УДК 621.397.7-182.3

ПРИМЕНЕНИЕ ZERO TRUST ПОДХОДА ДЛЯ МОБИЛЬНЫХ ANDROID-УСТРОЙСТВ В КОРПОРАТИВНОЙ СРЕДЕ

Агапова В.О.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Лихачевский Д.В. – к. т. н., доцент, декан ФКП

Аннотация. В статье рассматривается применение концепции *Zero Trust* для обеспечения безопасности мобильных *Android*-устройств в корпоративной среде. Описаны основные принципы модели *Zero Trust*, её преимущества по сравнению с традиционными подходами безопасности, а также возможности реализации на мобильных устройствах. Проанализированы риски, связанные с использованием *Android*-устройств в корпоративной инфраструктуре, и предложены меры по снижению угроз за счёт интеграции *Zero Trust*.

Ключевые слова: информационная безопасность, мобильные устройства, *Android, Zero Trust*, корпоративная среда микропроцессорная техника, микроконтроллер, электростатический разряд.

Введение. Распространение мобильных устройств, в частности на базе операционной системы *Android*, в корпоративной среде значительно увеличивает поверхность атаки. В условиях гибридной и удалённой работы организации сталкиваются с необходимостью защиты информации за пределами традиционного периметра.

Стандартные модели безопасности, основанные на доверии к внутренней сети, оказываются недостаточными. В этой связи модель *Zero Trust* (ноль доверия), базирующаяся на принципе «никому не доверяй, всегда проверяй», приобретает всё большую актуальность.

Основная часть. Концепция *Zero Trust* была предложена аналитической компанией *Forrester* и получила широкое распространение благодаря своей способности противостоять современным угрозам. В отличие от традиционной модели безопасности, в которой пользователи и устройства внутри периметра считаются доверенными, *Zero Trust* требует строгой верификации каждого субъекта и объекта независимо от их положения в сети.

К основным принципам *Zero Trust* относятся:

– постоянная проверка подлинности и авторизации;

– минимальные привилегии доступа (*principle of least privilege*);

– микросегментация сети;

– контроль и мониторинг всех действий пользователей и приложений;

– адаптивное применение политик безопасности.

В контексте мобильных *Android*-устройств реализация *Zero Trust* сопряжена с рядом особенностей. *Android*, как открытая платформа, отличается высокой степенью фрагментации и наличием множества производителей, что усложняет стандартизацию подходов к безопасности. Однако существуют технические решения, позволяющие внедрить принципы *Zero Trust*:

1 Управление мобильными устройствами (*Mobile Device Management, MDM*) и *EMM* (*Enterprise Mobility Management*) позволяют централизованно настраивать политики доступа, контролировать установку приложений, шифровать данные и применять многофакторную аутентификацию.

2 Использование современных механизмов защиты, таких как *Android Enterprise*, предоставляет организациям инструменты по разделению рабочих и личных данных, управлению приложениями и доступом к корпоративным ресурсам.

3 Интеграция с решениями по контролю доступа на основе идентификационных данных (*Identity and Access Management, IAM*), включая поведенческую аналитику и риск-ориентированную аутентификацию.

Кроме того, важным элементом является постоянный мониторинг состояния устройства, а также его соответствия политикам безопасности. В случае несоответствия – автоматическое ограничение доступа или его блокировка.

Zero Trust подход позволяет:

– значительно снизить риски при потере или компрометации устройства;

– ограничить распространение вредоносных программ внутри корпоративной сети;

– управлять доступом к ресурсам в режиме реального времени;

– повысить прозрачность и подотчетность действий пользователей.

Однако внедрение *Zero Trust* требует комплексного подхода и определённой зрелости информационной инфраструктуры. Необходимо учитывать совместимость решений, пользовательский опыт, затраты на реализацию и сопровождение.

Заключение. Применение *Zero Trust* подхода для мобильных *Android*-устройств в корпоративной среде представляет собой эффективную стратегию противодействия современным угрозам. Несмотря на сложность внедрения, преимущества в виде повышения уровня защищённости, управления доступом и минимизации потенциальных потерь делают этот подход перспективным направлением развития корпоративной информационной безопасности.

Список литературы

1. *Kindervag, J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. – Forrester Research, 2010.*

2. *Rose, S., Borchert, O., Mitchell, S., Connelly, S. Zero Trust Architecture. – NIST Special Publication 800-207, 2020.*

3. *Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M. Privacy issues and data protection in big data: A case study analysis under GDPR. – Computer Law & Security Review, 2018.*

4. *Android Enterprise security white paper. – Google, 2023. URL: https://source.android.com/security/overview*

5. *Zero Trust for Mobile Devices. – National Cybersecurity Center of Excellence (NCCoE), 2022.*

UDC 621.397.7-182.3

APPLYING ZERO TRUST APPROACH TO ANDROID MOBILE DEVICES IN AN ENTERPRISE ENVIRONMENT

Agapova V.O.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Likhachevsky D.V.. – Cand. of Sci., Associate Professor, Dean of the FCAD

Annotation. The article discusses the application of the Zero Trust concept to ensure the security of Android mobile devices in a corporate environment. The article describes the main principles of the Zero Trust model, its advantages over traditional security approaches, and the possibilities of implementation on mobile devices. The risks associated with the use of Android devices in a corporate infrastructure are analyzed, and measures to reduce threats through the integration of Zero Trust are proposed.

Keywords: information security, mobile devices, Android, Zero Trust, corporate environment, microprocessor technology, microcontroller, electrostatic discharge.