Поляков А.А. Технологии защиты данных на мобильных устройствах как часть комплексной системы защиты объектов информатизации // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 12(50) с. 29–32

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.8

ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ НА МОБИЛЬНЫХ УСТРОЙСТВАХ КАК ЧАСТЬ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Поляков А.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: artpol2001@gmail.com

Современные мобильные устройства, активно используемые в рабочих процессах и корпоративных сетях, становятся важными элементами объектов информатизации. Эта статья рассматривает основные технологии защиты данных, применяемые на мобильных устройствах для предотвращения утечек и несанкционированного доступа. Описаны методы шифрования, биометрическая аутентификация, управление мобильными устройствами и сетевой мониторинг. Эти технологии помогают интегрировать защиту мобильных устройств в общую систему безопасности, создавая многослойную защиту корпоративных данных и повышая общую устойчивость информационной среды к атакам.

Ключевые слова: Мобильные устройства, защита данных, шифрование, биометрическая аутентификация, управление мобильными устройствами, информационная безопасность.

DATA PROTECTION TECHNOLOGIES ON MOBILE DEVICES AS PART OF A COMPREHENSIVE INFORMATION SECURITY SYSTEM

Polyakov A.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: artpol2001@gmail.com

Modern mobile devices, increasingly used in work processes and corporate networks, have become essential components of information infrastructure. This article examines key data protection technologies on mobile devices, aimed at preventing data leaks and unauthorized access. It discusses encryption, biometric authentication, mobile device management, and network monitoring. These technologies contribute to integrating mobile device security into an overall security system, creating a multi-layered defense of corporate data and increasing the overall resilience of the information environment against attacks.

Keywords: Mobile devices, data protection, encryption, biometric authentication, mobile device management, information security.

Введение

В последние годы мобильные устройства стали неотъемлемой частью информационной инфраструктуры компаний, государственных учреждений и частных лиц. Использование смартфонов и планшетов в рабочих процессах открыло множество возможностей для повышения эффективности, но одновременно привнесло и серьёзные риски безопасности. Мобильные устройства могут хранить конфиденциальные данные и предоставлять доступ к корпоративным системам, и это делает их привлекательными целями для киберпреступников, заинтересованных в краже данных, вымогательстве и шпионаже.

Комплексная защита объектов информатизации требует многоуровневого подхода, в котором защита данных на мобильных устройствах занимает значимое место. Обеспечение безопасности данных на этих устройствах включает в себя не только физическую защиту, но и широкий набор технологий, таких как шифрование, аутентификация, управление мобильными устройствами и сетевой мониторинг. Эти методы помогают минимизировать риски и интегрировать мобильные устройства в общую систему защиты информации, обеспечивая безопасность корпоративных данных и непрерывность рабочих процессов.

Технологии защиты данных на мобильных устройствах как часть комплексной системы защиты объектов информатизации

Шифрование данных на мобильных устройствах — один из ключевых методов защиты информации от несанкционированного доступа. При помощи встроенного программного обеспечения создаётся зашифрованное хранилище, доступ к которому возможен только при введении уникального ключа или с использованием биометрии. Шифрование на уровне устройства особенно важно для предотвращения утечек при потере или краже устройства. На сегодняшний день современные операционные системы, такие как iOS и Android, предлагают пользователям возможность включить шифрование и для персональных, и для рабочих данных, что делает эту меру базовым элементом защиты информации[1].

Биометрическая аутентификация вносит весомый вклад в усиление безопасности мобильных устройств. Биометрические данные, такие как отпечатки пальцев и распознавание лица, предоставляют дополнительный уровень защиты и предотвращают доступ третьих лиц. Биометрия отличается от традиционных паролей своей устойчивостью к подделке и одновременно удобством: доступ к устройству можно получить быстрее и проще. Введение биометрической защиты снижает риск взлома, при этом улучшая пользовательский опыт и не снижая уровня безопасности[2].

Системы управления мобильными устройствами (MDM — Mobile Device Management) являются ещё одним неотъемлемым компонентом комплексной защиты информации. MDM позволяет администраторам внедрять корпоративные политики безопасности и управлять устройствами на расстоянии. С помощью этих решений можно контролировать установки приложений, удалённо блокировать или очищать устройства, настраивать параметры безопасности сети. Это позволяет предотвратить несанкционированный доступ к данным и обеспечить соответствие устройств корпоративным стандартам безопасности[3].

Также критически важен сетевой мониторинг и защита от угроз. Мобильные устройства часто подключаются к различным сетям, включая публичные и небезопасные, поэтому риск перехвата данных достаточно высок. Использование VPN (виртуальной частной сети) помогает шифровать сетевые подключения и снизить вероятность утечки данных, особенно при работе в публичных Wi-Fi-сетях. Дополнительные системы безопасности, такие как IDS и IPS (системы обнаружения и предотвращения вторжений), помогают отслеживать подозрительную активность в сети и блокировать потенциальные угрозы до их нанесения вреда[4].

Совокупность всех вышеперечисленных технологий позволяет создать многоуровневую защиту, где безопасность мобильных устройств интегрируется в единую систему защиты информационной инфраструктуры. Шифрование, биометрическая аутентификация, управление устройствами и сетевой мониторинг обеспечивают всестороннюю защиту данных

на мобильных устройствах и помогают снизить риски. Такой подход не только оберегает данные, но и усиливает общую безопасность корпоративной среды, снижая уязвимость перед потенциальными угрозами и обеспечивая пользователям более надёжные и безопасные условия работы[5].

Заключение

Современные мобильные устройства, активно использующиеся для хранения и передачи конфиденциальных данных, требуют серьёзного подхода к защите информации. Технологии защиты данных на мобильных устройствах, такие как шифрование, биометрическая аутентификация, управление мобильными устройствами и сетевой мониторинг, составляют основу комплексной системы защиты объектов информатизации. Эти методы создают многослойную систему безопасности, защищающую устройства как от физических угроз, так и от кибератак, обеспечивая целостность и конфиденциальность данных.

В условиях, когда мобильные устройства становятся важными элементами корпоративной среды, их защита должна быть приоритетом для компаний и организаций. Постоянное развитие технологий защиты данных на мобильных устройствах позволяет минимизировать риски и укрепить общую систему безопасности, что делает их значимой частью комплексной защиты объектов информатизации.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.
3. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
2. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables //Bulletin of the St. Petersburg State University of

Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 61-65.

3. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
5. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.