УДК - 004.056.53 + 658:004.4.056 + 004.738.5.056 Вестник УрФО № 1(23) / 2017, с. 10–13

**Гузенкова Е. А.**

# *ПРИМЕНЕНИЕ СРЕДСТВ ЗАЩИТЫ ПРИ ВЗАИМОДЕЙСТВИИ МОБИЛЬНЫХ УСТРОЙСТВ С КОРПОРАТИВНОЙ СРЕДОЙ ПРЕДПРИЯТИЯ*

*В статье проводиться анализ вопросов безопасности при использовании мобильного устройства в качестве средства, входящего в состав информационной системы на предприятиях, с помощью которого осуществляется взаимодействие с корпоративной средой предприятия. Рассматриваются вопросы организации доступа мобильных устройств в корпоративную сеть предприятия посредством сети передачи данных с использованием средств шифрования. Даются рекомендации по комплексному обеспечению безопасности информации при использовании мобильных устройств, как часть программно-аппаратного комплекса информационной системы предприятия, что в свою очередь приведет к повышению мобильности сотрудников предприятия, и позволит им в рамках своих должностных обязанностей иметь доступ через мобильные рабочие места к корпоративным информационным системам.*

***Ключевые слова:*** *мобильное устройство, защита информации, программное обеспечение, программно-аппаратный комплекс, передача информации.*

**Guzenkova E. A.**

# *THE APPLICATION OF THE REMEDIES IN THE INTERACTION OF MOBILE DEVICES WITH CORPORATE ENTERPRISE ENVIRONMENT*

*The article analyzes security issues when using mobile devices as a tool that is part of the information system in enterprises, which interacts with corporate enterprise environment. The arrangement of mobile access in the enterprise network through a data transmission network using encryption. Recommendations for integrated information security when using mobile devices as part of hardware-software complex of the enterprise information system, which in turn will lead to increased mobility of employees, and allow them as part of their official duties have access via mobile jobs to corporate information systems.*

***Keywords:*** *mobile device, data protection, software, hardware-software complex, the transmission of information.*

Распространение информационных технологий в современном мире привело к тому, что практически на каждом предприятии происходить автоматизация основной и вспомогательной деятельности. Крупные предприятия не ограничиваются локальным сегментом, и с расширением их сфер деятельности происходит их глобализация. Происходит распределение функциональной нагрузки по филиалам предприятия, за счет взаимодействия структурных единиц предприятия посредством распределенной информационной системы или систем. Современные условия рынка заставляют предприятия осваивать также и мобильную площадку взаимодействия своих сотрудников с корпоративной сетью, посредством организации доступа к информационным системам предприятия за счет создания мобильных рабочих мест, в качестве которых рациональнее всего использовать современные мобильные устройства.

Введение в структуру информационного обмена корпоративной сети создает необходимость дополнительной защиты информации при передаче ее между мобильных рабочим местом и корпоративной сетью.

Защита инфраструктуры, включающей в себя мобильные рабочие места предусматривает, как защиту информации, находящейся непосредственно на мобильном устройстве, так и при передаче ее через сеть передачи данных на сервера, обслуживающие информационную систему корпоративной сети.

Как показывает статистика последнего года, при подключении устройства к корпоративной сети утечка информации конфиденциального характера может произойти как на стадии хранения этой информации непосредственно на устройстве, так и при передаче ее через сеть.

При хранении информации непосредственно на устройстве, возникает угроза проникновения троянских программ на устройство, по статистики компании «Лаборатория Касперского» в 2016 году было обнаружено 1520931 вредоносных установочных пакетов мобильных угроз[1]. Основными способами заражения является использование рекламы, установка мобильных приложений (в том числе с официального магазина Google Play Store). Не смотря на постоянные обновления мобильных операционных систем статистический анализ показывает, что злоумышленники научились обходить защитные механизмы, встроенные в мобильные операционные системы. Самыми распространенными результатами вредоносного воздействия является как похищение или искажение конфиденциальной информации, так и создание помех в работе мобильного рабочего места пользователя (например, шифрование данных и попытка вымогательства выкупа, или развертывания активного рабочего окна поверх остальных рабочих столов программой-злоумышленником).

В банке данных угроз Федеральной службы технического и экспортного контроля были зафиксированы 183 уязвимости, имеющие отношение к операционной системе Android, большинство этих уязвимостей относятся к уязвимостям кода, и лишь небольшая часть из них – к уязвимостям архитектуры[2].

Для защиты от несанкционированного доступа к информации, хранящейся и передаваемой между мобильными устройствами и корпоративной сетью необходимо реализовать комплексный характер защиты.

Среди множества представленных на рынке мобильной связи телефонов, большинство используют мобильные телефоны с операционной системой Android. На уровне клиентской мобильной станции аппаратно-программная реализация может быть создана на основе мобильного устройства со встроенными средствами криптографической защиты информации, работа которых необходимо протестировать до введения в эксплуатацию[3]. Преимуществом такой реализации является возможность сертификации устройства на соответствии требованиям регуляторов (ФСБ России).

Другим вариантом решения защищенных мобильных устройств на базе операционной системы Android может стать реализация программно-аппаратного комплекса, заказанного под нужды организации. Таким решением стало устало производство мобильных устройств по заказу ОАО «РЖД», основными компонентами которого являются батарея, камера, тачскрин, контакты, антенны, мембраны влагозащиты, прокладки и наклейки, предназначенные для защиты мобильного устройства от внешних факторов негативного воздействия. Сама операционная система переработала таким образом, в ней устранено большинство уязвимостей, свойственных стандартной операционной системе Android, в том числе уязвимости, связанные с

возможностью предоставления злоумышленникам прав суперпользователя, в том числе в данной операционной системе установлена система защиты от выхода пользователем в сеть Интернет, блокирована возможность замены сим-карты и возможность добавления или удаления приложений, не требующихся для реализации информационного обмена с корпоративной сетью организации[4]. Для осуществления защиты мобильных устройств необходимо использовать защищенную операционную систему, в качестве которой может использоваться специализированная прошивка, разработанная специально под нужды компании, работающая на основе программной платформы с применением квалифицированной электронной подписи (ЭП) компании, посредством которой, мобильное устройство может взаимодействовать с информационными системами предприятия. За счет применения квалифицированной электронной подписи доступ к функционалу операционной системы мобильного устройства может осуществить только тот сотрудник, право доступа которого подтверждается соответствии с сертификатом ЭП подключенной МЭК. Возможность применения квалифицированной ЭП предоставляет возможность создания механизмов разграничения доступа по работе с информацией, которая в последствии будет передаваться в информационную систему предприятия.

В процессе организации безопасной передачи информации между мобильным рабочим местом (мобильным устройством) и корпоративной средой предприятия (информационной системой) необходимо организовать как безопасность самой мобильной станции, так и реализовать виртуальный канал передачи данных[5].

Первую задачу может решить применение специализированной SIM-карты (Subscriber Identity Module), в которой может содержаться информация о сервисах, необходимых для абонента. Предназначение SIM-карты заключается в том, что абонент и само устройство будут однозначно идентифицированы. При этом каждому абоненту будет присвоен уникальный, международный идентификатор мобильного абонента, который состоит из следующих компонентов:

– трехразрядный код страны;

– двухразрядный код сети;

– десятиразрядный код абонента MSIN (Mobile Subscriber Identity Number).

Доступ к SIM-карте защищен PIN-кодом (Personal Identification Number), который осуществляет блокировку карты, при троекратном не правильном вводе данных.

Безопасность информации мобильного устройства обеспечивается шифрованием и уникальным четырнадцатиразрядным идентификатором аппаратуры мобильной связи IMEI (International Mobile Equipment Identity) который позволяет однозначно идентифицировать мобильное устройство. За счет пограничных шлюзов, обеспечивается защита корпоративной сети от вторжений со стороны злоумышленников. В частности, пограничный шлюз защищает оператора от атак, связанных с подменой адреса. Также для обеспечения безопасной передаче информации, на пограничном шлюзе устанавливается соединение VPN между различными операторами[6].

Внутри сети предприятия, для взаимодействия мобильных устройств подключение пользователей организовано посредством корпоративной сети передачи данных, а все мобильные устройства проходят процесс аутентификации в системе Radius по уникальному серийному номеру, что исключает доступ при использовании SIM карт, номера которых не занесены в реестр для доступа в корпоративную сеть. При этом общественные сети не используются, а сетевой трафик от внешнего сетевого интерфейса к информационным ресурсам организации может циркулировать в открытом виде.

**Примечания**

[1] Унучек Р. Мобильные угрозы // Системный администратор – 2016. – №11 (168). – С. 38-42.

[2] Банк данных угроз информационной безопасности ФСТЭК // Портал ФСТЭКhttp://www.bdu.fstec.ru/vul (дата обращения: 05.05.2017).

[3] Документация АПШК «Континет» // Код безопасностиhttps://www.securitycode.ru/products/apksh_kontinent/documentation/ (дата обращения: 06.05.2017).

[4] Регламент функционирования аккредитованного удостоверяющего центра ОАО «РЖД» утвержденный Директором ГВЦ ОАО «РЖД» 03.032014. – 64 с.

[5] Ожиганова, М.И. Повышение защищенности от несанкционированного доступа компьютерной сети // М.И. Ожиганова, А.В. Колесников, А.Ю. Колодяжная. Новая наука: опыт, традиции, инновации: сборник статей Международной научно-практической конференции (г. Стерлитамак, 24 июня 2015 г.) – Стерлитамак: РИЦ АМИ, 2015. – с. 76 – 78.

[6] Росляков, А.В. Виртуальные частные сети. Основы построения и применения / А.В. Росляков. - М. : Эко-Трендз, 2006. – 304 с.

**ГУЗЕНКОВА Елена Алексеевна**, старший преподаватель кафедры «Информационные технологии и защита информации», ФГБОУ ВО Уральский государственный университет путей сообщения (УрГУПС), 620032 г. Екатеринбург ул. Колмогорова 66. E-mail: sato-hany@yandex.ru

**GUZENKOVA Elena**, Senior teacher the Department "Information technologies and protection of information", Ural State University of Railway Transport (USURT). 620032, the city of Ekaterinburg Kolmogorov 66. E-mail: sato-hany@yandex.ru