

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Казанский национальный исследовательский технологический университет»**

**(ФГБОУ ВО «КНИТУ»)**

Кафедра «Информационная безопасность»

ПРОЕКТНАЯ РАБОТА

по дисциплине «Теория информационной безопасности и методология защиты информации»

на тему «Аудит информационной безопасности устройств на базе операционной системы Android»

Исполнитель К.М.Галиахметов

(дата, подпись) (И.О. Фамилия)

Руководитель А.А.Алексеева

(дата, подпись) (И.О. Фамилия)

Казань, 2024 г.

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#__RefHeading___1)

[1. Исследование и анализ угроз 4](#__RefHeading___2)

[1.1 Текущие угрозы 4](#__RefHeading___3)

[2. Анализ существующих инструментов и технологий 7](#__RefHeading___4)

[2.1 Антивирусные программы 7](#__RefHeading___5)

[2.2 Защита с помощью криптографии 9](#__RefHeading___6)

[СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ 12](#__RefHeading___8)

ВВЕДЕНИЕ

Мобильные устройства с операционной системой Android пользуются широкой популярностью как в личном использовании, так и в корпоративной среде. Однако, с увеличением числа пользователей и расширением функциональности таких устройств растет и количество угроз, нацеленных на них. Обеспечение безопасности данных и предотвращение несанкционированного доступа становятся первоочередными задачами. В данной работе проводится исследование информационной безопасности Android-устройств, включая анализ современных угроз, обзор существующих методов защиты, а также разработку нового решения для улучшения уровня безопасности.

Цели и задачи:

• Изучение текущего состояния информационной безопасности Android-устройств.

• Анализ существующих инструментов и технологий для обеспечения безопасности.

• Разработка и тестирование собственного решения для улучшения безопасности Android-устройств.

Проект включает исследование, разработку, тестирование и документирование решения для информационной безопасности Android-устройств.

1. Исследование и анализ угроз
   1. Текущие угрозы

Мобильные устройства на базе операционной системы Android подвержены множеству угроз, среди которых:

1. Вредоносное ПО. Вредоносное программное обеспечение представляет собой серьезную угрозу для Android-устройств. Эти программы могут похищать личные данные, изменять системные настройки и причинять вред устройствам пользователей. Вредоносное ПО включает в себя различные типы программ, такие как вирусы, трояны, черви, шпионские программы и рекламное ПО. Эти программы могут проникнуть на устройство через различные каналы, такие как загрузка приложений из ненадежных источников, открытие подозрительных вложений в электронных письмах или переход по вредоносным ссылкам.

Методы обнаружения вредоносных программ включают использование антивирусного программного обеспечения, которое сканирует устройство на наличие известных сигнатур вредоносных программ и удаляет их. Однако этот метод не всегда эффективен против новых или неизвестных угроз. Другой метод обнаружения — это поведенческий анализ, который отслеживает поведение приложений на устройстве и выявляет подозрительную активность. Например, если приложение пытается получить доступ к конфиденциальной информации без явной причины или активно работает в фоновом режиме без ведома пользователя, это может быть признаком вредоносной активности.

Для защиты от вредоносных программ пользователям рекомендуется избегать загрузки приложений из ненадежных источников, не открывать подозрительные вложения в электронных письмах и использовать брандмауэры для фильтрации входящего и исходящего трафика. Брандмауэры могут блокировать доступ вредоносных программ к сети и предотвращать их распространение.

1. Фишинг — это метод социальной инженерии, при котором злоумышленники отправляют поддельные электронные письма или создают фальшивые веб-сайты, чтобы обманом заставить пользователей предоставить свои личные данные, такие как имена пользователей, пароли и номера кредитных карт. Фишинговые атаки часто маскируются под сообщения от доверенных источников, таких как банки, социальные сети или онлайн-магазины. Пользователи, переходя по поддельным ссылкам и вводя свои учетные данные на фальшивых сайтах, могут стать жертвами кражи личных данных.

Для защиты от фишинга рекомендуется использовать спам-фильтры, которые могут блокировать подозрительные электронные письма, не переходить по ссылкам в письмах от неизвестных отправителей, не загружать вложения из непроверенных источников и проверять URL веб-сайтов перед вводом личной информации. Пользователи также должны быть внимательны к мелким изменениям в адресах веб-сайтов и использовать поисковые системы для доступа к известным сайтам, чтобы избежать перехода по поддельным ссылкам.

1. Эксплойты уязвимостей: уязвимости в операционной системе Android или в отдельных приложениях могут быть использованы злоумышленниками для выполнения вредоносного кода с повышенными привилегиями. Например, уязвимости в компоненте WebView, который используется для отображения веб-страниц внутри приложений, могут привести к выполнению вредоносного кода, если реализация этого компонента небезопасна. WebView позволяет приложениям загружать и отображать веб-страницы, но отсутствие навигационных кнопок и адресной строки делает его уязвимым для атак.

Для снижения рисков, связанных с уязвимостями, разработчики приложений должны соблюдать лучшие практики безопасности, регулярно обновлять свои приложения и использовать современные методы защиты, такие как шифрование данных и аутентификация пользователей. Проведение регулярных оценок безопасности и тестирование приложений на проникновение также помогает выявлять и устранять уязвимости.

1. Общественные сети: подключение к общественным Wi-Fi сетям может подвергнуть устройства различным атакам, таким как атаки типа "человек посередине", при которых злоумышленники перехватывают данные, передаваемые между устройством и сетью. Такие атаки могут привести к утечке конфиденциальной информации, включая пароли, номера кредитных карт и личные сообщения.

Чтобы защититься от угроз, связанных с общественными Wi-Fi сетями, пользователям рекомендуется избегать передачи конфиденциальной информации через общественные сети, использовать виртуальные частные сети (VPN) для шифрования трафика, проверять безопасность соединений и избегать подключения к незашифрованным сетям. Также полезно отключать автоматическое подключение к известным сетям, чтобы предотвратить случайное подключение к вредоносным точкам доступа.

Эти меры помогут повысить безопасность Android-устройств и защитить их от множества современных угроз.

1. Анализ существующих инструментов и технологий
   1. Антивирусные программы

Смартфоны стали неотъемлемой частью нашей повседневной жизни, выполняя не только функции связи, но и выступая хранилищем конфиденциальной информации. Эти устройства содержат огромное количество данных, от личных фотографий до финансовых транзакций, что делает их привлекательными целями для киберпреступников. Платформа Android, обладая открытым исходным кодом, предлагает непревзойденную гибкость, но это также накладывает на пользователей необходимость активного управления безопасностью своих устройств.

Рассмотрим ключевые функции, которые делают антивирусные приложения для Android незаменимыми для обеспечения безопасности ваших устройств:

1. Сканирование в режиме реального времени. Эта функция постоянно отслеживает устройство на предмет потенциальных угроз, обнаруживая и нейтрализуя их по мере появления. Это обеспечивает непрерывную защиту вашего устройства, минимизируя риск заражения вредоносным ПО.
2. Защита от фишинга. Антивирусные программы идентифицируют и блокируют попытки фишинга, защищая вас от мошеннических веб-сайтов и электронных писем. Эта функция помогает предотвратить кражу личных данных, защищая вашу конфиденциальную информацию.
3. Безопасность Wi-Fi. Антивирусные приложения предупреждают о потенциальных угрозах при подключении к сетям Wi-Fi, предотвращая перехват данных в незащищенных сетях. Это особенно важно при использовании общественных Wi-Fi, которые часто становятся целью атак злоумышленников.
4. Сканирование по расписанию. Эта функция позволяет настроить регулярное сканирование устройства, обеспечивая постоянную защиту за счет регулярной проверки на наличие новых угроз. Регулярное сканирование помогает своевременно обнаруживать и устранять угрозы, поддерживая высокий уровень безопасности.

Для обеспечения максимальной безопасности вашего Android-устройства в 2024 году, рекомендуется использовать следующие антивирусные приложения:

* Avast Antivirus — Mobile Security & Virus Cleaner предлагает мощные функции защиты, включая сканирование в реальном времени и защиту от фишинга.
* Bitdefender Mobile Security: Известен своей высокой эффективностью и минимальным влиянием на производительность устройства.
* McAfee Mobile Security обеспечивает комплексную защиту, включая функции безопасности Wi-Fi и защиту от кражи.
* Мобильный антивирус Касперского предлагает надежную защиту от различных типов угроз, включая вредоносное ПО и фишинг.

Эти антивирусные приложения помогут вам сохранить безопасность вашего устройства и защитить личные данные от киберугроз.

* 1. Защита с помощью криптографии

Криптография — это процесс преобразования обычного текста (открытого текста) в непонятный текст (зашифрованный текст). Этот процесс обеспечивает защиту данных при их хранении или передаче, делая их доступными только для уполномоченных лиц. Криптография играет ключевую роль в защите данных от кражи и изменений, а также используется для аутентификации пользователей.

Современная криптография основывается на сочетании передовых методов безопасности, которые включают сложные алгоритмы шифрования для кодирования сообщений. Открытый текст преобразуется в зашифрованный текст с использованием алгоритма шифрования, который генерирует ключ шифрования. Получатель должен использовать ключ дешифрования, чтобы восстановить открытый текст из зашифрованного.

Симметричная криптография использует один ключ для шифрования и дешифрования. Отправитель зашифровывает открытый текст с помощью этого ключа и отправляет зашифрованный текст получателю. Получатель применяет тот же ключ для расшифровки зашифрованного текста. Примеры алгоритмов симметричной криптографии включают AES (Advanced Encryption Standard), DES (Data Encryption Standard) и IDEA (International Data Encryption Algorithm). Симметричные шифры могут быть потоковыми или блочными:

* Потоковые шифры: Преобразуют открытый текст в зашифрованный текст побайтно. Примеры: ChaCha, RC4.
* Блочные шифры: Преобразуют открытый текст в зашифрованный текст блоками фиксированного размера. Примеры: AES, DES.

Одним из рисков симметричной криптографии является компрометация общего ключа, что может привести к компрометации всей системы безопасности.

Асимметричная криптография решает проблему совместного использования ключей путем создания пары ключей — открытого и закрытого. Открытый ключ используется для шифрования данных, а закрытый ключ — для их дешифрования. Пример: алгоритм RSA (Rivest-Shamir-Adleman). Представьте, что открытый ключ — это ключ от почтового ящика, который позволяет любому отправить письмо, но только владелец закрытого ключа может это письмо прочитать.

Хэш-функции используют односторонние алгоритмы шифрования для преобразования открытого текста в зашифрованный текст (хэш-значение). Хэш-значения являются уникальными для каждого открытого текста и не могут быть обратно преобразованы в исходный текст. Примеры хэш-функций: SHA-1, SHA-224, SHA-256, SHA-384 и SHA-512.

Типы ключей

* Секретный ключ: используется в симметричном шифровании для шифрования и дешифрования сообщений.
* Открытый ключ: используется для шифрования в асимметричной криптографии.
* Закрытый ключ: используется для дешифрования в асимметричной криптографии.

Криптография в Android основана на архитектуре Java Cryptography Architecture (JCA), которая разделяет интерфейсы и реализацию. Это позволяет включать различных поставщиков безопасности, реализующих наборы криптографических алгоритмов. Большинство интерфейсов и классов JCA определены в пакете Java.security, что обеспечивает гибкость и расширяемость криптографических функций в приложениях Android.

ЗАКЛЮЧЕНИЕ

На основе проведенного анализа текущих тенденций, угроз и существующих решений можно сделать следующие выводы и рекомендации:

* Постоянное обновление системы и приложений - это один из самых простых и эффективных способов защиты от большинства угроз.
* Использование комплексных решений - объединение антивирусных программ, MDM-систем, шифрования и фаерволов для максимальной защиты.
* Повышение осведомленности пользователей - проведение обучающих программ и информационных кампаний для пользователей, направленных на повышение их знаний о киберугрозах и методах защиты.

Эти выводы и рекомендации станут основой для разработки предлагаемого решения информационной безопасности, которое будет рассмотрено в следующем разделе.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1) Avast Mobile Security // Avast URL: https://www.avast.com/en-us/free-mobile-security (дата обращения: 21.05.2024);

2) Kaspersky Internet Security for Android // Kaspersky URL: https://www.kaspersky.com/android-security (дата обращения: 21.05.2024);

3) McAfee Mobile Security // McAfee URL: https://www.mcafee.com/en-us/antivirus/mobile-security.html (дата обращения: 21.05.2024);

4) VMware Workspace ONE // VMware URL: https://www.vmware.com/products/workspace-one.html (дата обращения: 21.05.2024);

5) Norton Mobile Security for Android // Norton URL: https://us.norton.com/products/norton-mobile-security (дата обращения: 21.05.2024);

6) ISO/IEC 27001:2013 - Information security management systems // ISO URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 21.05.2024);

7) NIST Special Publication 800-53 // NIST URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата обращения: 21.05.2024);