т. 19, № 1. – С. 40-45.

36. Корченко, О. Г. Класифікація методів соціального інжинірингу / О. Г. Корченко, Є. В. Паціра, Д. А. Пуха // *Захист інформації.* – К.: НАУ. 2007. № 4. – С. 37-45.

37. Криворучко О. В. Кібергігієна. Кібербезпека. Безпека держави. 2020. URL:https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

38. Ластівка Г.І. Технічний захист інформації в інформаційних та телекомунікаційних системах: навчальний посібник / Г.І. Ластівка, П.М. Шпатар. Чернівці, Чернівецький національний університет, 2018. – 252 с.

39. Лисенко І. А. Основи управління кібербезпекою. 2018. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8431/1/Osn_ypr_kiber.pdf

40. Малиновський, В. І. Кібербезпека мобільних пристроїв таінтернетуречей : електронний практікум комбінованого (локального та мережевого) використання – / Маліновський В. І., Куперштейн Л. М., Каплун В. А. – Вінниця : ВНТУ, 2024 . – 208 с.

41. Міночкін А. І., Романюк В. А., Шацило П. В. Виявлення атак в мобільних радіомережах // Збірник наукових праць. К.: ВІТІ НТУУ «КПІ», 2005. № 1. – С. 102-111.

42. Наконечний В. С. Захист інформаційних ресурсів у мережах нового покоління LTE // *Сучасний захист інформації.* 2016. № 4. – С. 10-15.

43. Одарченко Р., Гнатюк В. Концептуальні засади підвищення рівня кібербезпеки сучасних стільникових мереж // *Ukrainian Scientific Journal of Information Security*. 2016. Vol. 22, № 2. P. 143-149.

44. Одарченко Р., Гнатюк В., Федюра Т., Коберник А. Розробка системи управління кіберінцидентами в мережах LTE // *Український міжнародний журнал інформаційної безпеки.* 2018. Вип. 24. – С. 84-90.

45. Павлюк О. М. Основи теорії надійності технічних систем : навч. посібник / О. М. Павлюк [та ін.] ; Нац. ун-т "Львів. політехніка". – Львів : Вид-во "Львів. політехніка", 2021. – 208 с.

46. Пономаренко В. С., Журавльова І. В. Основи захисту інформації : навч. посіб. Харків : ХДЕУ, 2003. – 176 с.

47. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.10.2025)

48. Сальник С. В., Сова О. Я., Міночкін Д. А. Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET // *Сучасні інформаційні технології у сфері безпеки та оборони*. 2015. № 1(22). – С. 103-112.

49. Семенов С. Г. Захист інформації в комп'ютерних системах та мережах : навч. посібник /С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків :НТУ "ХПІ", 2014. – 251 с.

50. Сенів М. М., Яковина В. С. Безпека програм та даних : навч. посібник. Львів : Видавництво Львівської політехніки, 2015. – 256 с.

51. Тарасюк А. В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник.* 2020. Вип. 1. – С. 133-136.

52. Урба С. І. Система економічної безпеки держави: сутність та особливості формування. *Науковий вісник Міжнародного гуманітарного університету*. 2017. – С. 22-25.

53. Шпортко Д.В. Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile. *Всеукраїнська наук. конф. «Актуальні проблеми кібербезпеки».* Державний університет інформаційнокомунікаційних технологій. 25.10.2024. – С. 247-251.

54. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

55. Alagic G., et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST Internal Report. 2022. 77 p.

56. Chen L., et al. Report on Post-Quantum Cryptography. NIST Internal Report 8105. National Institute of Standards and Technology. 2016. 90 p.

57. Denning, D. E. The Terrorism Research Center / D. E. Denning. – URL: http://www.washprofile.org/en/node/686

58. Ducas L., et al. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. Vol. 2018, № 1. P. 238-268.

59. Kamil Glowinski, Christian Gossmann, Dominik Strümpf. Gartner. Magic Quadrant for Mobile Device Management. 9 July 2022. ID G0055759. URL: https://www.gartner.com/en

60. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. CRC Press, 2020. 635 p.

61. Kerr, K. Putting cyberterrorism into context / K. Kerr. URL: http://www.auscert. org.au/ render.html?it=3552

62. Klimushyn P., Solianyk T., Mozhaev O., Nosov V. Kolisnyk, T. Yanov V. Hardware support procedures for asymmetric authentication of the internet of things. Innovative Technologies and Scientific Solutions for Industries. 2021. № 4 (18). P. 31-39.

63. Langlois A., Stehlé D. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography. 2015. Vol. 75, № 3. P. 565-599.

64. Mitnik, Kevin U. The Art of Deception / Kevin U. Mitnik, William L. Simon, Steve Wozniak. – Wiley, 2002. – 304 c.

65. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy. 2018. Vol. 16, № 5. P. 38-41.

66. Bi (Eileen) Li Тестування продуктивності мереж 5G за допомогою інструментів Spirent та Keysight / IEEE Access URL: https://www.spirent.com/blogs/enhancing-5g-network-performance-with-testing

67. Proos J., Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Information and Computation. 2003. Vol. 3, № 4. P. 317-344.

68. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978. Vol. 21, № 2. P. 120-126.

69. Son J., Kim Y.W., Oh D.B., Kim K. Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema. Forensic Science International: Digital Investigation. 2022. Vol. 40. P. 301-347.

70. Zhang Y., Li B., Sun Y. Android encryption database forensic analysis based on static analysis. Proceedings of the 4th International Conference on Computer Science and Application Engineering. 2020. P. 1-9.