УДК 004

Ахмадиева Виола Ф., Ахмадиева Вилена Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ: АНАЛИЗ УГРОЗ И МЕТОДЫ ЗАЩИТЫ

Аннотация. В статье рассматриваются современные угрозы безопасности мобильных устройств, такие как вредоносное ПО, фишинг, утечки данных и атаки на операционные системы. Проведен анализ существующих методов защиты, включая антивирусы, двухфакторную аутентификацию и шифрование данных. Предложена новая концепция использования блокчейн-технологий для повышения безопасности мобильных устройств, которая обеспечивает децентрализованное хранение данных и защиту от несанкционированного доступа.

Ключевые слова: мобильные устройства, угрозы, фишинг, утечка данных, атака, аутентификация, антивирусное программное обеспечение, блокчейн-технологии, уязвимость, шифрование.

Мобильные устройства стали важной частью нашей повседневной жизни. Мы используем их для работы, общения, проведения финансовых операций и хранения личной информации. Однако их широкое распространение привлекает внимание киберпреступников. С увеличением популярности мобильных гаджетов, таких как смартфоны и планшеты, вопросы безопасности этих устройств становятся все более важными. В этой статье мы обсудим ключевые угрозы, связанные с использованием мобильных устройств, а также способы их защиты и предложим новые стратегии для повышения уровня безопасности, включая современные решения.

Проведя анализ угроз безопасности мобильных устройств, можно сделать вывод, что основными угрозами безопасности мобильных устройств являются:

– вредоносные программы (Malware): представляют собой одну из самых серьезных угроз для мобильных устройств. Они могут быть установлены через зараженные приложения, ссылки или даже при подключении к незащищенным Wi-Fi сетям. Они представляют собой вирусы, трояны, шпионские программы и другие виды вредоносного ПО, которые могут украсть данные или повредить устройство. Примерами таких программ могут служить: приложения, маскирующиеся под легитимные, но содержащие вредоносный код;

– фишинг и социальная инженерия: фишинг представляет собой способ обмана пользователей с целью получения их конфиденциальной информации, такой как пароли и номера кредитных карт. Этот процесс может происходить через электронные письма, текстовые сообщения или поддельные веб-сайты, которые выглядят как настоящие;

– уязвимости в операционных системах: мобильные операционные системы, например, Android и iOS, могут иметь недостатки, которые хакеры могут использовать для получения неразрешенного доступа к устройствам. Часто пользователи не обновляют свои устройства своевременно, что повышает вероятность использования этих уязвимостей.

Утрата или кража гаджета: физическая утрата или кража мобильного устройства может стать серьезной угрозой. Если устройство не защищено надлежащим образом, злоумышленник может получить доступ ко всем хранящимся на нем данным:

– утечки данных: представляют собой несогласованный доступ к конфиденциальной информации, хранящейся на мобильных устройствах или в облачных сервисах. В качестве примера можно привести взломы облачных сервисов. Злоумышленники применяют различные техники, такие как фишинг или атаки методом «грубой силы», чтобы получить доступ к учетным записям пользователей в облачных хранилищах;

– атаки на операционные системы: атаки на операционные системы мобильных устройств связаны с эксплуатацией уязвимостей в ОС для получения несанкционированного контроля над устройством. Такие атаки могут быть направлены на системные компоненты и на пользовательские приложения;

– небезопасные приложения: Небезопасные приложения – это программы, которые требуют слишком много разрешений или имеют уязвимости, что позволяет злоумышленникам получить доступ к личной информации пользователя.

Существующие методы защиты от вышеперечисленных угроз, такие как:

– антивирусное программное обеспечение. Применение антивирусного ПО – это один из ключевых способов защиты мобильных устройств от вредоносных программ. Регулярные обновления баз данных антивирусов помогают обнаруживать новые угрозы;

– двухфакторная аутентификация. Двухфакторная аутентификация (2FA) обеспечивает дополнительную защиту при входе в аккаунты. Даже если хакер узнает пароль, ему все равно понадобится второй элемент (например, код, отправленный по SMS), чтобы получить доступ;

– постоянные обновления. Обновление операционной системы и программного обеспечения способствует устранению известных уязвимостей. Пользователям следует понимать важность регулярного обновления своих устройств;

– шифрование данных. Шифрование информации на мобильных устройствах способствует сохранению конфиденциальных данных в случае утраты или кражи устройства. Большинство актуальных операционных систем имеют встроенные возможности для шифрования;

– применение VPN. Подключение к виртуальным частным сетям (VPN) при работе с общественными Wi-Fi сетями способствует защите информации от возможного перехвата со стороны злоумышленников.

Существующие методы не справляются с современными угрозами, потому что они работают изолированно и зависят от действий пользователя, данные методы защиты не адаптированы к новым технологиям (IoT, 5G). Можно сделать вывод, что для поддержания безопасности требуется интегрированная система с использованием ИИ, блокчейна и автоматического устранения уязвимостей.

Внедрение блокчейн-технологий в системы защиты мобильных устройств позволит создать децентрализованную, прозрачную и устойчивую к взлому инфраструктуру для управления данными, аутентификации и защиты от киберугроз. Блокчейн обеспечивает высокий уровень безопасности за счет своей неизменяемости, распределенности и использования криптографических методов.

Основные компоненты системы:

– децентрализованное хранение данных: данные не хранятся на централизованных серверах, исключая риск массовых утечек. Предлагается хранить пароли, ключи шифрования и другие конфиденциальные данные в распределенной сети блокчейн. Пользователь может получить доступ к своим данным только через приватный ключ, а для хакеров доступ будет затруднителен;

– устойчивость к взлому: блокчейн использует криптографические алгоритмы, которые делают данные практически невозможными для подделки. Если злоумышленник изменит данные в блокчейне, то потребуется изменение всех последующих блоков, что сделает атаку экономически невыгодной;

– прозрачность и аудит: операции записываются в блокчейн, что обеспечивает прозрачность и возможность аудита. Пользователь беспрепятственно отследит, кто и когда пытался получить доступ к его данным;

– защита от фишинга: блокчейн позволяет устанавливать подлинность сайтов и приложений через децентрализованные реестры. Пользователь сможет видеть подтверждение легитимности ресурса перед вводом данных;

– удобная и безопасная аутентификация: использование цифровых подписей и смарт-контрактов для аутентификации пользователя. Предлагается осуществлять вход в приложения без передачи паролей через интернет, вместо традиционных паролей использовать цифровую подпись, которая хранится в блокчейне, что исключит риск перехвата;

– контроль доступа: смарт-контракты управляют доступом к данным на основе предустановленных правил. Можно установить ограничение доступа к данным приложения в зависимости от местоположения устройства.

Внедрение блокчейн-технологий в системы защиты мобильных устройств предлагает инновационный подход к обеспечению безопасности данных. Децентрализованное хранение, прозрачность и удобная аутентификация делают блокчейн идеальным решением для защиты от современных киберугроз. Внедрение данной системы способно существенно улучшить безопасность мобильных устройств и гарантировать защиту пользовательских данных.

Защита мобильных устройств продолжает оставаться важной проблемой на фоне увеличения числа киберугроз. Обеспечение безопасности мобильных устройств представляет собой многогранную задачу, требующую усилий как от пользователей, так и от создателей программного обеспечения. Несмотря на имеющиеся риски, использование современных защитных методов и внедрение новых технологий способны существенно улучшить уровень безопасности мобильных устройств. Предложенная концепция использования блокчейн-технологий предлагает инновационный подход к защите данных, обеспечивая децентрализованное хранение, прозрачность и контроль доступа. Необходимо учитывать, что безопасность – это не конечная цель, а непрерывный процесс, который требует регулярного обновления знаний и инструментов.

Список использованных источников:

1. Кузьминых Е.С., Маслова М.А. Анализ основных мобильных угроз и способы защиты от вирусов // Научный результат. Информационные технологии. 2022. № 2. URL: https://cyberleninka.ru/article/n/analiz-osnovnyh-mobilnyh-ugroz-i-sposoby-zaschity-ot-virusov

2. Аннамухаммедова О., Атаев Я., Бегмырадов Д. Безопасность мобильных приложений: лучшие практики защиты личной информации // Вестник науки. 2024. № 10 (79). URL: https://cyberleninka.ru/ article/n/bezopasnost-mobilnyh-prilozheniy-luchshie-praktiki-zaschity-lichnoy-informatsii

Akhmadieva Viola F., Akhmadieva Vilena F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

MOBILE DEVICE SECURITY: THREAT ANALYSIS AND PROTECTION TECHNIQUES

Abstract. This article discusses current security threats to mobile devices, such as malware, phishing, data breaches and attacks on operating systems. It analyzes existing protection methods, including antivirus, two-factor authentication and data encryption. A new concept of using blockchain technology to improve the security of mobile devices is proposed, which provides decentralized data storage and protection from unauthorized access.

Keywords: mobile devices, threats, phishing, data leakage, attack, authentication, anti-virus software, blockchain technology, vulnerability, encryption.