SECTION: COMPUTER ENGINEERING.

SEKCJA: INŻYNIERIA KOMPUTEROWA.

How to cite: Shkitov, A. (2024). Modern Methods of Information Protection in Mobile Devices Running Android and iOS. *Horizons of Innovation: Conference on Multidisciplinary Trends in Science 2024.* (pp. 221-227). Futurity Research Publishing. https://futurity-publishing.com/horizons-of-innovation-conference-on-multidisciplinary-trends-in-science-2024-2/

Modern Methods of Information Protection in Mobile Devices Running Android and iOS

Шкітов Андрій Анатолійович

Студент, 2 курс, група КІ-22-1а, спеціальність «Комп'ютерна інженерія»

Інститут комп'ютерних технологій Університету «Україна», м. Київ, Україна

Accepted: February 10, 2024 | **Published**: February 27, 2024 | **Language:** Ukrainian

Abstract: In this paper, the author discusses the key aspects of mobile device security, highlighting modern threats and protection strategies that users can apply to protect their personal data and devices. It outlines methods to bolster security, such as consistently updating the operating system and applications, employing distinct passwords, installing apps exclusively from official platforms, activating security options like two-factor authentication, and leveraging remote services for tracking and securing devices. The author underscores the significance of a deliberate security mindset and ongoing preventative actions to maintain the integrity of users' personal data and devices.

Keywords: OS, Android OS, IOS, smartphone, mobile phones, application, information security, information protection tools, information protection methods, security architecture.

Вступ

У нашому сучасному цифровому світі, де мобільні пристрої стали необхідними для повсякденного життя, захист інформації стає надзвичайно важливим. Операційні системи Android та iOS, які працюють на мільярдах смартфонів та планшетів, потребують постійного вдосконалення заходів безпеки. У цій статті ми розглянемо сучасні методи захисту інформації в мобільних пристроях під управлінням цих операційних систем, враховуючи нові виклики та загрози в цифровому середовищі.

Збереження конфіденційності та недопущення несанкціонованого доступу до особистої інформації користувачів є завданням пріоритетним. Постійно зростаюча функціональність мобільних пристроїв супроводжується збільшенням обсягу конфіденційних даних, що робить їх особливо привабливими для кіберзлочинців.

Серед основних проблем, які варто відзначити, це вразливості операційних систем Android та iOS. Незважаючи на заходи безпеки, вони можуть залишатися уразливими перед новими загрозами. Також важливо вивчати нові методи атак та розробляти стратегії для їх запобігання.

Мета дослідження полягає в аналізі сучасних методів захисту інформації на мобільних пристроях з операційними системами Android та iOS та прогнозуванні їхнього подальшого розвитку в контексті сучасних викликів та загроз.

Результати дослідження

У кібербезпеці вивчено захист інформації на мобільних пристроях з операційними системами Android та iOS. Проте, інтегровані аналітичні методи захисту ще досить мало досліджені. Невирішені питання стосуються вразливостей операційних систем та нових методів атак, що з'являються внаслідок постійного розвитку кіберзагроз. Для більш глибокого розуміння ситуації важливо вивчити та проаналізувати існуючі технології захисту, а також розглянути можливості впровадження нових методів, таких як штучний інтелект та блокчейн. Мета статті полягає в інтегральному аналізі сучасних методів захисту інформації на мобільних пристроях та прогнозуванні їх подальшого розвитку в контексті сучасних кіберзагроз.

До основних методів захисту інформації в мобільних пристроях Android та iOS та методів аутентифікації та авторизації відносяться (табл.1):

Таблиця 1

Основні методи захисту інформації в мобільних пристроях Android

Категорія	Метод	Опис
Захист від шкідливих додатків	Google Play Protect	Захист від шкідливих додатків від Google Play Store.
Контроль доступу	Права доступу	Контроль над дозволами для обмеження можливостей додатків.

Шифрування даних	Шифрування даних	Захист інформації на рівні файлової системи.
Зберігання конфіденційних даних	Безпечний елемент	Апаратний елемент для зберігання конфіденційних даних.

Джерело: власна розробка автора

Імплементація обмежень на встановлення програмного забезпечення виключно з авторизованих джерел є стратегічним заходом, спрямованим на зниження потенціалу вторгнення шкідливого програмного забезпечення в мобільні системи (табл. 2). Програмні додатки, отримані з легітимних маркетплейсів, обов'язково проходять детальну перевірку з метою ідентифікації та нейтралізації можливих загроз безпеці перед релізом для загального користування (Завгородній, 2019).

Таблиця 2

Захист інформації та методи аутентифікації в мобільних пристроях Android та iOS

Платформа	Категорія	Метод/Функція	Опис
Android	Обмеження неофіційних джерел	Встановлення додатків тільки з офіційних джерел	Захист від встановлення потенційно шкідливих додатків з неофіційних джерел.
iOS	Захист інформації	App Store Review Process	Строгий процес перегляду додатків перед допущенням до App Store.
		Sandboxing	Робота додатків в обмеженому середовищі.
		Face ID та Touch ID	Біометричні методи аутентифікації.
		Шифрування файлової системи	Захист даних на рівні файлової системи.
		iCloud Security	Додатковий захист для даних з використанням iCloud.
Android & iOS	Методи аутентифікації та авторизації	Різні методи	Перелік включає PIN, пароль, візерунок, відбиток пальця, розпізнавання обличчя, двоетапне підтвердження через додаток, код доступу, та розблокування через Apple Watch.

Джерело : власна розробка автора

Застосування біометричних даних для забезпечення безпеки є ефективним та зручним підходом. Основні види біометричних даних включають:

- відбиток пальця (fingerprint);
- обличчя (face recognition);
- відбиток руки (hand geometry);
- іридіум (iris recognition);
- голосовий аналіз (voice recognition).

Переваги використання біометричних даних для забезпечення безпеки:

- унікальність;
- зручність; висока безпека;
- швидкість;
- можливість мультифакторної аутентифікації.

Двоетапна аутентифікація є важливим аспектом забезпечення безпеки, додаючи додатковий шар захисту. Інтеграція цієї методики рекомендується для захисту важливих облікових записів і зниження ризику несанкціонованого доступу.

Віддалене відстеження та блокування пристрою дозволяє власнику мобільного пристрою віддалено визначати його місцезнаходження, взаємодіяти з ним та забезпечувати захист у випадку втрати чи крадіжки. Основні можливості цієї функції включають віддалене блокування, видалення даних, включення звукового сигналу та навіть фотографування вкрадача (Остапов, 2013).

Використання функцій захисту вбудованих в операційні системи Android та iOS є важливим для захисту особистої інформації та пристрою в цілому в разі втрати чи крадіжки. Функція "Remote Wipe" або "Віддалене видалення" дозволяє власникам віддалено видаляти всі дані на пристрої, запобігаючи несанкціонованому доступу до особистої інформації. Цю функцію слід активувати та налаштовувати для ефективного захисту даних.

Основні переваги та недоліки вбудованих захисних засобів Android та iOS включають (табл.3).

Таблиця 3

Основні переваги та недоліки вбудованих захисних засобів Android та iOS

Особливості	Переваги Android	Недоліки Android	Переваги iOS	Недоліки iOS

Захисні засоби	Google Play Protect; Права доступу; Шифрування даних; Find My Device	Фрагментація оновлень; Можливість встановлення додатків з неофіційних джерел; Можливість додатків вимагати зайвий доступ до даних користувача	Закритість та стандартизація; Face ID та Touch ID; App Store Review Process; Шифрування даних; Find My iPhone	Обмежена гнучкість вибору додатків та сервісів; Вища ціна; Потреба в частіших оновленнях ПЗ

Джерело: власна розробка автора

Вибір між Android та iOS залежить від потреб користувача та його вподобань. Різні виробники мобільних операційних систем, такі як Google (Android) та Apple (iOS), надають різні захисні функції та сервіси для забезпечення безпеки користувачів та їхніх пристроїв. Наприклад, на Android (Google) серед основних захисних функцій є Google Play Protect, права доступу, файлове шифрування, віддалений пошук та блокування пристрою, а також безпечний режим. У той час як на iOS (Apple) важливими функціями є Face ID та Touch ID для біометричної аутентифікації, процес перегляду додатків перед допущенням до App Store, шифрування даних та сервіс Find My iPhone для віддаленого відстеження пристрою. Загально кожна з операційних систем має свої унікальні функції та підходи до забезпечення безпеки. Порівняння рівня безпеки між Android та iOS складне, оскільки обидві мають свої унікальні підходи (табл.4). Важливо враховувати, що безпека також залежить від активного управління користувачем, такого як вчасне оновлення ПЗ та встановлення надійних паролів (Лісовський , 2023)

Таблиця 4

Безпеки мобільного пристрою: переваги та недоліки Android та iOS

Категорія	Android	iOS
Недоліки	Фрагментація та оновлення, тобто різні пристрої отримують оновлення з різною затримкою. Дозвіл на встановлення з неофіційних джерел може збільшити ризик зараження шкідливим ПЗ.	Закрита екосистема та висока вартість можуть обмежувати користувачів. Залежність від оновлень може бути невдоволенням для деяких користувачів.
Переваги		Кращий контроль над апаратним та програмним середовищем; Суворий процес перегляду додатків перед допущенням до App Store;

		Біометричні методи аутентифікації, як от Face ID та Touch ID для зручної та ефективної аутентифікації; Шифрування даних, а саме захист інформації на пристрої та в iCloud.	

Рекомендації для підвищення безпеки :

- Постійно оновлюйте операційну систему та додатки;
- Встановіть сильний пароль, PIN-код чи використовуйте біометричні методи аутентифікації;
- Обмежуйте дозволи додатків та завантажуйте їх лише з офіційних магазинів додатків;
- Активуйте вбудовані служби безпеки, такі як Find My Device чи Find My iPhone;
- Вмикніть шифрування файлової системи на пристрої;
- Уникайте відкриття підозрілих посилань чи завантажень з невідомих джерел;
- Використовуйте віртуальні приватні мережі (VPN) у відкритих мережах;
- **Регулярно робіть резервні копії важливих даних.**

Джерело : власна розробка автора

Для забезпечення безпеки мобільного пристрою, критично важливо здійснювати активне управління програмним забезпеченням та налаштуваннями пристрою. Ефективна стратегія включає активацію автоматичних оновлень операційної системи, що дозволяє пристрою автоматично завантажувати та інсталювати оновлення безпеки. Важливо також регулярно перевіряти доступність оновлень вручну, особливо у випадках, коли автоматичне оновлення не активовано, для забезпечення негайного встановлення критичних оновлень безпеки. Забезпечення актуальності програмного забезпечення додатків через автоматичні оновлення з офіційних магазинів додатків, як Google Play або App Store, є ще однією важливою мірою безпеки. Це допомагає уникнути ризиків, пов'язаних із встановленням ненадійного програмного забезпечення з неавторизованих джерел.

До того ж, критичний аналіз дозволів, які вимагають додатки перед їх встановленням, дозволяє ідентифікувати та уникнути потенційно небезпечних програм, що вимагають надмірного доступу до даних або функцій пристрою. Використання віртуальних приватних мереж (VPN) при підключенні до відкритих Wi-Fi мереж значно підвищує безпеку передачі даних, захищаючи користувача від можливих загроз. Уникнення ненадійних Wi-Fi мереж знижує ризик вразливості пристрою до атак. Активація двофакторної аутентифікації для облікових записів запроваджує додатковий рівень захисту, ускладнюючи несанкціонований доступ. Загалом, ці заходи формують комплексний підхід до захисту мобільних пристроїв, що вимагає від користувачів освіченості та активності у питаннях кібербезпеки.

Забезпечення регулярних оновлень та уважність під час завантаження додатків і обміну даними є ключовими для забезпечення безпеки вашого мобільного пристрою та особистих даних (Гребенюк, 2020)

Висновки

Отже, для забезпечення інтегрованого захисту мобільних пристроїв та конфіденційності особистих даних рекомендується дотримуватись комплексу стратегічних заходів. Пріоритетним є оновлення операційної системи та аплікацій до останніх версій, що включають актуалізовані заходи безпеки. Важливим аспектом є використання унікальних та складних паролів для кожного облікового запису з метою забезпечення їх надійності. Інсталяція додатків має відбуватися виключно з верифікованих джерел, таких як офіційні магазини додатків, з обов'язковим аналізом користувацьких відгуків та політики конфіденційності.

Під час передачі особистої інформації необхідно використовувати захищені з'єднання та уникати підключення до публічних Wi-Fi мереж, які не є надійними. Активація двофакторної аутентифікації слугує додатковим бар'єром для несанкціонованого доступу до облікових записів. Впровадження віддалених служб, що дозволяють відстежувати та блокувати пристрій у випадку його втрати чи крадіжки, є критично важливим. Регулярне створення резервних копій даних забезпечує їх збереження та доступність у випадку непередбачуваних обставин.

Виконання цих заходів сприяє формуванню ефективного механізму захисту мобільного пристрою та особистих даних, знижуючи ризик потенційних кіберзагроз.

Література

Гребенюк, А.М., & Рибальченко, Л.В. (2020). *Основи управління інформаційною безпекою*. Дніпропетровськ державний університет внутрішніх справ.

Завгородній, В.І. (2019). Системне керування інформаційними ризиками. Вибір механізмів захисту. *Проблеми управління*, (1), 53-58.

Захаров, В.П., & Рудешко, В.І. (2015). *Біометричні технології в XXI столітті та їх використання* (2-ге вид., доп.). Львівський державний університет внутрішніх справ.

Лісовський, П.М., Лісовська, Ю.П., & Глушков, В.О. (2023). *Сучасні кібервійни XXI століття: квантові технології*. Видавництво Ліра-К.

Остапов, С.Е., Євсеєв, С.П., & Король, О.Г. (2013). *Технологія захисту інформації*. Видавництво ХНЕУ.