Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

ОГЛЯД ТА АНАЛІЗ ЕФЕКТИВНОСТІ АНТИВІРУСНИХ АЛГОРИТМІВ ДЛЯ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Курсова робота
за спеціальністю “Комп’ютерні науки” 122

Керівник курсової роботи
старший викладач
Кирієнко О.В
(підпис)
“____” _____ 2025 р.

Виконала
студентка 3 року навчання
Голянська Т.С
“____” _____ 2025 р.

Київ – 2025

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

ЗАТВЕРДЖУЮ

Зав. кафедри інформатики,

к. ф.-м. н. С. С. Гороховський

_____ (підпис)

“____” _____ 2025 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсову роботу

студентки Голянської Тетяни Святославівни факультету інформатики 3 курсу

Тема: Огляд та аналіз ефективності антивірусних алгоритмів для мобільних операційних систем.

Зміст ТЧ до курсової роботи:

Вступ

1.Теоретичні основи антивірусних алгоритмів і мобільних загроз

2.Особливості мобільних операційних систем у контексті захисту

3.Огляд сучасних антивірусних рішень для мобільних операційних систем

Висновки

Список джерел

Дата видачі “___” _____ 2025р.

Керівник _____(підпис) Завдання отримано _____

ГРАФІК ВИКОНАННЯ КУРСОВОЇ РОБОТИ

No з/п	ПЕРЕЛІК РОБІТ	Термін виконання	Дата ознайомлення наукового керівника	Підпис наукового керівника
1.	Вибір теми та затвердження з керівником	жовтень 2024р.	25 жовтня 2024р.	
2.	Узгодження календарного графіка підготовки курсової роботи.	листопад 2024р.	5 листопада 2024р.	
3.	Складання плану курсової роботи та узгодження з науковим керівником	листопад 2024р.	5 листопада 2024р.	
4.	Збір та вивчення джерел літератури, матеріалів, наукових статей, даних та узагальнення фактів	листопад-грудень 2024р.	2 грудня 2024р.	
5.	Написання розділу 1 курсової роботи (аналіз предметної області, теоретичні основи)	грудень 2024р.	20 грудня 2024р.	
6.	Аналіз мобільних загроз та виявлення існуючих методів боротьби з ними	грудень-січень 2025р.	грудень-січень 2025р.	
7.	Написання розділу 2	січень 2025р.	15 січня 2025р.	
8.	Проміжний контроль виконання роботи	лютий 2025р.	лютий 2025р.	
9.	Написання розділу 3	лютий-березень 2025р.	25 березня 2025р.	
10.	Повне завершення написання курсової роботи, оформлення та подання на відгук науковому керівнику	березень-квітень 2025р.	березень-квітень 2025р.	
11.	Подання роботи для перевірки на академічну доброчесність	квітень 2025р.	5 травня 2025р.	
12.	Підготовка до захисту курсової роботи: написання доповіді та презентації	квітень 2025р	квітень - травень 2025р	
13.	Захист курсової роботи	травень 2025р	травень 2025р	

Графік узгоджено «_5__» ____листопада_____ 2025__р.
Науковий керівник __Кирієнко Оксана Валентинівна_____(ПІБ)
Виконавець курсової роботи ___Голянська Тетяна Святославівна __(ПІБ)

ЗМІСТ

Анотація

У курсовій роботі проаналізовано сучасні загрози, що виникають у сфері мобільної кібербезпеки, а також досліджено ефективність антивірусних алгоритмів, які використовуються для захисту мобільних операційних систем. Особливу увагу приділено архітектурі безпеки Android та iOS, їхнім ключовим відмінностям і підходам до захисту даних.

На основі порівняльного аналізу провідних антивірусних рішень було визначено переваги та недоліки різних методів виявлення шкідливого програмного забезпечення, зокрема сигнатурного, евристичного, статистичного та поведінкового аналізу. Розглянуто аналітичні дані незалежних лабораторій, що дозволило об’єктивно оцінити якість захисту мобільних пристроїв.

У роботі обґрунтовано необхідність комплексного підходу до мобільної безпеки в умовах постійного зростання кіберзагроз, а також запропоновано практичні рекомендації щодо підвищення рівня кіберзахисту для звичайних користувачів.

Вступ

Мобільні пристрої стали невід'ємною частиною повсякденного життя, забезпечуючи доступ до інформації, спілкування, банківських послуг та інших цифрових сервісів. Зростання популярності мобільних операційних систем, таких як Android та iOS, створює нові можливості для користувачів, але водночас стає привабливою ціллю для кіберзагроз. Кількість шкідливих програм, розроблених для мобільних платформ, щороку зростає, що зумовлює необхідність впровадження ефективних рішень для захисту.

Особливо важливою є розробка антивірусних алгоритмів, які здатні виявляти та запобігати діяльності шкідливих програм. Однак, з урахуванням швидких змін у способах атаки, традиційні методи, такі як сигнатурний аналіз, часто виявляються недостатніми. У цьому контексті виникає потреба у впровадженні більш інноваційних підходів, таких як евристичний аналіз, поведінкові моделі та машинне навчання.

Метою цієї курсової роботи є аналіз ефективності сучасних антивірусних алгоритмів, що застосовуються для захисту мобільних операційних систем. Завдання дослідження включають вивчення теоретичних основ антивірусних алгоритмів; аналіз мобільних загроз і класифікація вірусів; огляд сучасних антивірусних алгоритмів та їх порівняння; формулювання висновків і рекомендацій для покращення антивірусного захисту.

Об’єктом дослідження є системи та технології захисту мобільних операційних систем від шкідливого програмного забезпечення.

Предметом дослідження є методи, алгоритми та механізми виявлення та нейтралізації вірусів і шкідливого програмного забезпечення у мобільних операційних системах, їх ефективність та порівняльні характеристики.

Результатом дослідження буде сформоване цілісне уявлення про сильні й слабкі сторони існуючих антивірусних рішень, а також узагальнення практичних рекомендацій для підвищення ефективності мобільного захисту. Робота ґрунтується на порівняльному аналізі систем безпеки, реальних прикладах атак та сучасних підходах до виявлення шкідливого ПЗ. Такий підхід дозволяє не лише оцінити поточний стан мобільної кібербезпеки, а й запропонувати напрями для її вдосконалення з урахуванням поточних тенденцій та загроз.

1. Теоретичні основи антивірусних алгоритмів і мобільних загроз

1.1 Основні поняття кіберзахисту та мобільних загроз

Кіберзахист — це система практик, технологій і процесів, що використовуються для забезпечення захисту інформаційних систем, мереж і даних від несанкціонованого доступу, атак, крадіжок або пошкоджень. Він охоплює комплекс заходів, спрямованих на запобігання цифровим загрозам, які можуть порушити роботу критичних систем або завдати шкоди користувачам і організаціям. Основними завданнями кіберзахисту є збереження конфіденційності, цілісності та доступності даних, а також захист від сучасних видів атак, таких як шкідливе програмне забезпечення, фішинг чи програми-вимагачі [1].

Кіберзахист базується на трьох ключових принципах, які є основою забезпечення безпеки інформаційних систем: конфіденційність, цілісність і доступність.

Конфіденційність означає захист даних від несанкціонованого доступу. Це передбачає обмеження доступу до інформації тільки для авторизованих користувачів та запобігання розголошенню або витоку даних. Конфіденційність забезпечується такими методами, як шифрування, автентифікація користувачів та контроль доступу [2].

Цілісність передбачає захист даних від несанкціонованої модифікації, забезпечуючи їхню точність і достовірність. Це означає, що дані залишаються незмінними та цілісними під час зберігання або передачі. Цілісність даних підтримується за допомогою механізмів перевірки хешів, цифрових підписів і резервного копіювання [2].

Доступність гарантує, що авторизовані користувачі можуть отримати доступ до необхідних даних і систем у будь-який час. Для забезпечення доступності використовуються механізми захисту від атак типу "відмова в обслуговуванні" (DDoS), відновлення після аварій і резервне копіювання [2].

Ці три принципи, відомі як "тріада CIA" (Confidentiality, Integrity, Availability), є основою для побудови надійної системи кіберзахисту. Вони спрямовані на забезпечення цілісності, збереження та доступності даних, що є критично важливим для сучасних інформаційних систем [2].

1.2 Типи мобільних загроз

Мобільні пристрої стали невід’ємною частиною сучасного життя, забезпечуючи доступ до персональних даних, онлайн-банкінгу, соціальних мереж і бізнес-платформ. Проте їх повсюдне використання супроводжується зростанням кількості кіберзагроз, які становлять серйозну небезпеку для безпеки даних і конфіденційності користувачів.

Щоб краще зрозуміти актуальні виклики, з якими стикаються власники смартфонів і розробники мобільних додатків, доцільно проаналізувати найпоширеніші типи загроз. У таблиці нижче наведено систематизований перелік ризиків для мобільних платформ відповідно до OWASP Mobile Top 10 – 2023 Risks [3].

Таблиця 1.1 – Типи мобільних загроз за версією OWASP Mobile Top 10 – 2023 [3]

№	Тип загрози	Опис	Приклад
1	Неправильне використання облікових даних *(Improper Credential Usage)*	Відсутність захисту або недбале використання облікових даних, що створює ризик їх викрадення або несанкціонованого доступу.	Повторне використання простих паролів у різних додатках.

№	Тип загрози	Опис	Приклад
2	Уразливості в ланцюгах постачання *(Inadequate Supply Chain Security)*	Використання компонентів із неперевірених джерел або слабкий контроль над залежностями програмного забезпечення.	Інтеграція шкідливих бібліотек стороннього походження.
3	Ненадійна автентифікація / авторизація *(Insecure Authentication/Authorization)*	Недостатні або неправильно реалізовані механізми входу та розмежування прав користувачів.	Простий PIN-код без додаткового захисту чи багатофакторної автентифікації.
4	Недостатня перевірка вхідних/вихідних даних *(Insufficient Input/Output Validation)*	Відсутність перевірки правильності введених або виведених даних, що дозволяє здійснювати зловмисні маніпуляції.	SQL-ін’єкції у формах мобільного додатку.
5	Ненадійна передача даних *(Insecure Communication)*	Відсутність шифрування або його неправильна реалізація під час передавання конфіденційної інформації.	Атака типу “людина посередині” *(Man-in-the-Middle)* при передачі даних.

Аналіз першої групи мобільних загроз свідчить про те, що значна частина вразливостей виникає не лише через складність сучасних атак, а й через порушення базових принципів безпечної архітектури додатків. Неправильне використання облікових даних, як-от повторне застосування паролів або збереження логінів без шифрування, створює реальні ризики несанкціонованого доступу до конфіденційної інформації користувачів. Ця проблема особливо загострюється у випадках, коли відсутній контроль за зовнішніми компонентами — наприклад, підключенням сторонніх бібліотек, що можуть містити вразливий або шкідливий код (supply chain risks).

Окрему загрозу становлять некоректно реалізовані механізми автентифікації та авторизації, які відкривають шлях до підвищення прав доступу без належного підтвердження особи. В умовах мобільного середовища, де користувачі часто

використовують прості паролі, це призводить до численних атак на акаунти. Також критично важливо перевіряти всі введені дані — оскільки відсутність належної валідації створює вразливість до SQL-ін’єкцій та інших форм введення шкідливого коду.

Нарешті, особливо небезпечною є передача даних без захищених каналів зв’язку. Якщо мобільний додаток не використовує надійне шифрування, зловмисник може перехопити інформацію через публічні Wi-Fi мережі, використовуючи атаку типу "людина посередині" (Man-in-the-Middle). Усі ці фактори свідчать про те, що вже на етапі проєктування додатка розробники повинні враховувати основи кібергігієни, використовувати перевірені рішення і регулярно тестувати свої продукти на відповідність сучасним стандартам безпеки.

Після аналізу перших п’яти типів мобільних загроз можна зробити кілька практичних висновків. По-перше, розробникам варто звертати більше уваги на автентифікацію — прості паролі та відсутність додаткових способів підтвердження особи сильно знижують рівень безпеки. Найкраще — додати двофакторну автентифікацію.

Друге — багато проблем виникає через сторонні бібліотеки або фреймворки. Якщо просто взяти готовий компонент без перевірки, це може відкрити двері до серйозних уразливостей. Тому важливо не лише використовувати надійні джерела, а й оновлювати компоненти вчасно.

Ще одна порада — завжди перевіряти дані, які користувач вводить. Навіть просте обмеження довжини чи типу символів може захистити від атак. І, звісно, всі дані, що передаються мережею, особливо логіни чи особисті дані, мають бути зашифровані —це обов’язкова умова для будь-якого сучасного мобільного додатка.

Окрім уже розглянутих загроз, які переважно стосуються автентифікації, взаємодії з користувачем і передавання даних, існує ще низка важливих вразливостей, пов’язаних із зберіганням інформації, обробкою коду та використанням функцій платформи. Наступна таблиця продовжує перелік типових загроз для мобільних додатків згідно з OWASP Mobile Top 10 – 2023 [3].

Таблиця 1.2 – Типи мобільних загроз за версією OWASP Mobile Top 10 – 2023 [3]

№	Тип загрози	Опис	Приклад
6	Незахищене зберігання даних *(Insecure Data Storage)*	Дані зберігаються без шифрування або доступні іншим додаткам, що підвищує ризик їх викрадення.	Зберігання токенів автентифікації у відкритому вигляді в пам’яті телефону.
7	Недостатній захист коду *(Code Tampering Vulnerabilities)*	Відсутність захисту від модифікації коду або структури додатку.	Хакер змінює логіку програми для обходу авторизації або реклами.
8	Небезпечне використання WebView *(Insecure Use of WebView)*	Вбудовані браузерні елементи можуть використовуватись для атак, якщо налаштування WebView некоректні.	Відкриття неперевіреного сайту у WebView без обмежень JavaScript.
9	Недостатній контроль сесій *(Inadequate Session Handling)*	Погане керування сеансами може призвести до крадіжки сесії або несанкціонованого доступу.	Сесія не завершується після виходу з додатку або втрати підключення.
10	Зловживання платформою *(Improper Platform Usage)*	Недотримання рекомендацій і політик безпеки платформи, використання застарілих API або некоректних дозволів.	Запитування зайвих дозволів, як-от доступ до мікрофона без функціональної потреби.

Загрози, представлені у другій частині списку OWASP, більшою мірою стосуються технічних аспектів реалізації мобільних додатків, а саме — способів

зберігання, обробки та захисту даних на пристрої. Однією з найпоширеніших помилок є нехтування безпекою під час збереження даних — особливо тоді, коли додаток оперує чутливою інформацією, наприклад, токенами авторизації або історією платежів. Якщо така інформація не зашифрована або зберігається у відкритому доступі, вона стає легкою здобиччю для зловмисників, які отримають фізичний або root-доступ до пристрою.

Ще одним важливим напрямом є захист від модифікації коду — зокрема, тоді, коли користувачі встановлюють зламані версії додатків із неперевірених джерел. У таких випадках сам код може бути змінений, а його функціональність — використана в шкідливих цілях. Це стосується й помилок у роботі з WebView, який відкриває браузерні вікна прямо всередині додатку. Якщо його не обмежити, то зловмисник може впровадити фішинговий сайт або виконати шкідливий скрипт без відома користувача.

Особливу увагу слід звернути на керування сесіями — адже погане завершення сесій або їх автоматичне збереження після виходу з додатку може надати доступ до акаунтів стороннім особам. Це особливо критично для банківських або корпоративних застосунків, де кожна сесія повинна мати чітке завершення та таймаут неактивності.

Наостанок, варто відзначити, що чимало розробників нехтують правилами самої платформи — Android або iOS. Наприклад, запитують більше дозволів, ніж необхідно, або використовують застарілі інтерфейси, які вже не відповідають сучасним вимогам безпеки. Усе це створює додаткові вразливості, яких цілком можна було б уникнути ще на етапі проєктування додатку.

Щоб уникнути проблем із небезпечним зберіганням даних, варто одразу передбачити використання шифрування — не лише при передачі інформації мережею, але й при зберіганні її у файловій системі пристрою. Це особливо

актуально для застосунків, які працюють з фінансами, персональними або службовими даними.

Також важливо унеможливити модифікацію коду: варто впроваджувати перевірку цілісності додатку та використовувати захищені механізми підписування. Це допоможе запобігти використанню зламаних версій програми, які можуть містити доданий шкідливий функціонал.

Робота з WebView повинна бути обмежена і максимально контрольована. Якщо додаток відкриває вебсторінки всередині себе, розробник має переконатися, що немає доступу до JavaScript-команд, що можуть бути використані для атак або крадіжки даних.

Керування сеансами — ще один критичний момент. Рекомендується впроваджувати автоматичне завершення сесій після певного часу неактивності, а також скидання сесії після виходу з облікового запису. Також варто уникати збереження облікових даних у відкритому вигляді між сеансами.

Щодо взаємодії з платформою — варто дотримуватися актуальних стандартів Android та iOS. Не слід запитувати надмірних дозволів — це не лише знижує рівень довіри користувачів, але й створює потенційні вразливості. Крім того, необхідно регулярно оновлювати API та бібліотеки, що використовуються, аби уникнути експлуатації застарілих механізмів.

1.3 Класифікація мобільних вірусів і їх вплив на пристрої

Мобільний вірус є різновидом зловмисного програмного забезпечення, розробленого спеціально для ураження мобільних пристроїв, таких як смартфони та планшети. Його метою може бути викрадення особистих даних, завантаження шкідливого коду або навіть повний контроль над пристроєм. Ці віруси зазвичай поширюються через заражені додатки, шкідливі вебсайти або

фішингові повідомлення. Завдяки швидкому поширенню мобільних пристроїв, віруси цього типу стають дедалі серйознішою загрозою для користувачів і бізнесів [4]. Серед найпоширеніших типів мобільних вірусів виділяють трояни, руткіти, шпигунське програмне забезпечення та фішинг-програми.

Трояни є одними з найбільш поширених загроз для мобільних пристроїв. Ці шкідливі програми маскуються під легітимне програмне забезпечення, щоб обманом змусити користувача встановити їх. На відміну від традиційних вірусів, трояни не здатні до самореплікації, але вони можуть виконувати такі деструктивні функції, як крадіжка особистих даних, видалення файлів чи приховане завантаження іншого шкідливого коду [5].

У 2023 році трояни залишались однією з найнебезпечніших загроз для мобільних пристроїв, зокрема в банківському секторі. Як повідомляється у звіті ThreatFabric, троян Chameleon поширювався під виглядом легітимних додатків, зокрема Chrome або урядових застосунків. Після встановлення він отримував повний доступ до пристрою через служби доступності (Accessibility Service), а також міг обходити біометричний захист, замінюючи блокування екрана на PIN. Таким чином зловмисники отримували доступ до облікових даних і контролю над сесіями користувача [6].

Ще одним прикладом складного банківського трояна, що активно розвивався у 2023 році, є Xenomorph. На відміну від Chameleon, який маскується під урядові або системні програми, Xenomorph активно використовує фальшиві банківські інтерфейси та функціонал захоплення екрана для крадіжки чутливих даних користувачів.

За даними дослідження компанії ThreatFabric, нова хвиля заражень Xenomorph охопила понад 30 банківських додатків у США, Іспанії та Португалії. Зловмисники поширювали троян через підроблені мобільні додатки, які

візуально імітували Google Chrome або популярні криптогаманці. Після встановлення програма запитувала доступ до служб доступності Android, що дозволяло їй перехоплювати SMS-коди, зчитувати натискання, змінювати екран входу та навіть виконувати дії від імені користувача. Таким чином троян фактично дозволяв здійснювати повний контроль над банківським акаунтом без взаємодії з жертвою. Нижче наведено таблицю, що містить ключові характеристики та механізми роботи трояна Xenomorph [7].

Таблиця 1.3 – Характеристики банківського трояна Xenomorph [7]

Параметр	Опис
Назва трояна	Xenomorph
Рік активності	2023
Цільові додатки	Банківські програми США, Іспанії, Португалії; криптовалютні гаманці
Спосіб зараження	Завантаження через шкідливі додатки, що маскуються під Chrome, аналітичні інструменти, тощо
Механізм дії	Доступ до Accessibility Services, перехоплення 2FA, створення фальшивих форм входу, керування пристроєм
Основна загроза	Повний контроль над фінансовими транзакціями користувача без його відома
Рекомендації	Завантажувати додатки лише з перевірених джерел, перевіряти дозволи, оновлювати систему безпеки пристрою

Щоб краще зрозуміти, як діє типовий троян, варто розглянути спрощену модель його поведінки. Умовний приклад нижче демонструє, як шкідливе програмне забезпечення може збирати базову інформацію про пристрій користувача.

```python
import platform
import socket
import uuid
import json

def collect_device_info():
    device_info = {
        "OS": platform.system(),
        "OS_version": platform.version(),
        "Hostname": socket.gethostname(),
        "IP_address": socket.gethostbyname(socket.gethostname()),
        "MAC_address": ':'.join(['{:02x}'.format((uuid.getnode() >> i) & 0xff)
                                 for i in range(0,8*6,8)][::-1])
    }
    return device_info

if __name__ == "__main__":
    info = collect_device_info()
    print("Зібрана інформація про пристрій:")
    print(json.dumps(info, indent=4))
```

Рис.1.1 – Демонстраційний код на Python для збору інформації про пристрій

Даний рисунок ілюструє приклад умовного коду, який демонструє базовий процес збору технічної інформації про пристрій. Такий підхід може використовуватись у шкідливому програмному забезпеченні для первинної ідентифікації пристрою, створення унікального профілю або підготовки до подальших атак. У цьому прикладі здійснюється отримання інформації про операційну систему, IP- та MAC-адресу, а також назву пристрою. Хоча наведений код є безпечним і не виконує жодних деструктивних дій, його логіка нагадує механізми, які часто застосовуються у троянах на ранніх етапах зараження системи.

Окрім троянів, існує низка інших типів шкідливого програмного забезпечення, що становлять загрозу для мобільних пристроїв. Ці загрози відрізняються як за своїм функціоналом, так і за способом проникнення в систему користувача.

Руткіти призначені для приховування своєї присутності або активності іншого шкідливого програмного забезпечення. Вони можуть проникати у систему, використовуючи її слабкі місця, і надавати зловмисникам доступ до

конфіденційних даних. Завдяки своїй складності, руткіти зазвичай використовуються для тривалих атак [5].

Шпигунське програмне забезпечення (Spyware) розроблене для збору конфіденційної інформації користувачів без їхнього відома. Воно може включати доступ до місцезнаходження пристрою, історії браузера або даних про платежі. Наприклад, у багатьох відомих випадках шпигунські програми використовувалися для моніторингу дій користувачів і пересилання отриманих даних зловмисникам [5].

Фішинг – це метод, при якому зловмисники використовують підроблені повідомлення, вебсайти або програми для отримання конфіденційних даних, таких як паролі або дані кредитних карт. Фішинг-програми особливо небезпечні через їхню здатність імітувати легітимні служби, що підвищує ймовірність успішної атаки [5].

Таким чином, сучасне шкідливе програмне забезпечення для мобільних пристроїв охоплює широкий спектр загроз, кожна з яких потребує окремого підходу до виявлення та нейтралізації.

Висновок до розділу 1

У першому розділі курсової роботи було проведено ґрунтовний аналіз основних понять, пов’язаних з мобільною безпекою та шкідливим програмним забезпеченням, що становить загрозу для сучасних мобільних пристроїв. Розглянуто природу мобільних вірусів, способи їх розповсюдження, механізми впливу на систему, а також класифікацію найбільш поширених типів шкідливого програмного забезпечення.

Особливу увагу було приділено загрозам, які виникають у результаті використання мобільних додатків, зокрема троянам, руткітам, шпигунським

програмам та фішинговим атакам. Аналіз продемонстрував, що більшість шкідливого програмного забезпечення орієнтоване на крадіжку конфіденційних даних, отримання доступу до системних ресурсів або контроль над пристроєм без відома користувача. Важливо зазначити, що значна частина таких загроз поширюється через соціальну інженерію або використання вразливостей у самих додатках, що ще раз підкреслює необхідність обережного користування мобільними пристроями та програмним забезпеченням.

У результаті проведеного аналізу було підтверджено, що тема захисту мобільних пристроїв є надзвичайно актуальною. Сформоване в цьому розділі розуміння структури та динаміки розвитку мобільних загроз створює надійну теоретичну базу для переходу до розгляду антивірусного захисту, ефективності відповідних алгоритмів і сучасних технологій протидії шкідливому програмному забезпеченню.

2. Особливості мобільних операційних систем у контексті захисту

2.1 Архітектура безпеки Android

Мобільні пристрої відіграють ключову роль у сучасному цифровому середовищі, слугуючи не лише засобом зв’язку, а й основною платформою для зберігання, обробки та передавання конфіденційної інформації. Така концентрація персональних даних робить мобільні операційні системи привабливою ціллю для кіберзлочинців. У зв’язку з цим питання безпеки мобільного середовища набуває особливої актуальності. Оскільки кожна операційна система реалізує власні підходи до захисту, дослідження їхньої архітектури дозволяє глибше зрозуміти, як саме відбувається протидія загрозам на рівні платформи.

Архітектура безпеки операційної системи Android є одним із ключових компонентів забезпечення захисту мобільних пристроїв та персональних даних користувачів. З огляду на те, що Android є найпоширенішою мобільною операційною системою у світі, питання її надійності та захищеності набуває особливого значення. Система безпеки Android проєктувалася з урахуванням необхідності протидії потенційним загрозам, зокрема шкідливим програмам, несанкціонованому доступу до конфіденційної інформації, а також захисту операційного середовища під час виконання додатків.

Згідно з аналітичними даними Statcounter Global Stats, станом на березень 2025 року Android утримує близько 71,9% світового ринку мобільних операційних систем, тоді як iOS займає 27,68% [8].

Одним із викликів для системи безпеки Android залишається фрагментація — велика кількість активних версій операційної системи, які одночасно використовуються на ринку. За даними Statcounter, станом на березень 2025 року найбільшу частку користувачів мала версія Android 14 — 34,59%, що свідчить про її широке поширення за короткий час після релізу. На другому місці залишалася

Android 13 із часткою 17,39%, далі — Android 12 (12,43%) та Android 11 (10,85%). Також у статистиці з'явилась нова версія Android 15, яка вже встигла зайняти 7,56% ринку. Решта користувачів продовжують використовувати старіші версії, зокрема Android 10 та нижче, які сумарно охоплюють понад 11% пристроїв [9].

Така різноманітність у версіях ускладнює впровадження єдиної політики безпеки та оновлень, оскільки багато пристроїв залишаються на застарілих платформах із обмеженим захистом.

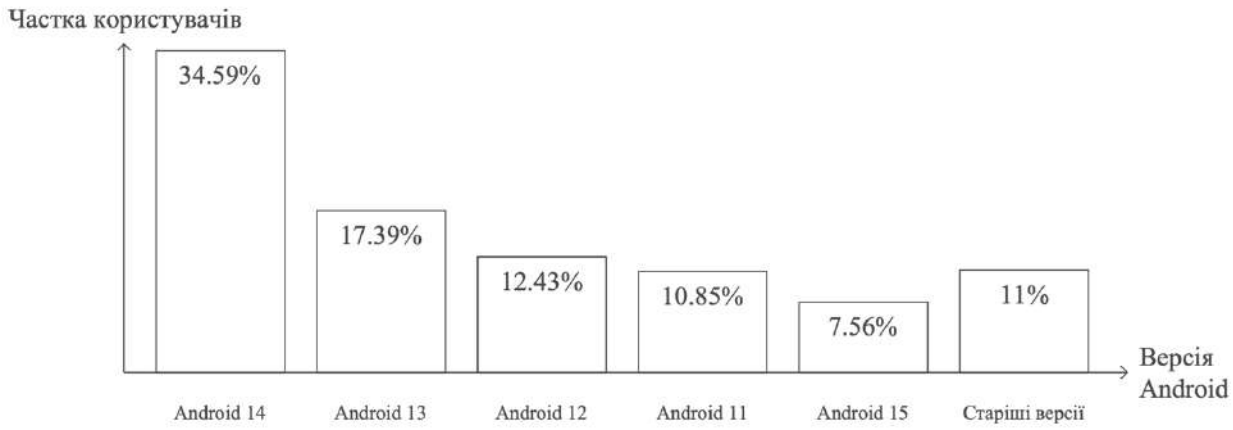

Рис. 2.1 – Розподіл частки користувачів за версіями Android станом на березень 2025 року [9]

Android можна розглядати як програмне забезпечення, яке складається з кількох шарів, кожен із яких виконує специфічні функції і надає послуги вищим шарам. В основі Android лежить ядро Linux, яке забезпечує базову функціональність. Понад ядром знаходяться рідні бібліотеки та Android runtime, зокрема Dalvik Virtual Machine (VM), що дозволяє запускати додатки. Шар, який взаємодіє з користувачем, є Application framework. Він дає можливість додаткам працювати з базовими бібліотеками та ядром Android. На верхньому рівні знаходяться самі додатки, які працюють в рамках цієї архітектури, забезпечуючи функціональність мобільного пристрою [10].

В Android безпека додатків забезпечується через кілька основних елементів, які визначають функціональність та взаємодію компонентів усередині операційної системи.

Одним із найважливіших елементів безпеки в Android є файл AndroidManifest.xml. Цей конфігураційний файл містить інформацію про основні компоненти додатка, такі як активності, сервіси, приймачі широкомовних повідомлень і контент-постачальники. Крім того, в ньому вказано, які дозволи необхідні для роботи цих компонентів. Таким чином, файл відіграє вирішальну роль у визначенні того, як додаток взаємодіє із системою і з іншими програмами [11].

Активності в Android відповідають за виконання завдань, пов'язаних із взаємодією користувача з додатком. Це можуть бути екрани, форми, діалоги тощо. Активність забезпечує виконання певного завдання, яке зазвичай включає відображення інтерфейсу для користувача. Однак деякі активності можуть працювати без відображення інтерфейсу або бути взаємодіючими з іншими компонентами в фоновому режимі. Такий підхід дозволяє гнучко керувати функціоналом додатка, не навантажуючи користувача зайвими екранами та процесами [11].

Іншим важливим компонентом є сервіси. Сервіси в Android виконуються в фоновому режимі і можуть бути незалежними від інтерфейсу користувача. Вони відповідають за виконання довготривалих завдань, таких як відтворення медіа, синхронізація даних або обробка великих обсягів інформації. Сервіси працюють без потреби в активному інтерфейсі та можуть підтримувати свою роботу навіть після того, як користувач закриває додаток. Це дає змогу забезпечити безперервність виконання критичних завдань, незалежно від того, чи взаємодіє користувач з додатком [11].

Ще одним важливим компонентом є приймачі широкомовних повідомлень (Broadcast Receivers). Вони реагують на певні системні або зовнішні події, які виникають під час роботи операційної системи або інших додатків. Наприклад, приймачі можуть отримувати повідомлення про низький рівень заряду батареї або про наявність нових оновлень для додатків. Ці компоненти дозволяють додаткам змінювати свою поведінку відповідно до подій, що відбуваються в системі, тим самим підвищуючи зручність для користувачів і забезпечуючи адаптацію додатків до поточних умов [11].

Ці елементи забезпечують основну безпеку Android, ізолюючи різні компоненти один від одного та обмежуючи доступ до системних ресурсів. Завдяки такій архітектурі, додатки можуть взаємодіяти між собою лише в межах дозволених взаємодій, що значно знижує ризик шкідливих атак і забезпечує захист даних користувача.

Однією з основних функцій безпеки в Android є використання механізму пісочниці (sandbox) для додатків. Це дозволяє ізолювати додатки один від одного та забезпечити захист даних від зловмисних програм. Android використовує унікальні ідентифікатори користувачів (UID), що призначаються кожному додатку. Завдяки цьому кожен додаток працює у своєму власному процесі, і не має можливості взаємодіяти з іншими додатками або доступати системні ресурси без відповідних дозволівця забезпечує безпеку на рівні процесів, ізолюючи додатки один від одного через стандартні можливості Linux, як-от ідентифікацію користувачів і груп, що запобігає небажаному доступу. Наприклад, якщо додаток A намагається отримати доступ до даних додатка B або здійснити несанкціоновані дії, такі як дзвінок на телефон, без наявності відповідних дозволів, ця операція буде заблокована. Однак, для належного виконання такого рівня безпеки необхідно, щоб Android використовував додаткові захисні механізми, що з часом посилюються на кожній новій версії системи [12].

Оскільки процес працює на рівні ядра, ця модель безпеки стосується як нативного коду, так і додатків операційної системи. Усі компоненти, включаючи бібліотеки ОС, фреймворк додатків та виконувані файли, працюють всередині пісочниці, що забезпечує їхню ізоляцію від інших компонентів системи та взаємодії між додатками. Тому безпека пісочниці є важливим елементом системи, яка гарантує правильну роботу Android, захищаючи пристрої від потенційних загроз і шкідливих програм [12].

Ще одним важливим аспектом безпеки в Android є система захищених API. Кожен додаток Android за замовчуванням працює в ізольованому середовищі, що обмежує доступ до системних ресурсів, таких як камера, дані про місцезнаходження (GPS), Bluetooth, функції телефонії та інші чутливі дані. Для того щоб додаток міг використовувати ці захищені API, він повинен запитати відповідні дозволи у користувача, які визначаються через механізм Permissions. Це забезпечує додатковий рівень безпеки, дозволяючи користувачеві мати контроль над тим, які ресурси додатки можуть використовувати. У нових версіях Android (6.0 і вище) використовується модель runtime permissions, що дозволяє користувачам надавати дозволи під час роботи додатка, покращуючи контроль над даними та забезпечуючи більшу гнучкість в управлінні безпекою [11].

Важливу роль у захисті Android від шкідливих програм відіграє також система Google Play Protect, що активно перевіряє додатки на наявність загроз перед їх публікацією в Google Play Store.

Це вбудована система безпеки, яка сканує додатки та пристрої на наявність шкідливих програм. Вона перевіряє додатки з Google Play перед їх завантаженням і регулярно сканує вже встановлені додатки на пристрої користувача. Якщо виявлено шкідливу програму, Google Play Protect може автоматично видалити її та попередити користувача про небезпеку [13].

Окрім автоматичної перевірки додатків через Google Play Protect, важливо враховувати, що деякі шкідливі програми здатні маскуватися під легітимне програмне забезпечення, що значно ускладнює їх виявлення. Наприклад, за результатами дослідження компанії Merit Solutions, понад 60 000 додатків для Android, які виглядали як звичайні утиліти чи сервіси, насправді поширювали рекламне програмне забезпечення (adware) на пристроях користувачів. Це підкреслює важливість завантаження програм лише з офіційних магазинів, таких як Google Play Store, адже більшість шкідливих додатків було встановлено зі сторонніх джерел [14].

Згідно з офіційним звітом компанії Doctor Web за третій квартал 2024 року, було зафіксовано декілька небезпечних типів шкідливого програмного забезпечення для ОС Android, які створюють серйозні ризики для безпеки користувачів. Однією з найбільш активних загроз є програма Android.FakeApp, яка імітує звичайний корисний застосунок, але фактично є троянською програмою. Її головна функція полягає у перенаправленні користувача на шахрайські ресурси, де, за допомогою соціальної інженерії, здійснюється спроба викрасти особисті або фінансові дані [15].

Ще однією поширеною загрозою є Android.HiddenAds — різновид рекламного трояна, що функціонує у фоновому режимі. Після встановлення така програма приховує свою іконку, уникаючи виявлення, і при цьому безперервно відображає настирливу рекламу. Це не лише створює серйозні незручності для користувача, а й помітно знижує продуктивність пристрою, перевантажуючи системні ресурси [15].

Серед виявлених загроз також була Android.Siggen — універсальна шкідлива програма, яка не підпадає під одну конкретну категорію зловмисного ПЗ. Вона здатна виконувати широкий спектр деструктивних функцій, що суттєво ускладнює її виявлення та класифікацію традиційними методами аналізу [15].

Окрему занепокоєність викликала загроза Android.Vo1d, зафіксована у серпні 2024 року. Ця шкідлива програма вразила понад 1,3 мільйона Android TV-пристроїв у 197 країнах світу, надаючи зловмисникам можливість дистанційного керування зараженими системами. У результаті, на інфіковані пристрої могли завантажуватись додаткові шкідливі компоненти, що створювало потенційну загрозу масштабних атак [15].

За офіційним звітом Google за 2023 рік, у магазині Google Play було заблоковано понад 2,28 мільйона додатків, які порушували вимоги безпеки. Більшість із них містили потенційно шкідливе програмне забезпечення або запитували надмірні дозволи, що могло створити загрозу для конфіденційності користувачів. Крім того, компанія заблокувала 333 тисячі облікових записів розробників, які були причетні до створення або повторного поширення небезпечних додатків [21].

Проаналізовані приклади свідчать про те, що шкідливе програмне забезпечення для Android продовжує активно розвиватися та адаптуватися до нових умов. Зловмисники використовують різні техніки — від маскування під легітимні додатки до проникнення у пристрої через телевізійні приставки. Це підтверджує, що загрози стали більш гнучкими, прихованими та технічно складними. У зв’язку з цим захист мобільних пристроїв має базуватися не лише на антивірусних інструментах, а й на постійному оновленні системи, обережності під час встановлення програм і використанні лише перевірених джерел. Особливої актуальності набуває також впровадження поведінкової аналітики та використання хмарних технологій, які дозволяють виявляти нетипову активність. Тільки поєднання технічних засобів і підвищення цифрової грамотності користувачів може забезпечити ефективний рівень захисту.

2.2 Система безпеки iOS

Після розгляду архітектури безпеки Android, доцільно звернути увагу на іншу провідну мобільну операційну систему — iOS, яка реалізує власні підходи до захисту інформації та контролю над додатками. На відміну від Android, платформа iOS відзначається жорсткішою структурою безпеки, яка базується на суворій ізоляції додатків, обмеженому доступі до системних ресурсів та централізованому управлінні оновленнями. Така архітектура спрямована на зменшення векторів атаки та підвищення загальної стабільності й надійності системи.

Операційна система iOS була спроектована з урахуванням високих вимог до безпеки, зокрема для захисту особистих даних користувачів. Apple реалізує багаторівневу архітектуру безпеки, яка включає в себе механізми захисту на рівні апаратного забезпечення, програмного забезпечення та на рівні операційної системи. Один із основних принципів iOS полягає в тому, що безпека є вбудованою в кожен компонент системи, починаючи від апаратного забезпечення і до програмних додатків, що значно знижує ймовірність успішних атак на пристрій [16].

Однією з основних технологій безпеки iOS є пісочниця (sandboxing), яка ізолює додатки один від одного, обмежуючи їх доступ до чутливих системних ресурсів і даних користувача. Кожен додаток на платформі iOS працює в окремому середовищі, де він не може впливати на інші програми або отримувати доступ до ресурсів без відповідних дозволів. Пісочниця обмежує операції, які можуть бути виконані додатком, знижуючи таким чином ризик шкідливих програм. Це забезпечує безпеку, навіть якщо додаток був скомпрометований: у разі атак чи інших загроз вони не зможуть поширюватися на інші частини системи або додатки. Такий підхід дозволяє ефективно ізолювати шкідливі програми та

обмежити їхній вплив на пристрій. Оскільки пісочниця працює в межах моделі обмеженого доступу, доступ до критичних системних компонентів iOS, таких як файлові системи, мережеві ресурси та апаратні функції, строго контролюється через дозволи, які надаються додаткам лише за потребою [16].

Одним із важливих аспектів захисту є система дозволів iOS, яка обмежує доступ додатків до чутливих даних, таких як фотографії, місце розташування та контакти. Кожен раз, коли додаток намагається отримати доступ до цих даних, користувач отримує запит на дозвіл, що дозволяє йому контролювати, які програми можуть працювати з їхньою особистою інформацією. Цей механізм дозволяє користувачам зберігати контроль над своїми даними та знижувати ризик несанкціонованого доступу [16].

Для забезпечення високого рівня безпеки iOS також використовує шифрування даних як одну з основних технологій захисту. Всі дані на пристрої, включаючи особисту інформацію, зберігаються в зашифрованому вигляді, що робить їх недоступними для сторонніх осіб навіть у разі фізичного доступу до пристрою. Використання технології Secure Enclave гарантує захист ключів шифрування та інших чутливих даних, що додатково підвищує безпеку користувачів. Шифрування є однією з основних функцій, яка захищає дані навіть при спробах доступу через сторонні методи, такі як злому пристрою або витоку інформації [16].

Для захисту персональної інформації користувача в iOS використовується Keychain — вбудований контейнер для зберігання критично важливих даних таких як паролі, токени доступу та криптографічні ключі. Ключовою перевагою цього контейнера є те, що він функціонує у вигляді зашифрованого сховища, куди кожна програма може додавати власні секрети, але не має змоги переглядати вміст інших додатків [17].

На базовому рівні Keychain спирається на тришарову модель безпеки: інтерфейс прикладного програмування (API Layer), рівень шифрування (Encryption Layer) та рівень контролю доступу (Access Control Layer). Перший шар надає розробникам методи для додавання, оновлення та отримання даних. Другий шар відповідає за шифрування, що робить інформацію недоступною, якщо хтось отримає фізичний доступ до файлової системи. Третій шар забезпечує гнучкі політики, які регулюють, за яких умов можна взаємодіяти з даними (наприклад, лише за розблокованого пристрою чи після біометричної автентифікації [17].

При роботі з Keychain розробники використовують стандартні функції, що приймають так звані “запити” (queries), в яких зазначається, який саме елемент шукається, або які дані потрібно додати. Усі операції виконуються через методи, що дають змогу чітко визначати властивості елемента, його доступність і додаткові параметри безпеки. Важливо регулярно перевіряти дані, які повертаються з Keychain, щоб унеможливити зловживання чи помилки в налаштуваннях[17].

Додатковим рівнем безпеки є можливість інтегрувати Keychain із Touch ID чи Face ID. Це дає змогу налаштувати такий сценарій, коли навіть після встановлення певних політик доступу користувач все одно повинен підтвердити свою особу за допомогою біометрії. Крім того, якщо дані зберігаються в Keychain і користувач створює зашифрований бекап у iCloud або iTunes, то після відновлення на новому пристрої ці секретні записи залишаються доступними [17].

При цьому розробники мають бути обережними із синхронізацією чутливих даних через iCloud Keychain. Хоча ця функція може бути зручною для користувачів, котрі хочуть мати однакові паролі на різних пристроях, важливо заздалегідь визначити, які саме дані варто синхронізувати, а які краще тримати лише локально на одному пристрої [17].

Таким чином, iOS Keychain виступає однією з ключових ланок системи безпеки Apple, поєднуючи гнучкі механізми контролю доступу з потужним шифруванням. Для розробників це означає можливість безпечно працювати з конфіденційними даними, дотримуючись найкращих практик — мінімізувати обсяг збереженої інформації, налаштовувати надійні політики доступу та ретельно перевіряти будь-які дані, які повертаються з Keychain. Усе це робить екосистему iOS більш стійкою до зовнішніх загроз і забезпечує високий рівень захисту користувацьких даних [17].

Важко переоцінити роль оновлень системи в забезпеченні стабільної роботи та захисту пристроїв під управлінням iOS. З кожною новою версією операційної системи Apple усуває вразливості, які потенційно могли б бути використані зловмисниками, і водночас удосконалює механізми шифрування, автентифікації та контролю доступу. Регулярне отримання таких оновлень є однією з ключових переваг екосистеми Apple, оскільки користувачі зазвичай отримують актуальні патчі одночасно, без затримок. Це дозволяє значно зменшити вікно для потенційної атаки та підтримувати високий рівень безпеки впродовж усього життєвого циклу пристрою.

2.3 Порівняння мобільних ОС: Android vs iOS

Порівняння безпеки мобільних операційних систем Android та iOS є важливим для розуміння їхніх сильних і слабких сторін. Обидві платформи використовують різні підходи до захисту даних, контролю доступу, шифрування та оновлень, що визначає рівень їхньої стійкості до загроз.

Щоб наочно продемонструвати ключові контрасти між Android та iOS, нижче представлено узагальнену таблицю, яка порівнює основні аспекти безпеки обох платформ.

Таблиця 2.1 – Порівняльна характеристика механізмів безпеки в ОС Android та iOS

Аспект	Android	iOS
Архітектура	Відкрита платформа, заснована на ядрі Linux, що дозволяє модифікацію коду виробниками та розробниками. Це забезпечує гнучкість, але може створювати потенційні ризики безпеки.	Закрита екосистема, розроблена Apple, з обмеженим доступом до вихідного коду. Це дозволяє Apple підтримувати суворий контроль над безпекою та якістю додатків.
Модель безпеки	Використовує модель безпеки, засновану на дозволах, де користувачі повинні надавати додаткам доступ до певних функцій або даних. Ця система може бути вразливою, якщо користувачі неуважно надають дозволи.	Застосовує суворіший підхід до безпеки, зосереджуючись на ізоляції додатків та контролі доступу до даних. Кожен додаток працює в "пісочниці", що обмежує його можливості взаємодії з іншими додатками та системою в цілому.
Управління додатками	Дозволяє встановлення додатків з різних джерел, включаючи сторонні магазини додатків, що може підвищити ризик встановлення шкідливого ПЗ.	Обмежує встановлення додатків лише через офіційний App Store, де всі додатки проходять ретельну перевірку перед публікацією, що знижує ймовірність поширення шкідливого ПЗ.
Оновлення безпеки	Оновлення безпеки залежать від виробників пристроїв та операторів зв'язку, що може призводити до затримок у впровадженні критичних оновлень.	Apple контролює процес оновлення, забезпечуючи швидке та одночасне розповсюдження оновлень безпеки для всіх підтримуваних пристроїв.

Загалом, обидві платформи мають сильні сторони у забезпеченні безпеки. Android надає більше гнучкості та підтримки сторонніх рішень, тоді як iOS пропонує більш контрольоване та уніфіковане середовище, що підвищує загальний рівень захисту.

За даними CVE Details, кількість зареєстрованих вразливостей для Android перевищує аналогічні показники для iOS. Зокрема, у період з 2015 по 2025 рік в Android зафіксовано 1 624 випадки пошкодження пам’яті (Memory Corruption) та 961 випадок переповнення буфера (Overflow), що є найбільш поширеними типами атак. Водночас для iOS ці показники становлять 1 057 та 695 відповідно, що свідчить про меншу загальну кількість критичних уразливостей у системі Apple [18, 19].

Ще однією суттєвою відмінністю є вразливості, пов’язані з валідацією введених даних (Input Validation), які можуть використовуватися для впровадження шкідливого коду або отримання несанкціонованого доступу. У Android таких вразливостей зафіксовано 457, тоді як у iOS – 158, що може вказувати на більш ефективні механізми перевірки введених даних у системі Apple (27, 28). Також варто зазначити, що в Android було зафіксовано 25 випадків SQL-ін’єкцій, тоді як у iOS – лише 2, що підтверджує більшу вразливість платформи Google до атак на бази даних [18, 19].

Значні відмінності спостерігаються і в динаміці вразливостей. У iOS кількість зареєстрованих уразливостей почала суттєво знижуватися після 2020 року, тоді як в Android у 2022 році зафіксовано рекордні 341 випадок пошкодження пам’яті, що свідчить про потенційні загрози, які залишаються актуальними навіть у нових версіях ОС (27, 28). Однак у 2024–2025 роках кількість вразливостей у обох системах різко скоротилася, що може бути пов’язано з покращенням механізмів безпеки та активною політикою оновлень [18, 19].

Ще одним важливим чинником, який впливає на загальний рівень безпеки мобільних платформ, є швидкість реагування на виявлені вразливості. Згідно зі звітом дослідницької групи Google Project Zero, середній час усунення критичних загроз у системі iOS становить 70 днів. Аналогічний показник для Android-пристроїв, зокрема Google Pixel та Samsung, сягає 72 днів. Незважаючи

на незначну різницю в середньому часі, основною відмінністю є те, що Android залежить від багатьох посередників у процесі оновлення, що може затримувати доставку патчів кінцевим користувачам. Централізована модель Apple дозволяє надійніше контролювати процес оновлень і мінімізувати вікно вразливості [20].

Висновки до розділу 2

Проведене дослідження показало, що мобільні операційні системи Android та iOS реалізують різні стратегії безпеки, кожна з яких має свої переваги й недоліки. Android забезпечує гнучкість і ширші можливості для користувача, проте це супроводжується підвищеним ризиком через відкритість платформи та повільніший механізм оновлень. Натомість iOS демонструє більш контрольоване середовище, яке дозволяє ефективніше протидіяти загрозам, але обмежує доступ до системних ресурсів.

Аналіз статистики вразливостей і кількості заблокованих шкідливих додатків підтвердив, що Android залишається більш привабливою ціллю для зловмисників. Разом із тим, ефективність систем захисту в обох ОС багато в чому залежить не лише від технічних рішень, а й від своєчасного оновлення, архітектури доступу та поведінки користувача. Звідси випливає, що безпека мобільного пристрою — це спільна відповідальність розробників, виробників і самих користувачів.

3. Огляд сучасних антивірусних рішень для мобільних операційних систем

3.1. Основні алгоритми захисту

Сигнатурний аналіз є одним із базових підходів, що застосовується в антивірусних системах для виявлення шкідливого програмного забезпечення. Його суть полягає в тому, що кожен відомий зразок загрози має власну цифрову характеристику — сигнатуру, яку можна зберігати у вигляді послідовності байтів або хеш-функції. Антивірусні продукти використовують ці «підписи» для зіставлення з файлами, які скануються, що дозволяє швидко виявляти вже відомі типи загроз [22].

У процесі аналізу програма порівнює вміст кожного перевіреного файлу з базою сигнатур, що постійно оновлюється. Якщо знайдено збіг між сигнатурою з бази та вмістом файлу, система розпізнає його як шкідливий об’єкт і автоматично блокує або видаляє його. Такий механізм забезпечує ефективне розпізнавання знайомих загроз, проте не здатен виявляти нові або модифіковані варіанти шкідливих програм [23].

Однією з головних переваг сигнатурного аналізу є його висока швидкодія та простота реалізації. Оскільки порівняння хешів або послідовностей байтів не вимагає значних обчислювальних потужностей, цей метод дозволяє оперативно виявляти загрози, які вже відомі антивірусній системі. Для кожного зразка шкідливого ПЗ заздалегідь формується унікальна сигнатура — як правило, у вигляді цифрового хешу або характерного фрагмента коду. Під час сканування антивірус перевіряє, чи містить файл відповідності хоча б одній з наявних у базі сигнатур. У разі позитивного збігу загроза блокується, а користувач отримує повідомлення про виявлену небезпеку. Цей підхід не потребує складного аналізу вмісту файлів, тому його застосовують навіть у програмному забезпеченні для пристроїв із обмеженими ресурсами [22].

Попри високу швидкість роботи, сигнатурний аналіз має суттєве обмеження — він не здатен розпізнавати загрози, яких ще немає у базі даних. Це стосується як нових, так і модифікованих зразків шкідливого програмного забезпечення. Якщо файл не має відповідної сигнатури, антивірусна система просто не зможе ідентифікувати його як небезпечний [23].

Особливо вразливим сигнатурний підхід є до так званих поліморфних вірусів, які змінюють свій код при кожному запуску, зберігаючи при цьому ту саму шкідливу функціональність. У таких випадках кожна нова версія може мати унікальну сигнатуру, тож виявлення вимагає створення нового запису в базі для кожної зміни. Це суттєво знижує ефективність традиційного аналізу підписів, особливо в умовах, коли кількість варіантів загроз постійно зростає [23].

Попри ефективність сигнатурного аналізу для швидкого виявлення вже відомих загроз, його обмеження стають очевидними у випадках нових або модифікованих атак. Тому сучасні антивірусні рішення дедалі частіше поєднують цей підхід з іншими, зокрема зі статистичними методами. Така інтеграція дозволяє не лише розширити спектр виявлюваних загроз, а й зменшити кількість хибнопозитивних спрацювань. У подібних системах сигнатурна перевірка зазвичай використовується як перший етап — вона швидко аналізує вхідні дані на наявність збігів із базою відомих шкідливих кодів. Якщо загроза не визначена, активуються більш складні статистичні або поведінкові модулі аналізу, що дозволяє виявити аномалії або підозрілу активність навіть у незнайомих зразках коду.

Наступним рівнем аналізу після базового сигнатурного підходу виступає статистичний контроль мережевої активності. Цей метод базується на оцінці поведінкових параметрів трафіку, зокрема аналізі середніх значень, коливань і відхилень від звичного режиму функціонування системи. Застосовуючи вагові коефіцієнти, система зіставляє нещодавні характеристики з типовими

історичними даними. Якщо зафіксовані суттєві відхилення, це може свідчити про спробу атаки або іншу аномальну активність у мережі [24].

Поєднання статистичних підходів із сигнатурним аналізом дозволяє створити адаптивні системи виявлення загроз. У той час як сигнатури забезпечують оперативне розпізнавання вже відомих зразків шкідливого коду, статистичні методи виступають у ролі додаткового інтелектуального фільтра, що дозволяє виявляти потенційно небезпечні дії навіть без наявної інформації про конкретну загрозу. Така комбінація значно зменшує ризик хибнопозитивних результатів та покращує загальну якість захисту [24].

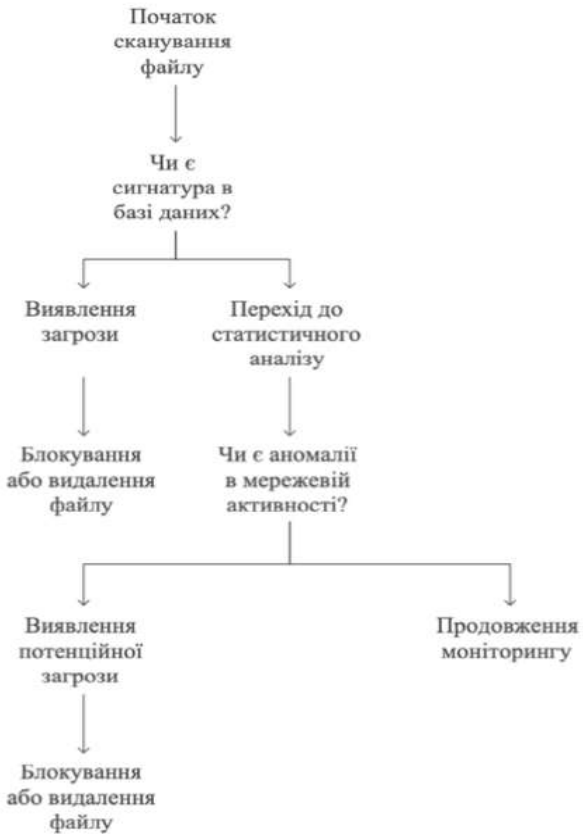

Рис. 3.1 – Логіка роботи комбінованої системи виявлення загроз: сигнатурний та статистичний аналіз

Як видно з рисунку 3.1, комбінований підхід дозволяє спочатку відсіяти відомі загрози за допомогою сигнатур, а потім — задіяти глибший аналіз, якщо загроза не ідентифікована одразу. Завдяки цьому підходу системи безпеки здатні не лише швидко реагувати на добре відомі ризики, а й своєчасно виявляти нові атаки, які ще не описані у сигнатурних базах. Це робить подібні системи більш гнучкими, а захист — ефективнішим у реальному часі.

Оскільки сигнатурний аналіз ефективний лише для відомих загроз, виникає потреба у більш гнучких методах, таких як евристичний аналіз, здатний виявляти ще неідентифіковані або модифіковані шкідливі програми. На відміну від останнього, цей метод не спирається на заздалегідь відомі «підписи» вірусів, а орієнтується на характерні ознаки та шаблони поведінки програм. Саме тому евристика дозволяє виявляти нові або змінені версії шкідливого коду, які ще не потрапили до баз даних загроз [25].

Зазвичай евристичний аналіз реалізується у два послідовні етапи. Спочатку система фіксує поведінку програми в контрольованому середовищі — без активного втручання чи запуску потенційно небезпечних функцій. Потім зібрані дані аналізуються з точки зору наявності аномальних дій: несанкціонованого доступу до системних ресурсів, підозрілих мережевих з'єднань, спроб обійти захисні механізми тощо. Якщо поведінка програми відповідає відомим шаблонам шкідливості, вона розпізнається як потенційно небезпечна навіть без наявної сигнатури [25].

Таким чином, евристичний підхід не лише розширює можливості виявлення загроз, а й значно підвищує рівень адаптивності антивірусного програмного забезпечення до нових викликів, характерних для сучасного кіберпростору.

Хоча евристичні методи значно покращили здатність виявляти нові загрози, для ще глибшого розуміння дій потенційно небезпечного коду все частіше

застосовують поведінковий аналіз, що ґрунтується на оцінці реальних дій програм під час виконання.

Поведінковий аналіз все частіше розглядається як ефективний інструмент виявлення загроз у мобільному середовищі, де класичні підходи можуть виявлятися недостатньо надійними.

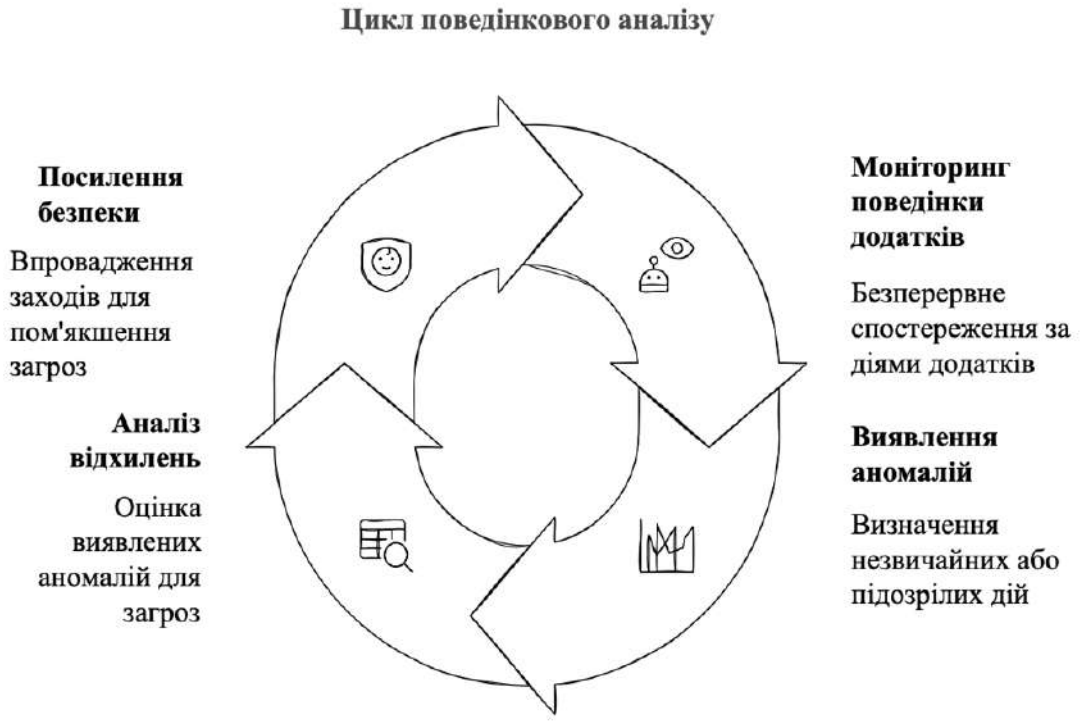

Рис. 3.2 – Цикл поведінкового аналізу: від моніторингу до адаптації системи безпеки

Його ключова перевага полягає в здатності виявляти потенційно шкідливі дії не на основі зовнішнього вигляду програми, а за її реальними діями під час виконання. Це особливо актуально в умовах постійної модифікації зловмисного коду, коли зловмисники намагаються приховати свою присутність, змінюючи структуру файлів або використовують методи обфускації. Поведінковий аналіз дозволяє визначити відхилення від нормальної роботи мобільного додатку — наприклад, атипову взаємодію з системними ресурсами чи надмірну активність у фоновому режимі. [26].

Сучасні дослідження доводять, що такий підхід здатен успішно виявляти навіть ті загрози, які не ідентифікуються сигнатурними чи евристичними методами. Завдяки використанню поведінкових моделей, системи захисту можуть адаптуватися до нових атак, не очікуючи на оновлення бази загроз, що істотно підвищує рівень безпеки пристроїв.

Таблиця 3.1 – Порівняльна характеристика антивірусних алгоритмів у мобільних продуктах

Алгоритм	Основний принцип	Переваги	Недоліки	Приклади використання
Сигнатурний	Виявлення загроз за унікальними "підписами" (сигнатурами) відомих вірусів	Висока швидкість, низьке споживання ресурсів	Не виявляє нові чи модифіковані загрози	Avast, Bitdefender, AVG
Евристичний	Аналіз типових ознак або поведінкових шаблонів, характерних для шкідливих програм	Виявляє невідомі загрози, не потребує сигнатури	Може давати хибнопозитивні результати	TotalAV, Lookout
Поведінковий	Спостереження за діями програми в режимі реального часу	Адаптивність, ефективність проти складних атак	Потребує ресурсів, складна реалізація	Sophos Intercept X, Norton Mobile

Ця таблиця наочно демонструє відмінності між основними алгоритмами антивірусного захисту, їхні переваги, обмеження та приклади використання в популярних мобільних рішеннях.

3.2 Порівняльний аналіз компаній-лідерів на ринку мобільної кібербезпеки

Ринок антивірусного програмного забезпечення для мобільних пристроїв активно розвивається у відповідь на зростання загроз у цифровому середовищі. Провідні компанії пропонують продукти, що поєднують традиційні методи захисту з новітніми технологіями, такими як машинне навчання, поведінковий аналіз і хмарні рішення. У цьому контексті доцільним є аналіз функціональних можливостей, рейтингових позицій і ключових особливостей найпопулярніших антивірусних продуктів. Серед найбільш відомих постачальників антивірусних рішень, орієнтованих на мобільні операційні системи, вирізняються такі компанії, як Bitdefender, Norton, SentinelOne, Panda Security, McAfee, TotalAV та інші.

McAfee спеціалізується на розробці антивірусного програмного забезпечення для широкого спектра пристроїв, у тому числі для мобільних платформ Android та iOS. Їх рішення забезпечують захист від фішингових атак, шкідливих додатків та пропонують інструменти для віддаленого керування пристроєм, що є особливо важливими для мобільних користувачів[36].

Bitdefender відомий своїм високоефективним антивірусним захистом, який використовує передові технології для виявлення загроз. У рамках мобільного сегмента компанія пропонує антивірусні продукти для Android та iOS, серед яких Bitdefender Mobile Security є одним із найпопулярніших [28].

TotalAV пропонує комплексні рішення з антивірусного захисту, орієнтовані на простоту використання та доступність за привабливою ціною. Одним із основних продуктів компанії є TotalAV Mobile Security, який представлений у версіях для Android та iOS[32].

Panda Security займає важливе місце на ринку завдяки своїм рішенням, які поєднують антивірусний захист з інноваційними функціями, зокрема антикрадіжними засобами та інструментами для управління конфіденційністю. Одним із основних антивірусних рішень компанії є Panda Dome Antivirus, представлений у версіях для Android та iOS, який підтримує функції віддаленого блокування, захисту персональних даних та перевірки дозволів застосунків [39].

Отже, кожен із вказаних продуктів має свої особливості, що дозволяє користувачам обирати оптимальне рішення відповідно до індивідуальних потреб — від базового захисту до корпоративного рівня безпеки.

Для узагальнення технічних показників розглянутих антивірусних продуктів доцільно звернутися до результатів незалежного тестування. У таблиці 3.5 наведено порівняльну характеристику мобільних антивірусних рішень для операційної системи Android, що дозволяє оцінити їхню ефективність за ключовими параметрами: рівнем захисту, продуктивністю та зручністю використання.

Таблиця 3.2 – Результати тестування мобільних антивірусних продуктів для Android [27]

Антивірусний продукт	Захист (макс. 6)	Продуктивність (макс. 6)	Зручність використання (макс. 6)	Загальний бал (макс. 18)
Bitdefender Mobile Security	6.0	6.0	6.0	18.0
McAfee Mobile Security	6.0	6.0	5.5	17.5
TotalAV Mobile Security	6.0	6.0	6.0	18.0
Norton 360 Mobile	6.0	6.0	6.0	18.0
Panda Dome Antivirus (Mobile)	5.5	5.5	5.5	16.5

Як видно з наведених результатів, усі представлені продукти демонструють високий рівень ефективності. Зокрема, Bitdefender, Norton та TotalAV досягли максимальних оцінок за всіма критеріями, що свідчить про їхню збалансованість і надійність у мобільному середовищі. McAfee також показав стабільні результати, однак дещо поступається за показником зручності використання. Найнижчі бали отримав Panda Dome Antivirus, що може свідчити про обмежений функціонал або меншу оптимізацію для мобільної платформи. Всі дані наведені станом на січень 2025 року за результатами тестування лабораторії AV-TEST. Отже, отримані показники дають змогу порівняти ключові аспекти роботи антивірусних продуктів та обґрунтовано підійти до вибору оптимального рішення.

3.3 Технічний аналіз ефективності антивірусного захисту мобільних операційних систем

Після виявлення провідних постачальників антивірусного програмного забезпечення для мобільних платформ, доцільно зосередити увагу на технічних характеристиках їхніх продуктів та ефективності захисту.

Bitdefender є одним із провідних світових розробників рішень у сфері кібербезпеки, який пропонує високоефективні засоби антивірусного захисту для різних платформ, включаючи мобільні операційні системи. На офіційному сайті компанії представлена детальна інформація про доступні продукти, використовувані технології виявлення загроз, а також політику регулярного оновлення баз шкідливого ПЗ з метою підтримання актуального рівня захисту користувачів [28].

Продукт Bitdefender Mobile Security забезпечує багаторівневий захист, поєднуючи класичний сигнатурний аналіз із сучасними методами евристичної перевірки та поведінкової аналітики. Завдяки використанню алгоритмів

машинного навчання система здатна виявляти не лише відомі, але й нові модифікації загроз, що ще не були внесені до бази сигнатур [28].

Серед додаткових можливостей слід відзначити інтегрований VPN-сервіс для безпечного інтернет-з'єднання, функцію віддаленого керування пристроєм у разі втрати або крадіжки, а також модуль контролю дозволів для встановлених додатків. Такий комплексний підхід дозволяє забезпечити високий рівень захисту мобільного пристрою без помітного впливу на його продуктивність [28].

Згідно з результатами тестування від незалежної лабораторії AV-Test, рішення Bitdefender Mobile Security для Android (версія 3.3-253105, січень 2025 року) продемонструвало виняткову ефективність, досягнувши рівня виявлення загроз у 99,9%. Продукт також показав відмінні результати за показником відсутності хибнопозитивних спрацьовувань та мінімальний вплив на продуктивність пристрою, що робить його одним із найбільш збалансованих за критеріями «захист–зручність» [29].

Для користувачів macOS, антивірус Bitdefender Antivirus for Mac (версія 10.2-245404, грудень 2024 року, macOS Sonoma) також показав аналогічно високі результати, підтверджуючи ефективність продукту на різних платформах та його здатність забезпечувати потужний захист без шкоди для продуктивності [30].

Крім того, відповідно до звіту AV-Comparatives Awards 2024, рішення Bitdefender отримало високі оцінки за комплексну ефективність, що ще раз підтверджує його лідерські позиції серед антивірусних продуктів. Оцінювання проводилося за кількома критеріями, включаючи точність виявлення загроз та вплив на системні ресурси. Такий збалансований підхід до тестування дозволяє вважати Bitdefender одним із найнадійніших рішень для користувачів, які цінують як безпеку, так і стабільність роботи системи [31].

TotalAV — це міжнародна компанія, що спеціалізується на розробці універсальних рішень у сфері кібербезпеки для різних платформ, включаючи мобільні пристрої. Для пристроїв на базі Android програма забезпечує захист у режимі реального часу, виявляє потенційно небезпечне програмне забезпечення, блокує фішингові ресурси, а також містить модуль VPN, що дозволяє шифрувати з'єднання в публічних мережах. Окрім основних функцій, додаток включає інструменти для оптимізації системи, зокрема очищення від дублікатів файлів і моніторинг витоків персональних даних. Версія для iOS зосереджується на захисті від онлайн-загроз завдяки функціям WebShield, VPN-сервісу та засобам перевірки QR-кодів на наявність шкідливих посилань. Крім цього, програма дозволяє перевірити, чи потрапила особиста інформація користувача до загальнодоступних баз даних унаслідок витоку [32].

За даними AV-Test, антивірусні продукти TotalAV демонструють стабільно високі показники на різних операційних системах. Наприклад, версія ProtectedNet TotalAV 5.9 для macOS Sonoma, протестована у грудні 2024 року, відзначилася високим рівнем виявлення загроз при майже повній відсутності хибнопозитивних спрацьовувань і мінімальному впливі на продуктивність [33].
Аналогічно, мобільна версія TotalAV Mobile Security 3.0 для Android (січень 2025) підтвердила свою ефективність у виявленні шкідливих програм, зберігаючи при цьому низьке навантаження на систему та високу точність роботи [34].

У тестуванні версії для Windows 10 (6.1–6.2, грудень 2024), TotalAV продемонстрував відмінні результати за всіма ключовими критеріями — виявлення загроз, продуктивність та кількість хибних спрацьовувань — підтверджуючи універсальність і надійність свого захисту на десктопній платформі [35].

Таким чином, поєднання позитивної репутації, широкого функціоналу та високих результатів незалежних тестів дозволяє розглядати TotalAV як конкурентоспроможне рішення для всіх основних операційних систем.

Ще однією вагомою компанією у сфері антивірусного захисту мобільних пристроїв є McAfee. Вона має багаторічний досвід у галузі кібербезпеки, а її продукти орієнтовані як на приватних користувачів, так і на бізнес-сегмент. Згідно з інформацією з офіційного сайту, рішення McAfee забезпечують надійний захист від фішингових атак, шкідливих застосунків і пропонують функції віддаленого керування пристроєм. Це особливо корисно у випадках втрати або крадіжки смартфона, коли можна дистанційно заблокувати доступ до даних або видалити їх повністю [36].

У технічному плані продукти McAfee поєднують сигнатурний підхід з евристичним аналізом, що дозволяє ефективно виявляти як відомі загрози, так і нові модифікації шкідливого ПЗ. За результатами незалежних тестувань, зокрема AV-Test, мобільні рішення компанії демонструють стабільний рівень виявлення загроз на рівні 98,5% при мінімальній кількості хибнопозитивних спрацьовувань. Водночас, деяке зниження продуктивності пристрою може пояснюватися наявністю додаткових функцій безпеки, таких як можливість дистанційного керування [36].

Таблиця 3.3 – Результати тестування антивірусних продуктів для Android-пристроїв [29,34]

Антивірусний продукт	Рівень виявлення загроз (%)	Хибнопозитивні спрацьовування (%)	Вплив на продуктивність
Bitdefender Mobile Security (версія 3.3-253105)	99.8	0.2	Низький

Антивірусний продукт	Рівень виявлення загроз (%)	Хибнопозитивні спрацьовування (%)	Вплив на продуктивність
McAfee Mobile Security (версія 8.10-253110)	98.5	0.3	Середній
TotalAV Mobile Security (версія 3.0-253115)	99.0	0.3	Низький

Як видно з наведених даних, усі три продукти продемонстрували високі показники ефективності виявлення загроз — від 98,5% до 99,8%, що свідчить про надійний рівень базового захисту. Найкращий результат показав Bitdefender Mobile Security, який поєднує високий рівень виявлення (99,8%) із мінімальним числом хибнопозитивних спрацювань та низьким впливом на продуктивність. TotalAV також має сильні позиції, поступаючись лише незначно. Продукт McAfee демонструє хороший результат, але має дещо більший вплив на систему, що слід враховувати при виборі захисного рішення для мобільних пристроїв.

Таблиця 3.4 – Результати тестування антивірусних продуктів для macOS [38]

Антивірусний продукт	Рівень виявлення загроз (%)	Хибнопозитивні спрацьовування (%)	Вплив на продуктивність	Загальний бал*
Bitdefender Antivirus for Mac (версія 10.2-245404)	99.2	0.4	Низький	9.2/10
TotalAV 5.9 for Mac	99.0	0.3	Низький	9.0/10
Norton 360 (версія 24.11-245407)	100.0	0.0	Низький	10.0/10

Антивірусні рішення для macOS, представлені у таблиці, демонструють високу ефективність виявлення загроз. Усі продукти мають рівень виявлення на рівні 99% або вище при мінімальній кількості хибнопозитивних спрацювань. Особливо варто відзначити Bitdefender, який, окрім стабільного рівня захисту, має також низький вплив на продуктивність системи. TotalAV також продемонстрував конкурентоспроможний результат, що свідчить про надійність і цього рішення. Додатково варто згадати Norton, який підтвердив свою високу якість захисту, зберігаючи оптимальну продуктивність macOS-пристроїв.

Отже, ефективність антивірусного захисту мобільних пристроїв визначається не лише точністю виявлення загроз, але й ширшим комплексом характеристик, що включає низку взаємодоповнюючих компонентів. Найрезультативніші рішення на ринку поєднують кілька підходів до аналізу — сигнатурний, евристичний та поведінковий, що забезпечує виявлення як вже відомих, так і нових типів шкідливого ПЗ. Оновлення баз загроз у режимі реального часу дозволяє підтримувати захист у актуальному стані, тоді як адаптація програмного забезпечення до обмежених ресурсів мобільних пристроїв гарантує стабільну роботу системи без надмірного навантаження. Вбудовані механізми контролю дозволів, інтеграція з хмарними сервісами репутації, а також освітні інструменти, що попереджають користувача про потенційні загрози, формують цілісний підхід до кібербезпеки. Саме така мультикомпонентна стратегія забезпечує найбільш надійний та стійкий захист у мобільному середовищі.

Висновки до розділу 3

У третьому розділі було здійснено комплексний огляд сучасних антивірусних алгоритмів, які використовуються для захисту мобільних операційних систем, а також проведено їх порівняльний аналіз з точки зору ефективності, гнучкості та технічних характеристик.

Розгляд сигнатурного аналізу підтвердив його високу швидкість роботи та ефективність у випадках з уже відомими загрозами, однак було встановлено його низьку результативність проти модифікованих або нових зразків шкідливого ПЗ. Евристичні методи, навпаки, продемонстрували здатність виявляти невідомі загрози за характерними ознаками, хоча й мають ризик хибнопозитивних результатів. Поведінковий аналіз, що базується на спостереженні за діями програми у режимі реального часу, виявився найбільш гнучким і адаптивним у виявленні складних атак, проте потребує значних ресурсів та складної реалізації.

Значну увагу було приділено комбінованим системам виявлення загроз, які поєднують сигнатурний, евристичний та поведінковий підходи. Такі системи виявилися найбільш ефективними завдяки багаторівневій структурі, що дозволяє реагувати як на відомі загрози, так і на нові варіації вірусів, ще не описані у сигнатурних базах.

Окрім теоретичного огляду, у розділі проведено порівняння конкретних антивірусних продуктів від провідних компаній. На основі незалежного тестування було сформовано таблиці з ключовими показниками: рівень виявлення, кількість хибнопозитивних спрацьовувань та вплив на продуктивність.

Таким чином, антивірусні алгоритми, орієнтовані на мобільні платформи, мають різні характеристики, але їх поєднання в рамках комбінованих систем забезпечує найвищу ефективність захисту в умовах постійно змінюваних кіберзагроз.

Висновки

У результаті виконання курсової роботи було досліджено основні типи загроз, що становлять небезпеку для мобільних пристроїв, а також розглянуто архітектуру безпеки двох провідних мобільних операційних систем — Android та iOS. Особливу увагу було приділено сучасним антивірусним рішенням, принципам їхньої роботи, ефективності виявлення шкідливих програм і впливу на продуктивність пристроїв.

У ході дослідження було встановлено, що безпека мобільних пристроїв залежить не лише від внутрішньої архітектури операційної системи, але й від використання додаткового захисного програмного забезпечення. Найвищий рівень захисту забезпечують багаторівневі підходи, які поєднують сигнатурний, евристичний, статистичний та поведінковий аналіз.

Порівняльний аналіз показав, що кожна система має свої переваги: Android пропонує більше можливостей для налаштування, але водночас є більш вразливою до атак, тоді як iOS забезпечує вищу інтеграцію безпекових механізмів за рахунок закритої екосистеми.

На підставі проведеного аналізу можна рекомендувати користувачам мобільних пристроїв дотримуватися комплексного підходу до кіберзахисту: оновлювати операційну систему, використовувати лише перевірені додатки з офіційних джерел, надавати дозволи додаткам лише за потреби та встановлювати сучасне антивірусне програмне забезпечення, що підтримує декілька методів виявлення загроз.

Проведене дослідження засвідчило, що ефективність антивірусних алгоритмів полягає не лише в точності виявлення шкідливих об’єктів, а й у здатності адаптуватися до нових типів загроз. Поєднання різних методів виявлення, своєчасне оновлення сигнатурних баз, оптимізація антивірусних рішень для

мобільного середовища, контроль дозволів, інтеграція з хмарними сервісами та наявність освітніх функцій у додатках — усі ці компоненти формують комплексний підхід до кіберзахисту. Саме така інтегрована стратегія дозволяє забезпечити ефективне та стійке виявлення шкідливого ПЗ в умовах зростання кількості мобільних загроз.

Список використаних джерел

1. Cisco. What is Cybersecurity? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html
2. Kabanda P., Austin R.J. Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature [Електронний ресурс]. – Режим доступу: https://www.academia.edu/113281835/Confidentiality_Integrity_and_Availability_in_Network_Systems_A_Review_of_Related_Literature
3. OWASP. Mobile Top 10 – 2023 Risks [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-mobile-top-10/2023-risks/
4. Microsoft. What is Malware? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/business/security-101/what-is-malware
5. Dunham K. Mobile Malware Attacks and Defense [Електронний ресурс]. – Режим доступу: https://books.google.com.ua/books?id=Nd1RcGWMKnEC
6. ThreatFabric. Android banking trojan Chameleon is back in action [Електронний ресурс]. – Режим доступу: https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action
7. ThreatFabric. Xenomorph Malware Strikes Again: Over 30+ US Banks Now Targeted [Електронний ресурс]. – Режим доступу: https://www.threatfabric.com/blogs/xenomorph
8. Statcounter Global Stats. Mobile Operating System Market Share Worldwide [Електронний ресурс]. – Режим доступу: https://gs.statcounter.com/os-market-share/mobile/worldwide
9. Statcounter Global Stats. Android Version Market Share Worldwide [Електронний ресурс]. – Режим доступу: https://gs.statcounter.com/android-version-market-share

10. Dubey A., Misra A. Android Security: Attacks and Defenses. – Springer, 2018
11. Android Developers. App Security Overview [Електронний ресурс]. – Режим доступу: https://source.android.com/docs/security/overview/app-security
12. Google. Application Sandbox [Електронний ресурс]. – Режим доступу: https://source.android.com/docs/security/app-sandbox
13. Google Support. Google Play Protect: Overview and scanning [Електронний ресурс]. – Режим доступу: https://support.google.com/accounts/answer/2812853
14. Merit Solutions. 60,000+ Android Apps Delivered Adware to Users' Devices [Електронний ресурс]. – Режим доступу: https://meritsolutions.net/60000-android-apps-delivered-adware-to-users-devices/
15. Doctor Web. Doctor Web's Q3 2024 review of virus activity on mobile devices [Електронний ресурс]. – Режим доступу: https://news.drweb.com/show/review/?i=14912&lng=en
16. Apple. Apple Platform Security Guide [Електронний ресурс]. – Режим доступу: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
17. Cybellium. Mastering iOS Security: A Comprehensive Guide to Learn iOS Security. – Cybellium Ltd, 2023 [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/books/edition/Mastering_iOS_Security/FjXZEAAAQBAJ
18. CVE Details. Apple iPhone OS Security Vulnerabilities [Електронний ресурс]. – Режим доступу: https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
19. CVE Details. Google Android Security Vulnerabilities [Електронний ресурс]. – Режим доступу: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

20. Google Project Zero. A walk through Project Zero metrics [Електронний ресурс]. – Режим доступу: https://googleprojectzero.blogspot.com/2022/02/a-walk-through-project-zero-metrics.html
21. Google. How we fought bad apps and bad actors in 2023 [Електронний ресурс]. – Режим доступу: https://security.googleblog.com/2024/04/how-we-fought-bad-apps-and-bad-actors-in-2023.html
22. Mohanta A., Saldanha A. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. – Apress, 2021 [Електронний ресурс]
23. Skoudis E. Malware: Fighting Malicious Code. – Prentice Hall, 2004 [Електронний ресурс]
24. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system // Cybersecurity and Critical Infrastructure Protection. – 2019 [Електронний ресурс]
25. Malware and Malware Detection Techniques: A Survey // International Journal for Research in Applied Science & Engineering Technology. – 2021 [Електронний ресурс]
26. Zou D., Zhang J., Jin H., Li S. An effective behavior-based Android malware detection system // Security and Communication Networks. – [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/268632930_An_effective_behavior-based_Android_malware_detection_system
27. AV-Test. Mobile Security Test for Android – January 2025 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/mobile-devices/android/january-2025
28. Bitdefender [Електронний ресурс]. – Режим доступу: https://www.bitdefender.com
29. AV-Test. Bitdefender Mobile Security 3.3-253105 for Android, January 2025 [Електронний ресурс]. – Режим доступу: https://www.av-

test.org/en/antivirus/mobile-devices/android/january-2025/bitdefender-mobile-security-3.3-253105/

30. AV-Test. Bitdefender Antivirus for Mac 10.2-245404 for macOS Sonoma, December 2024 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/home-macos/-macos-sonoma/december-2024/bitdefender-antivirus-for-mac-10.2-245404/
31. AV-Comparatives. AV-Comparatives Awards 2024 for Bitdefender [Електронний ресурс]. – Режим доступу: https://www.av-comparatives.org/av-comparatives-awards-2024-for-bitdefender/
32. TotalAV [Електронний ресурс]. – Режим доступу: https://www.totalav.com
33. AV-Test. ProtectedNet TotalAV 5.9 for macOS, December 2024 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/home-macos/-macos-sonoma/december-2024/protectednet-totalav-5.9-245408/
34. AV-Test. ProtectedNet TotalAV Mobile Security 3.0 for Android, January 2025 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/mobile-devices/android/january-2025/protectednet-totalav-mobile-security-3.0-253115/
35. AV-Test. ProtectedNet TotalAV 6.1–6.2 for Windows 10, December 2024 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/home-windows/windows-10/december-2024/protectednet-totalav-6.1--6.2-241616/
36. McAfee [Електронний ресурс]. – Режим доступу: https://www.mcafee.com
37. AV-Test. McAfee Mobile Security 8.10-253110 for Android, January 2025 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/mobile-devices/android/january-2025/mcafee-mobile-security-8.10-253110/
38. AV-Test. Norton 360 24.11 for macOS Sonoma, December 2024 [Електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/home-macos/-macos-sonoma/december-2024/norton-norton-360-24.11-245407/

39. Panda Security [Електронний ресурс]. – Режим доступу: https://www.pandasecurity.com/en/