УДК Вестник УрФО № 1(19) / 2016, стр. XX–XX

Куц Д. В., Третьяк Н. В., Саруханян Х. С.

РАЗВИТИЕ ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНОГО ДОСТУПА К СЕТИ

Данная статья посвящена развитию технологий обеспечения безопасного мобильного доступа к корпоративной сети в условиях широкого внедрения пользовательских устройств в корпоративную информационную систему. В обзоре уделено внимание использованию MDM/EMM решений, описываются их общие характеристики вне зависимости от производителя продукта, а также рассматриваются основные угрозы, связанные с управлением корпоративной мобильностью. В первую очередь применение таких решений имеет место в коммерческом секторе в связи с недостаточным уровнем защиты, обеспечиваемым MDM/EMM решениями. Дальнейшее использование данных решений, в том числе и в госсекторе, возможно в составе комплексных систем безопасности.

Ключевые слова: *мобильные устройства, мобильные приложения, MDM/EMM решения, концепция BYOD.*

Kuts D. V., Tretiak N. V., Sarukhanyan H. S.

DEVELOPMENT OF TECHNOLOGIES GRANTING SECURE MOBILE ACCESS TO NETWORK

This article describes the development of technologies of secure mobile access to a corporate network in conditions of massive introduction of user devices to a corporate information system. The review concerns the use of MDM / EMM solutions, describes their common characteristics regardless of the product manufacturers, and also introduces common threats faced in corporate mobility management.In the first place, due to insufficient level of protection provided by MDM / EMM, the use of such solutions takes place in commercial sector. The further use of this solutions is possible as a part of complex safety systems, including the government sector.

Keywords: *mobile devices, mobile applications, MDM/EMM solutions, BYOD concept.*

В настоящее время в области информационных технологий стали актуальными такие ключевые направления, как мобильность, корпоративная мобильность, мобильные информационные системы, виртуализация и облачные вычисления и работа с большими массивами данных. Для предприятий, различных организаций и учреждений обеспечение мобильности и дистанционной работы сотрудников, переход к системе электронного документооборота, доступ к своим внутренним информационным ресурсам, проведение удаленных совещаний стало возможно с использованием мобильных устройств и решений.

Электронные коммуникации используются в качестве универсального средства получения и обмена информацией, но в то же вре-

мя, Интернет, являющийся одной из глобальных составляющих электронных коммуникаций, стал полем противоправной деятельности против государства и личности. Значительно увеличились риски и угрозы информационной безопасности, следовательно, важнейшей задачей современного информационного общества стало обеспечение информационной безопасности.

Развитие технологий корпоративной мобильности

Консьюмеризация информационных технологий (внедрение пользовательских устройств в корпоративную информационную систему, доступ сотрудников к внутренней сети и в Интернет с их личных мобильных устройств) и стратегия BringYourOwnDevice (BYOD, Использование персональных устройств в рабочих целях) отражают наиболее распространенные тенденции технологий корпоративной мобильности.

По оценкам компанииGartner, около 90% компаний планируют поддерживать бизнес-приложения на устройствах, принадлежащих конечным пользователям, поскольку это позволит значительно сократить расходы на оборудование[1]. Использование персональных мобильных устройств поможет поддерживатьсвязь с сотрудником после окончания рабочего дня, даст возможность работать со служебной информацией в свободное время.

Компания «Первый БИТ» провела исследование российского рынка, которое выявило ключевые особенности использования мобильных решений для бизнеса. В опросе приняли участие руководители высшего звена, директора и собственники 400 компаний с численностью до 500 сотрудников.

По данным исследования 77% руководителей и собственников бизнеса используют смартфоны и приложения для работы; 7,5% руководителей проводят в офисе практически все рабочее время; 5% заявили, что практически не появляются в офисе, либо не имеют офиса вообще. В среднем руководители и владельцы бизнеса почти половину (42%) рабочего времени проводят вне офиса. Как отмечено, абсолютное большинство руководителей проверяют каждый день показатели бизнеса: информацию о платежах, объем продаж, дебиторскую задолженность и многое другое. Но при этом мы видим, что также большую часть времени современный руководитель проводит вне офиса. Смартфон, оснащенный соответствующими мобильными приложениями, становится необходимым инструментом контроля бизнеса [2].

По отраслевой направленности самыми активными пользователями информационныхтехнологий всегда являются представители финансовых, телекоммуникационных и занимающихся розничной торговлей компаний, а также госсектора. Мобильные приложения для госзаказчика — это специализированные элементы мероприятий, таких как Олимпиада в Сочи, или мобильные версии печатной периодики [3].

Совокупность компонентов корпоративной мобильности можно разделить на три основные составляющие – мобильные устройства компании/сотрудников, мобильное программное обеспечение (ПО) и услуги по созданию мобильных корпоративных решений. Мобильное ПО включает платформы разработки приложений (MobileEnterpriseApplicationPlatform или MEAP), корпоративные мобильные приложения (CorporateMobile Applications или CMA), ПО управления корпоративной мобильностью (Enterprise Mobile Management илиEMM) и ПО управления мобильной безопасностью (Mobile Enterprise SecurityилиMES).

Платформы MEAP реализуют клиент-серверную среду исполнения и инструменты для разработки корпоративных мобильных приложений и упрощают процесс разработки мобильного ПО для мобильных устройств с разными операционными системами (кроссплатформенность).

Мобильные приложения CMA включают средства управления корпоративными ресурсами, ПО автоматизации операционной и производственной деятельности, ПО автоматизации стратегий взаимодействия с клиентами (CustomersRelationshipManagement или CRM) и пр.

Область управления корпоративной мобильностью EMM включает продукты управления мобильными устройствами (Mobile Device Management или MDM), продукты управления мобильными приложениями (Mobile Application Management или MAM), продукты управление мобильным контентом (Mobile Content Management или MCM) и продукты, предлагающие решения, включающие набор функций MDM/MAM/MCM. Контейнерные решения также входят в данную область.

Область обеспечения мобильной корпоративной безопасностиMES имеет определенное перекрытие с областью управления корпоративной мобильностью EMM, потому что часть функций безопасности встроена в EMM-решения.

Мобильная безопасность MES оперирует средствами управления угрозами, включая антивирусы и управление мобильными приложениями;средствами защиты и контроля информации, включая шифрование, системы контроля утечки данных (DataLeak Prevention или DLP) и контейнерныетехнологии по разделению корпоративных и персональных данных; средствами обеспечения конфиденциальности и целостности информации, передаваемой по каналам связи; средствами обеспечения безопасности и управления уязвимостями, включая удаленное стирание информации, блокировку устройств и управление корпоративными политиками.

О ключевых игроках на рынке корпоративной мобильности можно судить по «магическим» квадратам Gartner, где представлены основные поставщики EMM продуктов за 2014 и 2015 годы. Лидерами поставок с положительными оценками как по полноте видения, так и по способности реализациимобозначены компании AirWatchbyVMware, MobileIron, IBM, Citrix, GoodTechnology (в конце 2015 г. Blackberry, отнесенная в квадрате к нишевым игрокам поглотила конкурента GoodTechnology). К бросающим вызов компаниям отнесена SAP. Нишевые игроки – Blackberry, Landeck, Globo. Визионеры – Soti, Microsoft, Sophos [4].Основанное на облачных технологиях MDM решение есть у Cisco. В России существует MDM решение SafePhoneразработанное «НИИ СОКБ» и другие отечественные решения данного класса.

Управление корпоративной мобильностью

Управление мобильностью предприятия (EMM) является интенсивно развивающимся направлением его развития, объединяя действия сотрудников, процессы и технологии на основе применения широкого спектра мобильных устройств, беспроводных сетей и связанных с ними услуг.

Решения класса MDMобеспечивают возможность использовать существующую в компании или организации структуру групповых политик для оснащения мобильных устройств сотрудников. Беспроводное управление мобильными устройствами позволяет администраторам производить обновление или устанавливать приложения на этих устройствах. Виртуальная частная сеть (VPN) мобильных устройств открывает пользователям доступ к данным и приложениям за брандмауэром, одновременно контролируя работающие подключения.Таким образом решения MDM предусматривают определенные ограничения для пользователей и наличие системы контроля в компании или организации.

Мобильными устройствами управлять труднее, чем другим сетевым оборудованием: мобильные устройства подключаются к сети разными способами, используют различные операционные системы (Android, Windows, iOS и т.д.), имеют разный уровень защиты, кроме того их легко потерять из-за небольших размеров. С другой стороны современные мобильные устройства обладают широкими возможностями, которые интересны предприятиям и организациям, а также и самим пользователям. Все указанные факторы усложняют поддержку этих устройств, обеспечение защитыкорпоративных данных при наличииидоступа к важным бизнес-приложениям и клиентским данным илипри потере, краже, неаккуратном использовании самого устройства.

По мере приближения возможностей мобильных устройств к возможностям традиционных сетевых устройств появляется необходимость в управлении мобильными устройствами таким же образом, как и портативными или настольными компьютерами. И одним из решений по управлению мобильными устройствами стало появлениеMDM систем.

MDMэто высоко масштабируемые системы, имеющие возможность поддерживать десятки тысяч устройств и обеспечивающая различные варианты настройки. На стороне сервера в MDM имеются четыре основных компонента системы: сервер-шлюз, сервер управления устройствами, сервер регистрации и SQL Server (сервер баз данных).

Сервер-шлюз как правило устанавливается в граничной сети и служит терминалом для сетевого подключения устройства, проверяет подлинность входящих подключений устройств, предоставляет стабильные IP-адреса для устройств и выполняет другие функции, относящиеся к сетевым подключениям и подключениям устройств.

Сервер управления устройствами является узлом администрирования и управления устройствами, включая применение групповых политик, распространение программного обеспечения по беспроводной связи и стирание памяти устройств. Он работает с существующими контроллерами доменов. Серверы управления устройствами выступают в качестве заменителей сетевых клиентов для устройств, позволяя этим устройствам сообщаться с другими системами.

Сервер регистрации создает объекты доменных служб ActiveDirectory, представляющие мобильные устройства в контроллере домена, позволяя управлять этими устройствами подобно остальным членам домена. Этот сервер также занимается запросами и получением сертификатов для мобильных устройств. Он использует ActiveDirectory как основу для проверки подлинности устройств перед тем, как принимать или выпускать сертификаты регистрации.

Базы данных SQL Server предоставляют хранилище для всей информации, относящейся к настройке устройств, задачам, параметрам состояния и так далее[5].

У разных производителей MDM решений программное обеспечение различается набором функций, но, в целом, можно выделить основные реализуемые возможности:

1) обеспечение доступа мобильного решения к корпоративным информационным системам и базам данных независимо от его поставщика, а также от используемой предприятием информационной платформы, интернет-провайдера или провайдера сотовой связи;

2) синхронизация мобильного решения с корпоративной информационной системой;

3) разделение полномочий администраторов MDM по наборам функций системы и доступа администраторов к управлению устройствами по группам пользователей (применение политик из ActiveDirectory);

4) подготовка к работе, регистрация, и учет используемых устройств, оперативное управление(управление конфигурациями ОС, управление и настройка мобильных приложений, в том числе их инициализация и деинициализация, удаленная очистка, блокировка, оповещение о факте получения root-прав, контроль за текущим статусом и сбойными ситуациямимобильного устройства и пр.);

5) обеспечение работы индивидуальных приложений в соответствии с корпоративными политиками (правила использования личного опознавательного номера (Personal IdentificationNumber, PIN); разрешение/запрет установки приложений и их функций; управление источниками приложений; работа с облачным хранилищем и пр.);

6) аудит, мониторинг и подготовка отчетности — контроль соответствия устройств и приложений корпоративным политикам, а также отслеживание вопросов, связанных с использованием тех или иных сервисов и приложений, создание отчетов по зарегистрированным устройствам, по неактивным устройствам, по клиентским сессиям и пр.;

7) обеспечение безопасности посредством защищенного доступа к средствам совместной работы (управление правами доступа, запрет доступа со взломанных устройств), организации выделенных информационных каналов (VPN-сетей, параметры виртуальных частных сетей мобильных устройств определяют уровень контроля пользователей над их подключениями к такой сети),возможности работы с документами в защищенном файловом контейнере, контроля информационных потоков, шифрования передаваемых данных, удаленного администрирования, возможности уничтожения информации на мобильном устройстве в случае его потери или хищения в случае сохранения его подключения к сети и пр.;

8) техническая поддержка пользователей — оперативное решение специалистами ИТ-отделов проблем использования мобильных устройств сотрудниками организации.

MDM/EMM решения не обеспечивают полноценного функционала, поддерживаемого, например, продуктами класса DLP (защита от потери данных) и IRM (управления правами доступа к информации), но все же они могут обеспечить необходимый уровень безопасности при использовании в определенных условиях мобильных устройств, а в случае необходимости их можно интегрировать в более мощные системы безопасности [6].

Защита корпоративной мобильности

Одним из основных факторов, препятствующих эффективному использованию мобильных устройств в корпоративной среде, являются ограничения со стороны информационной безопасности.

Защита информации на мобильных устройствах основывается на различных вариантах шифрования данных и на использовании методов управления доступом к данным (использование PIN, контроль за временем ожидания и пр.). MDM системы в отличие от DLP-решений не обладают возможностью анализировать данные в состояниях «Передаваемые данные» (data-in-motion), «Используемые данные» (data-in-use), и/или «Хранимые данные» (data-at-rest) по их содержимому. Указанные виды анализа данных имеют решающее значение для выполнения задач контроля, мониторинга и обеспечения целостности данных. MDM-системы при наличии доверенного доступа к устройству и хранимым на нем данным не обеспечивают фильтрацию исходящих коммуникаций или подключаемых съемных носителей – ни по содержимому, ни по контексту пользователя, данных или используемого канала.

В современной ситуации этого недостаточно привыходе данных за пределы контролируемого организацией ИТ-периметра. Источником уязвимостейтакже может быть использование личных почтовых ящиков для работы с корпоративной информацией, копирование данных на домашние ПК, необорудованные достаточными средствами защиты, утеря мобильных устройств и пр.

Таким образом при активном использовании персональных устройств в рабочих целях по всем секторам экономики и в госсекторе, стоит задача защиты собственно данных независимо от физического места их нахождения и поиска баланса между мобильностью сотрудников и информационной безопасностью. Ее решение возможно при условии, что система управления мобильными устройствами MDM/EMM будет использоваться в качестве составного компонента в более широкой, комплексной стратегии обеспечения безопасности данных на мобильных устройствах. MDM-системы следует применять для решения задач общего управления и контроля мобильных устройств, а также для шифрования данных. Одним из решений безопасности данных при использовании мобильных устройств в работе и бизнесе является предоставление доступа к информации любой компании или учреждения через удаленное подключение мобильных устройств через терминальные сессии к виртуальным Windows-средам, которые в свою очередь защищены функционирующей на хосте DLP-системой, обеспечивающей предотвращение неконтролируемых утечек данных. При таком решении не требуется локальное хранение данных на мобильных устройствах, обработка данных в рамках виртуальной Windows-сессии и хранение происходят на сервере компании или учреждения. Сотрудники могут пользоваться выложенными на сервере виртуализации необходимыми приложениями (браузер для выхода в Internet, электронная почта, разрешенная программаобмена мгновенными сообщениями, программа для работы документами и пр. требуемые для выполнения должностных обязанностей приложения), служба информационной безопасности при этом сохранит полный контроль над обрабатываемыми данными. Данный подход называется VirtualData LeakPrevention (VDLP) [7].

Следует также отметить ключевые проблемы, связанные с безопасностью MDM решений. В первую очередь это проблемы с безопасностью самих мобильных устройств. Поскольку большинство политик MDM систем не препятствует установке стороннего софта на устройства (это вызвало бы значительное недовольство пользователей), существуют серьёзные риски, связанные с целым рядом угроз информационной безопасности. Во первых, значительная часть разработчиков ПО под мобильные платформы имеет довольно поверхностное представление об информационной безопасности и не умеют избегать ошибок в программировании, создающих уязвимости в прикладном ПО. Через уязвимое ПО, используемое на мобильном устройстве могут быть реализованы атаки различного типа, нацеленные на получение личной информации или контроля над устройством. Например, некорректная организация межпроцессного взаимодействия в приложениях вследствие ошибок программиста может стать причиной утечки личной информации или коммерчески значимой информации, учетных данных пользователя. Во вторых это риски связанные с наличием вредоносного ПО на мобильном устройстве пользователя. В первую очередь представляют опасность программы класса spyware, т.е. «шпионские программы» или «программные закладки». Благодаря скрытому размещению на устройстве, они позволяют получить доступ к корпоративным ресурсам, т.к. процедуры аутентификации устройства и аутентификации пользователя в MDM системах в этом случае проходят без каких-либо проблем. Конечно, антивирусная защита устройств может дать некоторую гарантию безопасности, но далеко не во всех случаях.

Мобильные устройства также уязвимы, по причине использования сетей стандарта GSM. Этот стандарт использует одностороннюю аутентификацию, т.е. процедуру аутентификации проходит только мобильное устройство, но не базовая станция. Таким образом существует угроза подмены базовой станции злоумышленником, т.е. весь информационный трафик пойдёт через поддельную станцию злоумышленника (см.рис. 1). При использовании технологии VPN, доступа к информационным активам коммерческой организации это не даст, но модификация входящего трафика мобильного устройства может обернуться заражением устройства вредоносным ПО, что открывает уже совсем другие возможности по сбору информации. Также возможен перехват GSMтрафика с устройства по радиоканалу, т.к. криптозащита GSMтрафика недостаточно эффективна. Это позволит злоумышленнику собрать больше информации о устройстве для реализации атаки другого типа. Уязвимым также является интерфейс bluetooth, который позволяет злоумышленнику получить удалённый доступ к устройству (см. рис. 1). Беспроводной доступ с применением технологии wi-fi также имеет ряд проблем с безопасностью. Злоумышленник может, перехватив пакеты аутентификации, выполнить перебор возможных комбинаций пароля. В этом плане уязвим и корпоративный WPA – Enterprise, только для этого требуется поддельная точка доступа (см. рис. 1)

Для защиты мобильных устройств необходимо учитывать специфику различных операционных систем и аппаратных различий устройств различных производителей. Реализовывать грамотно разработанную политику в профилях безопасности мобильных устройств. Клиентская часть MDM систем должна контролировать наличие средств антивирусной защиты, следить за своевременным обновлением ПО, осуществлять многофакторную аутентификацию пользователя и устройства, при доступе к корпоративным ресурсам, осуществлять криптографическую защиту трафика и корпоративных данных, хранящихся на телефоне. Однако, даже применение всех этих механизмов не может дать стопроцентной гарантии защиты. Разумно применять MDM системы на предприятии вместе с DLP и IDS системами.

Резюмируя результаты исследования, можно сказать, что внедрение средств управления использованием мобильных устройств (MDM/EMM) в составе комплексных систем безопасности может оказать решающее влияние на обеспечение легитимности и контроля мобильного доступа к информационным ресурсам компаний и учреждений, а также к системам в рамках принятых политик и регламентов. Однако обязательным условием внедрения данных решений является их использование в рамках комплексной системы защиты информации на предприятии и эволюции самих решений.

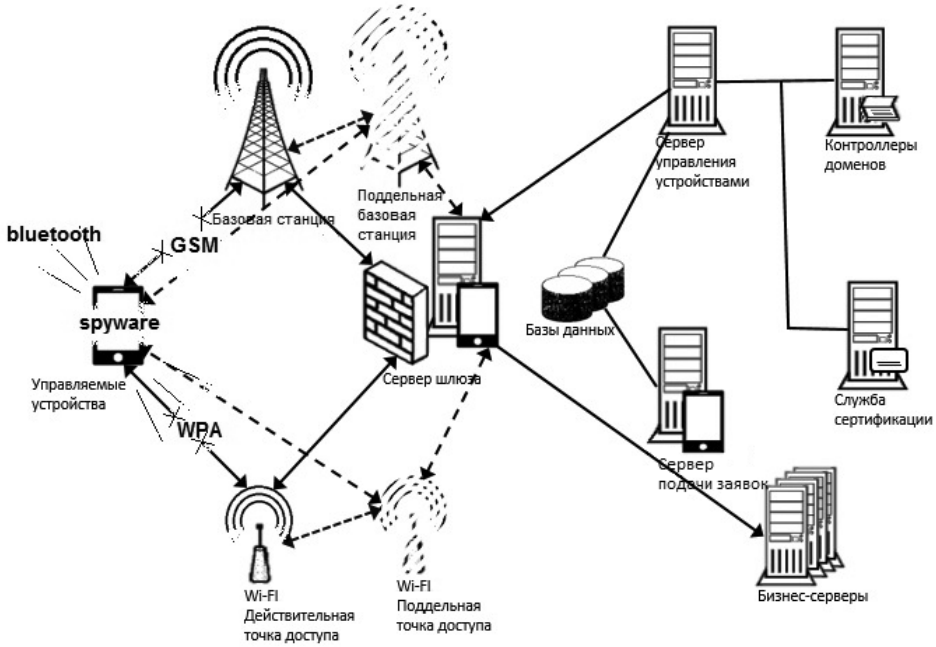

Рис.1. Общая схема потенциальных угроз

Примечания

1. Gartner Says Tablets Are the Sweet Spot of BYOD Programs [Электронный ресурс] // – Режим доступа:http://www.gartner.com/newsroom/id/2909217 (дата обращения: 12.01.2016).

2. «Первый БИТ» изучил, как в российских компаниях используют мобильные приложения. Открытые системы. Новости, №2, 2016 [Электронный ресурс] // – Режим доступа: http://www.osp.ru/news/2016/0221/13031751/ (дата обращения: 22.02.2016).

3. Мобильность в бизнесе 2015. Отраслевая направленность. [Электронный ресурс] // – Режим доступа: http://www.cnews.ru/reviews/mobile_2015 (дата обращения: 22.02.2016).

4. Magic Quadrant for Enterprise Mobility Management Suites // – Режим доступа: https://www.gartner.com/doc/reprints?id=1-2HF4VDW&ct=150608&st=sb(дата обращения: 30.01.2016).

5. МэттФонтейн. Введениев System Center Mobile Device Manager. [Электронный ресурс] // – Режим доступа: https://technet.microsoft.com/ru-ru/magazine/2008.05.scmdm.aspx (дата обращения: 30.01.2016).

6. Колесов А. Управление корпоративной мобильностью. Взгляд Gartner[Электронный ресурс] // – Режим доступа:http://www.pcweek.ru/mobile/article/detail.php?ID=175881 (дата обращения: 30.01.2016).

7. 5 мифов о безопасности BYOD [Электронный ресурс] // – Режим доступа: http://www.devicelock.com/ru/articles/detail.html?ID=2558(дата обращения: 30.01.2016).

Куц Дмитрий Владимирович, старший преподаватель кафедры теоретических основ радиотехники, Института радиоэлектроники и информационных технологий – РтФ, Уральский федеральный университетимени первого Президента России Б.Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail:d.v.kutc@urfu.ru

Третьяк Наталия Вадимовна, магистрант кафедры управления общественными отношениями Института государственного управления и предпринимательства, Уральский федеральный университет имени первого Президента России Б.Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: n.v.tretiak@urfu.ru

Саруханян Ханум Сейрановна, магистрант кафедры управления общественными отношениями Института государственного управления и предпринимательства, Уральский федеральный университет имени первого Президента России Б.Н.Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: khanum.sarukhanyan@urfu.ru

Kuts Dmitry Vladimirovich, seniorteacherof the "Basic Theory of Radio Engineering"department, Institute of Radioelectronics and Information Technologies, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail:d.v.kutc@urfu.ru

Tretyak Nataliya Vadimovna, master of the "Public Administration" department, Institute of Public Administration and Entrepreneurship, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: n.v.tretiak@urfu.ru

Sarukhanyan Khanum Seyranovna, master of the "Public Administration"department, Institute of Public Administration and Entrepreneurship, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: khanum.sarukhanyan@urfu.ru