Безопасность мобильных платформ – настоящее и будущее

Александр ВЕСЕЛОВ,
ведущий инженер, «S-Terra CSP»

Мобильные платформы не роскошь, а необходимость

На заре своего появления смартфоны предлагали рядовому пользователю расширенные мультимедиавозможности по сравнению с обычными средствами коммуникаций. Несколько лет назад планшеты и смартфоны позиционировались как «игрушки» – поиск информации в Интернете, электронная почта, работа с мультимедиаприложениями. Решения для корпоративного сектора встречались довольно редко и по качеству операционной системы и приложений не дотягивали до ноутбуков.

Темпы ведения современного бизнеса буквально заставляют людей постоянно находиться на связи, быть готовыми отреагировать в сжатые сроки на любые виды запросов. А работа с ноутбуком, согласитесь, не всегда удобна – немалый вес и габариты, сравнительно долгая загрузка ОС, емкость аккумулятора.

В последнее время производительность и удобство мобильных платформ возросли, появились решения на любой вкус, увеличилась и степень интеграции в бизнес-процессы. Планшеты и смартфоны всегда готовы к работе, нужно лишь достать устройство из кармана или сумки, при необходимости подключиться к сети и начать работу.

Эти и другие причины привели к тому, что достаточно большая часть рынка «оккупирована» различными гаджетами – планшетами и смартфонами. Мобильные устройства используются для доступа к корпоративным ресурсам, таким как электронная почта, CRM-системы, удаленный рабочий стол, различные ресурсы в облаке. Кроме того, новые модные устройства просочились в Правительство и Государственную Думу, экс-президент и премьер-министр Дмитрий Медведев уже достаточно давно использует iPad и iPhone, а недавно в СМИ появилась информация о том, что скоро iPad будет почти у каждого сотрудника ГИБДД.

Купили, потом защитим

Анализ сложившейся на данный момент ситуации в корпоративном сегменте позволяет заметить тенденцию использования мобильных платформ для доступа к корпоративным ресурсам вопреки политике безопасности компании, а также правовым аспектам информационной безопасности. Обычно так поступают либо системные администраторы, которые, пренебрегая политикой безопасности, могут организовать себе удаленный доступ, либо высокопоставленные сотрудники, которые в силу своего положения позволяют себе нарушать политику безопасности. Кроме того, во многих компаниях увеличивается доля сотрудников, которые хотят использовать планшет вместо ноутбука или получить доступ к корпоративным ресурсам с собственных устройств.

Справедливости ради стоит отметить, что есть попытки по наведению порядка в этой области. Термины BYOD (Bring your own device) и MDM (Mobile Device Management) широко распространились среди экспертов отрасли буквально за последний год. Концепция «Принеси свое собственное устройство»

мнение специалиста

Алексей АНДРИЯШИН,
системный инженер, Fortinet

Перед тем как приступать к выполнению практических действий в рамках концепции BYOD, необходимо оценить риски, которым подвержена компания. Мобильные сотрудники могут представлять реальную угрозу информационной защищенности компании. К рискам можно отнести несанкционированный доступ к информации, хранящейся на устройстве; утечки данных при использовании облачных сервисов, таких как Dropbox или iCloud; регистрация мобильных устройств в корпоративной сети с последующим неэффективным использованием доступа к Интернету.

Если уж компаниям и приходится мириться с наличием личных мобильных устройств, то оставлять этот процесс неуправляемым не рекомендуется. На рынке существует широкий выбор средств MDM, позволяющих эффективно решать задачу управления мобильными устройствами. Одним из эффективных способов доступа к корпоративным данным, таким как электронная почта, календари, контакты, общие документы, является изолированный доступ к данным, или sandboxing. Этот метод исключает возможность утечки данных.

Тем не менее даже при наличии рисков концепция BYOD обладает большим количеством привлекательных свойств. Это и повышение непрерывности бизнеса, повышение лояльности сотрудников, снижение операционных затрат. Несмотря на то что отечественная специфика выбора и использования средств защиты информации обладает рядом сдерживающих факторов, положительная динамика по адаптации популярных мобильных платформ существует, о чем достаточно подробно рассказал автор статьи.

уже используется во многих компаниях, и процесс продолжает набирать обороты. Появились первые отечественные MDM-решения. И все же вернемся к реальности: довольно часто организации для защиты канала доступа к критичным ресурсам используют VPN с применением западных алгоритмов шифрования, например SSL или IPsec на RSA сертификатах. Но если мы подключаемся к системе, в которой обрабатываются персональные данные (или другая конфиденциальная информация, подлежащая защите по закону), то необходимо применять сертифицированные средства криптографической защиты информации (СКЗИ). Вспомним про депутатов, сотрудников министерств и ведомств, врачей скорой помощи, наконец, сотрудников ГИБДД – им нужен доступ к служебным базам данных и другим ресурсам, содержащим конфиденциальную информацию. Российские вендоры наперебой заявляют о наличии VPN-клиента для мобильных устройств, но сертифицированным решением пока могут похвастаться немногие. Причин у такой ситуации множество.

Рассмотрим подробно наиболее популярные мобильные операционные системы и варианты защиты.

iOS

Компания «Инфо-КС» одной из первых получила соответствующий сертификат ФСБ России для VPN-клиента, работающего под операционной системой iOS компании Apple. Однако в сертификате не указана версия операционной системы, а правила пользования и формуляр отсутствуют в открытом доступе. Кроме того, производитель предлагает установку СКЗИ с помощью «jail-break». Данная возможность не документирована компанией Apple и является, по сути, взломом операционной системы, приводящим к потере гарантии производителя. Никто не гарантирует стабильную работу системы после проведения такого взлома, изменения в устройство пользователь вносит на свой страх и риск. Для некоторых пользователей это приемлемо, но для корпоративного, а тем более финансового сектора этот вопрос требует весьма тщательного изучения и анализа, ибо влечет за собой множество дополнительных рисков.

Если пользователь или администратор безопасности все-таки решился на «jail-break», не стоит забывать, что ПО, предназначенное для подобного взлома, появляется значительно позже выхода операционной системы. Например, на всех новых моделях устройств Apple установлена одна из актуальных на сегодняшний день версий iOS (6.0, 6.0.1, 6.1 beta). Для этих версий iOS еще не существует ПО для «jail-break». Следовательно, пользователи самых последних моделей Apple лишены возможности установить VPN-клиент и защитить трафик между своим устройством и корпоративной сетью.

По той же причине придется отказаться от обновлений тем пользователям, на чьих устройствах установлена версия iOS 5.XX. Использование устаревшей прошивки

мнение специалиста

Владимир СМИРНОВ,
генеральный директор, компания «Сигнал-КОМ»

Некоторые протоколы защиты, например SSL/TLS, могут быть реализованы на уровне приложений, и это наиболее перспективный путь их внедрения на мобильные платформы, включающий сертификацию и получение разрешений на вывоз от ФСБ РФ и на распространение через интернет-магазин, например App Store от Apple. Другие протоколы – типа iPSec требуют встраивания криптографии в драйверы, на уровне ядра ОС и могут быть реализованы либо путем «взлома» ОС, либо на уровне официальных договоренностей с вендором. Оценить вероятность последнего пути для IOS и ОС Android достаточно трудно.

мнение специалиста

Антон НОВОСЕЛОВ,
эксперт Центра информационной безопасности, компания «Инфосистемы Джет»

Развитие корпоративного сектора российского рынка мобильных устройств и необходимость соблюдения компаниями действующих законов и политик безопасности привели к существенному росту спроса на защиту, адаптированную для портативных устройств. Более того, когда речь идет, например, о защите персональных данных, без использования сертифицированных по требованиям Регуляторов средств обойтись все-таки нельзя.

Многие производители средств защиты информации, включая отечественных, уже вышли на рынок с собственными продуктами, позволяющими обезопасить мобильные устройства под управлением ОС iOS и Android. Предлагаемые средства имеют ряд ограничений, связанных прежде всего с необходимостью получения привилегированного доступа к ресурсам устройства (так называемое «рутование» или «jail-break»), что является одним из наиболее критичных с точки зрения безопасности моментов.

Что касается предлагаемых сертифицированных средств: в настоящий момент, например, представлено всего несколько сертифицированных средств защиты, которые могут использоваться для реализации защищенного удаленного доступа мобильных устройств к корпоративным ресурсам компании. Но все они также имеют ограничения, связанные с необходимостью привилегированного доступа к ОС.

Плохо это или хорошо? Насколько необходимо? В части отсутствия проблем совместимости и сохранения гарантии на устройство все же стоит ожидать результатов благотворного сотрудничества с производителями мобильных устройств. Относительно информационной безопасности: операции, требуемые для контроля над ОС мобильного устройства, приводят к необходимости получения дополнительных привилегий доступа, не предусмотренных изначально для приложений ОС iOS и Android из соображений безопасности. Установку на устройство «доверенных» сертифицированных программных средств защиты, пусть даже с использованием «рутования» или «jail-break», можно охарактеризовать как вполне оправданную процедуру. Этот «взлом» заключается в установке в системную память устройства программы, реализующей возможность привилегированного доступа. Опыт зарубежных производителей средств защиты (например, решений MDM) показывает, что использование указанного метода не создает «дыру» в безопасности мобильного устройства, а позволяет заменить «недоверенные» средства защиты ОС на «доверенные», реализуемые сертифицированным средством. При этом устройство может быть приведено в соответствие с требованиями действующих законов и политик безопасности.

мнение специалиста

Алексей ЛЫСЕНКО,
начальник отдела развития бизнеса интегратора «Техносерв» по направлению информационная безопасность

Использование различных мобильных устройств для доступа к корпоративным ресурсам все чаще становится головной болью для специалистов по ИБ. Преимущества работы в корпоративной сети с мобильных устройств очевидны, особенно для менеджмента высшего звена. Но возникает ряд рисков, связанных в первую очередь с перемещением важных корпоративных данных различного характера на мобильные устройства и возможностью компрометации данных в случае, например, утери смартфона или заражения вредоносным ПО. Для таких запросов есть решения, построенные на базе платформ ведущих разработчиков на рынке защиты мобильных устройств, например компании Iron Mobile, позволяющие гибко настраивать политики конфиденциальности для устройств – вплоть до запрета использования встроенной фотокамеры при нахождении в здании офиса, которое определяется по GPS-координатам. Стоит отметить, что пользователь самостоятельно может как установить клиентскую часть решения из глобального репозитория программ, так и удалить его и вернуть себе возможность использовать свой смартфон в привычном личном общении, поскольку доступ к корпоративной сети будет закрыт, а конфиденциальная информация удалена. Эти же процедуры при необходимости (например, потере аппарата) может сделать удаленно системный администратор или сам пользователь, даже если SIM-карта на мобильном устройстве была заменена. Обеспечивается контроль не только над информацией, но и телефонными звонками и объемами передаваемых данных, особенно в роуминге, что позволит компании быстро окупить затраты на внедрение такой системы.

очень часто приносит пользователю массу неудобств.

О скорой сертификации СКЗИ для iOS заявила и компания «КриптоПро». Установка криптопровайдера планируется только в составе приложения. Основным способом распространения предполагается поставка через разработчиков приложений. На сегодняшний день в этом направлении работают несколько компаний. Сертификат ФСБ России для «КриптоПро CSP» под данную операционную систему ожидается в ближайшее время.

Компания «Аладдин Р.Д.» пошла немного другим путем и представила на PKI-форуме новый считыватель смарт-карт для устройств Apple, который даст возможность владельцам iPad и iPhone использовать квалифицированную электронную подпись. Решение позволяет обойти архитектурные ограничения платформы iOS, связанные с ее закрытостью и монолитностью кода приложений.

Android

Ситуация с ОС Android во многом аналогична ситуации с iOS, но имеет свои особенности. В версиях 2.2.x, 2.3.x и 3.x не была обеспечена совместимость драйверов для устройств различных производителей. Ядро системы может претерпевать серьезные изменения в ходе обновлений даже в рамках одной модели и версии ОС. В версии 4.x проблему постарались решить. Возможно, это поможет разработчикам средств защиты и позволит упростить сертификацию.

На сегодня у многих производителей СКЗИ есть клиенты безопасности для ОС Android. Устанавливаются они на конкретные модели устройств под управлением определенной версии операционной системы. Для установки требуется получение административного доступа («рутование») – это тоже является взломом операционной системы и, как и в случае с устройствами Apple, ведет к спорным ситуациям с гарантией и усложнению сертификации. Сертифицированного продукта для мобильных платформ на базе ОС Android на данный момент не существует.

Хотя перспективы у устройств на базе ОС Android довольно радужные.

В 2013 г. на рынке можно ожидать несколько полноценных сертифицированных СКЗИ как минимум от трех лидеров рынка: «Код Безопасности», «С-Терра СиЭсПи» и «Инфо[illegible]КС».

И все же выход есть...

Российские разработчики СКЗИ нацелены на сотрудничество с производителями современных мобильных устройств – Apple, Samsung, HTC и др. Добавление соответствующих драйверов и приложений производителем непосредственно в прошивку устройства решило бы проблему с необходимостью взлома операционной системы и ее дальнейшего обновления стандартными средствами. Более того, такое решение можно было бы смело и уверенно сертифицировать. Для того чтобы сделать этот шаг, отечественным разработчикам необходимо иметь доступ к исходным кодам мобильных операционных систем. Но, к сожалению, лидеры рынка мобильных устройств явно не торопятся выходить на такой уровень сотрудничества с разработчиками российских СКЗИ.

В качестве альтернативного пути можно рассматривать разработку собственных защищенных планшетов на базе Android. В таких устройствах необходимый набор программ и средств защиты предустанавливается производителем. Сделав данное устройство корпоративным стандартом, можно получить единообразное решение для корпоративных мобильных пользователей с реальной перспективой сертификации решения в целом. Подобное решение есть у компании «Код Безопасности» – «Континент Т10», но оно пока не сертифицировано.

Рассматривая рынок мобильных устройств, нельзя обойти вниманием еще одну операционную систему, на базе которой в последнее время появляется все больше смартфонов и планшетов. Это ОС Windows. С выходом свежей версии, Windows 8, на рынке ожидается резкое увеличение количества подобных устройств. Ситуация с защитой информации для новой системы хорошо прогнозируема – о технологической совместимости своих продуктов с новой операционной системой уже

мнение специалиста

Дмитрий УШАКОВ,
руководитель отдела по подготовке и внедрению технических решений корпорации Stonesoft Russia

1. Достаточно сомнительной и нецелесообразной представляется трата бюджетных средств именно на дорогие американские i-устройства, когда на рынке есть гораздо более дешевые их корейские и китайские аналоги на базе ОС Android, ничем не уступающие в плане основной функциональности.

2. Главная проблема использования мобильных платформ помимо контроля политик безопасности сводится еще и к ограниченности применения на них корпоративных приложений. Согласитесь, сложно представить бухгалтера, сводящего отчет в 1С на 7-дюймовом планшете. Аналогичная ситуация и со среднестатистическим пользователем: подключился он к сети по защищенному каналу, а дальше что? Для почты у него есть предустановленный клиент с поддержкой AcitveSync/Lotus Notes Traveller/IMAP/POЗ/SMTP, для доступа к корпоративному порталу с информацией о сотрудниках (если ее нет в почте), новостях, другой информации – браузер, а еще? А больше, как показывает практика, в 90% и не нужно. В автомобиле/поезде/самолете или на вокзале вряд ли кто-то будет работать со сложным приложением. Особенно с учетом небольших возможностей точного позиционирования и размеров экрана, да и совместная работа с теми же офисными документами сегодня поддерживается электронными системами документооборота через общедоступный веб-интерфейс. Таким образом, основным набором приложений для мобильных платформ будут и остаются серфинг страниц Интернет и почта.

3. Получить криптографический модуль на устройстве проблемно по целому ряду причин – как технических (связанных с особенностями архитектуры самой платформы), так и организационных (экспорт СКЗИ без специального разрешения запрещен).

4. Любое мобильное устройство становится мобильным, только если у него есть возможность сохранить связность, будучи отключенным от проводов. Поэтому любой телефон, имеющий интегрированные GSM/3G/LTE-модули, а также средства работы с Wi-Fi, потеряет к себе интерес, когда эти средства будут заблокированы. Таким образом, сертификация таких устройств целесообразна, только если данное ограничение будет снято.

5. При организации доступа не стоит забывать про качественную аутентификацию. Опять же работа с сертификатами на мобильных платформах представляет большие сложности, поэтому для них следует использовать альтернативные надежные методы, например одноразовые пароли. А чтобы не мучиться с дополнительными аппаратными токенами, гораздо удобнее использовать программные, устанавливаемые прямо на мобильное устройство (и защищаемые от компрометации паролем или PIN-кодом).

мнение специалиста

Сергей КОНОШЕНКО,
директор департамента информационной безопасности ООО «КАБЕСТ», группа «Астерос»

Внедрение решений MDM (Mobile Device Management) и MS (Mobile Security) является важной частью общей стратегии обеспечения безопасности информации компании при использовании мобильных устройств. Данные системы позволяют контролировать мобильные устройства, имеющие доступ к корпоративным сервисам, способствуют снижению рисков, связанных с утечкой конфиденциальной информации. Разработчики решений, лидеры рынка, такие как MobileIron, McAfee, AirWatch, Symantec, Good Technology и другие, постоянно совершенствуют подходы и продукты, удовлетворяя растущий спрос на подобные услуги.

Наиболее остро в настоящий момент стоит проблема использования криптографических алгоритмов для защиты передаваемой информации. Необходимость применять сертифицированные ФСБ России решения по криптографической защите данных ограничивает или существенно затрудняет использование систем MDM и MS зарубежных производителей. В первую очередь ограничения касаются государственных организаций и ведомств, а также компаний, которые в силу специфики деятельности обрабатывают и передают информацию, защищаемую в соответствии с законодательством РФ (например, персональные данные). Отечественные разработки также представлены на российском рынке, однако их возможности не в полной мере могут составить конкуренцию ведущим мировым решениям. Таким образом, потенциальные заказчики встают перед выбором: использовать решение с максимальными функциональными возможностями и исключать передачу информации, защита которой необходима по законодательству, или ограничивать себя в возможностях, обеспечивая при этом легитимность передачи защищаемой информации.

мнение специалиста

Дмитрий ГУСЕВ,
ОАО «ИнфоТеКС»

Для увеличения степени понимания читателями тех задач и вопросов, которые встают перед нами, разработчиками отечественных СКЗИ для мобильных платформ, имеет смысл кратко рассказать об истории создания ViPNet Client iOS. Данному продукту уже более полутора лет, однако только к середине 2012 г. нам удалось завершить работы по его сертификации в ФСБ России по требованиям к СКЗИ класса КС1. Почему так долго и такой низкий (наименьший из возможных) класс безопасности? Основная проблема – закрытость операционной системы iOS. Компания Apple сделала все возможное, чтобы сторонние разработчики (не будем брать в расчет американские компании – это уже из разряда дел семейных) не могли разрабатывать и устанавливать свои продукты на системный уровень ОС. По словам Apple, это было сделано исключительно ради заботы о безопасности пользователя. Все сторонние приложения должны использовать только декларированный Apple набор функций и библиотек (API) и устанавливаться в iPad/iPhone только через «правильный» механизм Apple Store. Как следствие, все разработчики системных приложений, которым не хватает данного API, включая разработчиков средств безопасности низкого уровня, к которым и относятся VPN-клиенты для защиты и фильтрации IP-трафика, сразу же оказались за рамками «правового» поля Apple. Но, как известно, ничто так не мотивирует программистов к эффективной работе, как попытки других программистов как-то ограничить первых в их желании делать свою работу. Так и появился jailbreak...

Наша компания предпринимала несколько попыток обратиться в Apple с целью решить вопрос установки VPN-клиента ViPNet на ОС iOS легитимным путем, т. е. без необходимости осуществлять jailbreak на iPad/iPhone и нарушать политику Apple. Однако Apple никак не отреагировала на эти обращения. В устных разговорах менеджеры Apple комментировали позицию своей компании в духе «мы за день продаем столько устройств, что ваши корпоративные продажи нам не интересны». Но позиция компании Apple, очевидно, не может быть выше требований российского законодательства по защите информации ограниченного доступа в государственных ИС. Поэтому с jailbreak или без него, но отечественные СКЗИ для iOS будут создаваться и сертифицироваться, пока на продукцию Apple будет спрос в корпоративной среде. Также следует понимать, что jailbreak – это не что иное, как программное средство, демонстрирующее наличие уязвимостей в «надежной» ОС iOS! Поэтому рассуждения про надежность мобильных устройств без jailbreak сродни рассуждениям о надежности входной двери, в которой замок сломан еще на этапе ее продажи в магазине. Конечно, сломанного замка можно и не замечать, ссылаясь на рекламный листок производителя двери, где написано «нет на свете двери надежней», но, согласитесь, такой подход будет выглядеть по меньшей мере наивным.

И в завершение несколько слов об Android. Действительно, перспективы создания защищенных решений для мобильных устройств на данной ОС выглядят достаточно оптимистичными. Сама рыночная ситуация, когда нет монополии одного производителя с его требованиями и желаниями никого не подпускать к своей операционке, в сильной степени способствует конструктивному диалогу разработчиков отечественных СКЗИ и разработчиков Android-устройств. И здесь можно согласиться – 2013 год будет богатым на отечественные сертифицированные СКЗИ для разнообразных Android-устройств.

заявили «КриптоПро», «С-Терра СиЭсПи», «ИнфоТеКС», «Амикон» и др. Данные решения пока не сертифицированы, но это вопрос времени, связанный с особенностями порядка сертификации. Первые сертифицированные СКЗИ можно будет ожидать по прошествии года с момента официального релиза Windows 8. Отметим, что использование внешне знакомой ОС, разработанной для хорошо известной x86-архитектуры, будет особенно удобно и приятно системным администраторам и сотрудникам внутренней службы технической поддержки. Более того, во многих компаниях наверняка давно сформирован перечень средств защиты информации, в том числе СКЗИ, под предыдущие версии ОС Windows из расчета на то, что их обновление под новую ОС уже не за горами.

Однако необходимо отметить, что между Windows 8 и мобильными версиями Windows существует некоторое различие. Если для Windows 8, как уже было сказано, вскоре появятся надежные, сертифицированные решения от известных производителей, то для мобильных версий для защиты каналов связи пока не анонсировалось ни одного решения. Хотя есть основания полагать, что существенных изменений Microsoft в обновленную мобильную версию своей операционной системы все-таки не внесет и клиентов безопасности для нее долго ждать не придется.

Кстати, внимательный пользователь СКЗИ наверняка заметил, что требования по криптографической защите, как правило, содержат пункт: «Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал». Сложно представить, как можно выполнить подобное условие при использовании мобильного устройства. Другими словами, даже с учетом нарушений условий работы, которые останутся на совести пользователя и/или администратора безопасности, напрашивается вопрос о возможности одновременного доступа к ресурсам сети Интернет и корпоративной сети. Основными возможными вариантами доступа представляются следующие:

- разрешить только доступ к корпоративной сети по защищенному каналу, запретить остальной интернет-трафик, по сути, пожертвовав удобством;
- разрешить доступ к корпоративной сети по защищенному каналу, остальной интернет-трафик маршрутизировать через корпоративный прокси-сервер. При этом увеличивается нагрузка на VPN-шлюз и корпоративный прокси-сервер;
- разрешить доступ к корпоративной сети по защищенному каналу, разрешить доступ к интернет-ресурсам с использованием дополнительных средств защиты, например антивируса.

Таким образом, вопрос в том, насколько реально выполнять правила пользования СКЗИ. Не теряется ли при этом смысл использования устройства?

Напоследок отметим, что при выборе мобильного устройства для применения в корпоративной среде с целью доступа к защищаемой информации следует принимать во внимание следующие факторы:

- наличие сертификата СКЗИ для мобильного устройства (или перспектива его получения). Причем не только наличие сертификата для конкретного СКЗИ, но и возможность в дальнейшем провести проверку соответствия всей системы в целом;
- необходимость компромисса между надежной защитой и удобством при использовании средств защиты информации на мобильных устройствах. ■