АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ТЕХНОЛОГИЙ В КОРПОРАТИВНОМ СЕКТОРЕ

ОБЩИЕ РЕКОМЕНДАЦИИ

Версия 1.0

**При участии Центра компетенции ООО «НИИ СОКБ»
по безопасности мобильной корпоративной инфраструктуры**

НАУЧНО-ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ
СИСТЕМ ОБЕСПЕЧЕНИЯ
КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

Москва
2015

АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ТЕХНОЛОГИЙ В КОРПОРАТИВНОМ СЕКТОРЕ

ОБЩИЕ РЕКОМЕНДАЦИИ

Версия 1.0

Москва
2015

СОДЕРЖАНИЕ

ПРЕАМБУЛА 1
ВВЕДЕНИЕ 2
1. ПРЕДМЕТНАЯ ОБЛАСТЬ 2
2. КОРПОРАТИВНЫЕ КОНЦЕПЦИИ ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ 5
2.1 Корпоративное устройство, управляемое пользователем (Corporate-Owned, Personally-Enabled, COPE) 5
2.2 «Принеси свое устройство» (Bring Your Own Device, BYOD) 6
2.3 «Выбери свое устройство» (Choose Your Own Device, CYOD) 6
3. КОРПОРАТИВНЫЕ МОДЕЛИ ПРЕДОСТАВЛЕНИЯ МОБИЛЬНЫХ УСЛУГ 6
4. КЛАССИФИКАЦИЯ УГРОЗ 8
4.1 Программные угрозы 8
4.2 Использование уязвимых мобильных ОС и приложений 8
4.3 Web-угрозы 9
4.4 Сетевые угрозы 10
4.5 Физические угрозы 14
4.6 Угрозы мобильных устройств для организации 15
4.7 Пользовательские угрозы 16
4.8 Угрозы со стороны поставщика услуг 17
4.9 Статистика угроз 19
5. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ 22
6. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ОС 24
6.1 Контейнер (container) или «песочница» (sandboxing). 24
6.2 Упаковка приложений (app wrapping). 25
6.3 Виртуализация (virtualization). 25
6.4 «Двойной профиль» (Dual persona). 26
7. ТЕХНОЛОГИИ И ФУНКЦИИ УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ И ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ 27
7.1 Управление мобильными устройствами (Mobile Device Management, MDM) 27
7.2 Управление мобильными приложениями (Mobile Application Management, MAM) 33
7.3 Управление мобильными данными (Mobile Information Management, MIM) 35
8. КОРПОРАТИВНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ МОБИЛЬНЫХ ТЕХНОЛОГИЙ 36
9. ПРОЕКТИРОВАНИЕ МОБИЛЬНОГО БИЗНЕСА И ОБЕСПЕЧЕНИЕ ЕГО БЕЗОПАСНОСТИ 38
ЗАКЛЮЧЕНИЕ 40

ПРЕАМБУЛА

Необходимость подобной публикации назрела давно. Она обусловлена стремительным развитием мобильных технологий, особенно в корпоративном секторе. За последние три года мобильные технологии проделали путь от простых (по сегодняшним меркам) устройств и приложений до полнофункциональных компонентов корпоративных систем. На рынок мобильных технологий вышли крупные компании, которые ранее мобильными технологиями не занимались: IBM, Oracle, Dell, SAP, Symantec, Citrix, VMware. Произошли десятки слияний и поглощений, с целью усиления рыночных позиций в области мобильных технологий образованы альянсы IBM и Apple, Samsung и BlackBerry.

В 2013 г. вышла публикация «Рекомендации СОДИТ по применению мобильных технологий», подготовленная Союзом ИТ-директоров России (СоДИТ) при участии ряда специалистов, в т.ч. из Ассоциации руководителей служб информационной безопасности (АРСИБ). Однако в данных рекомендациях отсутствует раздел по информационной безопасности. АРСИБ предложила разработать такой раздел, но в силу значительного объема и многогранности информации в формат раздела она не укладывалась. Для решения данной задачи в АРСИБ создана рабочая группа по безопасности мобильных технологий. Результатом работы группы является данная публикация (под ред. А. Першина).

В документе отсутствует раздел «Термины и определения». В настоящее время многие понятия в этой области не имеют установившихся определений не только в России, но и за рубежом. Сами понятия меняются настолько быстро, что соответствующие им определения, сделанные год-два назад, устарели. Кроме того, сейчас в мире на государственном уровне отсутствуют нормативные документы, определяющие средства и методы обеспечения информационной безопасности мобильных технологий, только рекомендательные или методические. Существуют лишь ведомственные и корпоративные стандарты и политики. Наиболее яркий пример – Министерство обороны США. Раздел «Термины и определения» предполагается ввести в одной из последующих редакций документа.

Также благодарность М. Одувалову (ОАО «Банк ВТБ»), Г. Фальковичу (ООО «Гейзер-Телеком»), членам АРСИБ Н. Носову и А. Макару за высказанные замечания и предложения.

Данная публикация не претендует на завершенность. Основные цели данного документа – определить область проблемы по обеспечению информационной безопасности мобильных технологий, инициировать дальнейшее обсуждение этой проблемы и развитие ее решений. Это относится к формулировке терминов и определений, подготовке нормативных, методических и рекомендательных документов, разработке организационных и технических средств и методов обеспечения информационной безопасности мобильных технологий, а также к другим задачам.

ВВЕДЕНИЕ

Применение мобильных технологий в бизнесе[1] позволяет ускорить, облегчить и удешевить бизнес-процессы, что приведет к повышению эффективности этих процессов. С другой стороны, за «мобилизацией» бизнес-процессов организации кроются различные риски и угрозы, которые необходимо соотносить с перспективами и выгодами.

Развитие средств и методов обеспечения безопасности в области информационных технологий (ИТ) всегда отстает от развития самих ИТ. Однако для мобильных технологий этот разрыв существенно шире, чем для стандартных ИТ: постоянно выпускаются новые модели мобильных платформ и операционных систем (ОС) с новыми функциями, количество мобильных приложений, включая корпоративные[2], исчисляется сотнями тысяч, развиваются средства управления. Между тем, средства и методы обеспечения безопасности мобильных технологий уже частично сформированы и продолжают развиваться как самостоятельное направление информационной безопасности (ИБ). Применение средств и методов обеспечения ИБ мобильных технологий в бизнесе позволяет существенно снизить риски «мобилизации» бизнес-процессов. Однако для этого, как минимум, необходимо:

- Четко соотносить перспективы и выгоды, с одной стороны, риски и угрозы, а также затраты на их минимизацию до приемлемого уровня – с другой;
- Знать или хотя бы иметь представление о средствах и методах обеспечения информационной безопасности при использовании мобильных технологий в бизнесе;
- Иметь четкую, внятную и гибкую политику безопасности при использовании мобильных технологий, обеспечить ее безусловное выполнение;
- Иметь подготовленный персонал или доверенных квалифицированных партнеров в области мобильных технологий и обеспечения их безопасности.

В данной публикации предлагается рассмотреть основные составляющие проблемы обеспечения ИБ мобильных технологий.

1. ПРЕДМЕТНАЯ ОБЛАСТЬ

В первую очередь необходимо определить предметную область проблемы: что есть мобильные технологии, безопасность которых необходимо обеспечивать?

Одно из наиболее «внятных» определений: «Мобильные (информационные) технологии – это возможность организации предоставлять работникам корпоративные информационные услуги и сервисы где угодно и с любого (мобильного) устройства»[3]. Или: «Мобильные технологии – это технологические платформы, специально разработанные и используемые в мобильных устройствах»[4].

---

[1]Под терминами «бизнес», «бизнес-процессы» будем понимать деятельность, действия, процессы организаций любых форм собственности.

[2]Также, термин «корпоративные» (технологии, процессы, устройства и пр.) применим к организациям любых форм собственности.

[3]http://searchcio.techtarget.com/definition/mobile-IT-mobile-information-technology

[4]http://blog.designlove.co.uk/definition-mobile-technology/

Корпоративные мобильные технологии включают, как правило, следующие составляющие:

1. Одно или более мобильных устройств, управляемых пользователями – работниками организации.

2. Беспроводная среда передачи данных (Wi-Fi, сотовая, спутниковая и др.), обеспечиваемая одним или несколькими операторами связи – от абонента до приемного устройства оператора связи.

3. Канал передачи данных от сети оператора связи до объекта доступа (ресурс в корпоративной, ведомственной, общедоступной или другой сети).

4. Корпоративная информационная система, включая приложения и данные.

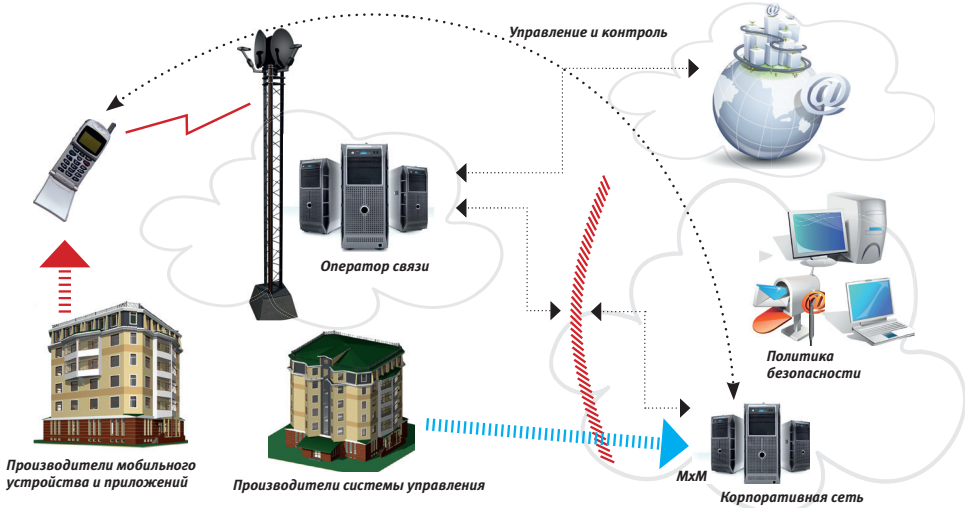
5. Сторонние информационные системы, доступ пользователя (работника организации) к которым осуществляется посредством мобильных устройств (публичные, ведомственные и др., исключая корпоративные) – если это разрешено политикой организации.

6. Сторонние участники: производители мобильных устройств, приложений и систем управления ими.

А также соответствующие технологии, протоколы и способы передачи голоса и данных.

Обобщенная схема взаимодействия этих составляющих представлена на рисунке 1.

ОБОБЩЕННАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ КОРПОРАТИВНЫХ МОБИЛЬНЫХ ТЕХНОЛОГИЙ



Таким образом, «мобильные технологии» есть частный случай общей объект – субъектной модели доступа, особенностью которого является наличие беспроводной составляющей. Теперь необходимо определить особенность этой составляющей, а именно: что есть мобильное устройство (будем считать, что определение или хотя бы понимание остальных составляющих известны)? Возьмем за основу определение мобильного устройства из публикации NIST SP800-124 release 1.

Характеристики мобильных устройств постоянно изменяются, поэтому термину «мобильное устройство» трудно дать четкое однозначное определение. В зависимости от характеристик мобильных устройств, им присущи свои специфические угрозы, а также меры и средства безопасности. В связи с этим необходимо определить некий набор базовых характеристик любого мобильного устройства:

- Малые геометрические размеры и вес.
- Наличие, как минимум, одного беспроводного интерфейса сетевого доступа (для передачи данных): интерфейс Wi-Fi, сотовой связи или другой для подключения устройства к сетевой инфраструктуре оператора связи с возможностью подключения к сети Интернет или к другой сети передачи данных.
- Специализированная мобильная операционная система (ОС), не являющаяся полнофункциональной ОС стационарных компьютеров и ноутбуков.
- Наличие встроенных в мобильную ОС функций для синхронизации данных (со стационарным компьютером или ноутбуком, с серверами организации, поставщиками услуг или третьими сторонами и т.п.).

Кроме базовых существуют распространенные, но необязательные характеристики мобильных устройств. Эти характеристики определяют не группу устройств, а описывают функции, наиболее важные с точки зрения угроз безопасности:

1 Наличие в составе сетевых служб:

- Одного или нескольких интерфейсов персональной беспроводной сети, например, Bluetooth или NFC (Near Field Communication);
- Одного или нескольких беспроводных сетевых интерфейсов для голосовой связи, например, сотовой;
- Глобальной навигационной системы (GPS и/или ГЛОНАСС), предлагающей сервисы определения местоположения.

2 Наличие одной или более фото/ видео камер.

3 Возможность хранения данных:

- Поддержка съемных носителей информации.
- Использование в качестве съемного носителя информации.

Необходимо отметить, что «мобильным» может называться любое носимое вычислительное устройство. Под мобильным устройством с беспроводным подключением можно понимать, например, ноутбук с установленным USB-модемом. Однако при этом необходимо учитывать два нюанса:

1 Такие устройства не могут управляться специализированными системами класса MxM (MDM/ MAM/ MIM – см. раздел 7).

2 С точки зрения сетевого администрирования они будут выглядеть как стационарные компьютеры, а не как специализированные мобильные устройства. Соответственно, управляться они будут, как и любые другие сетевые устройства, вне зависимости, с проводным они подключением или с беспроводным.

Таким образом, в данной публикации под мобильными устройствами будем понимать те из них, которые имеют специализированные мобильную ОС и систему управления. Другие устройства, которые можно считать мобильными с беспроводным подключением, с точки зрения безопасности (угрозы, средства и методы защиты и управления) никаких особенностей не имеют, поэтому здесь они рассматриваться не будут.

Кроме того, существует понятие «мобильные вычисления» (mobile computing), характеризующее функционал мобильного устройства. Прежде всего, мобильные вычисления – это способность мобильного устройства вне зависимости от местоположения или времени суток выполнять определенные приложения или получать доступ к определенным сервисам, включая отображение, сбор, обработку и передачу данных, в публичной или корпоративной информационной системе с использованием беспроводных сетей.

Далее рассматриваются составляющие понятия «безопасность мобильных технологий» в контексте описанной предметной области и сделанных ограничений.

2.КОРПОРАТИВНЫЕ КОНЦЕПЦИИ ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ

2.1 Корпоративное устройство, управляемое пользователем (Corporate-Owned, Personally-Enabled, COPE)

Корпоративное устройство, управляемое пользователем (COPE) – это концепция ИТ-бизнеса, подразумевающая, что организация приобретает и обслуживает вычислительные устройства, используемые и управляемые работниками, обычно с разрешением на использование этого устройства в личных целях. При использовании концепции COPE корпоративные устройства настраиваются работниками самостоятельно. Однако работник – по крайней мере, до определенной степени – самостоятельно отвечает за его настройку и текущее техническое обслуживание, поэтому концепция COPE может применяться, только если пользователи обладают достаточными знаниями и навыками обращения с устройствами и операционными системами.

Концепция COPE является противоположностью BYOD (см. ниже) и традиционной модели обеспечения ИТ, при которой работникам выдаются служебные вычислительные устройства, которые постоянно находятся на рабочем месте. Организации часто могут приобретать продукцию ИТ в массовом порядке и по оптовым ценам, поэтому модель COPE может быть более эффективна с точки зрения затрат, как для организации, так и для работника. Несмотря на то, что устройство принадлежит организации, и она отвечает за его обслуживание и поддержку, работники могут его использовать в нерабочее время.

Также модель COPE может способствовать проектам развития систем управления мобильными устройствами (MDM) и приложениями (MAM) и обеспечить более высокий уровень защиты корпоративных данных с технической и юридической сторон (раздел 7). Поскольку организация является собственником данного вида услуг, у нее есть возможность выбора поставщика устройств и услуг (включая тарифные планы).

2.2 «Принеси свое устройство» (Bring Your Own Device, BYOD)

«Принеси свое устройство» (BYOD) – это концепция, при которой любое устройство, находящееся в собственности пользователя, может использоваться где угодно, как в личных, так и в служебных целях.

BYOD является динамично развивающейся концепцией в бизнесе. Смартфоны – самый яркий пример ее использования, однако эта модель в равной степени относится и к планшетам, ноутбукам и другим мобильным устройствам. BYOD является частью общей концепции «консьюмеризации» («consumerization»), при которой клиентское программное обеспечение и оборудование может использоваться на предприятии. Использование устройств, которые являются собственностью работника, зачастую санкционировано руководством организации, и они поддерживаются ее инфраструктурой. В других случаях, такие устройства являются частью дублирующей или резервной системы, а также, в некоторых случаях, частью систем организации, которые не обслуживаются центральным подразделением ИТ.

Обе модели BYOD и COPE отражают современные тенденции мягкого разделения между личным и служебным использованием современных технологий.

2.3 «Выбери свое устройство» (Choose Your Own Device, CYOD)

В соответствии с концепцией «выбери свое устройство» (CYOD) предприятие предоставляет своим работникам те устройства, которые оно само приобрело, с уже оформленным договором на оказание услуг связи. Работник при этом может выбрать из предложенного ассортимента мобильных телефонов, смартфонов или планшетных ПК тот аппарат, который лучше всего соответствует его рабочим задачам и личным предпочтениям.

В отличие от концепций BYOD и COPE, из названия этого подхода неясно, можно ли использовать устройство, являющееся собственностью предприятия, в личных целях. Соответственно, следует различать более «строгую» концепцию CYOD, допускающую использование корпоративных устройств исключительно в служебных целях, и более мягкий вариант, разрешающий их эксплуатацию в личных целях. При этом использование устройства всегда должно соответствовать корпоративным требованиям и правилам, установленным политикой безопасности организации и реализованным в системе управления мобильными устройствами.

3. КОРПОРАТИВНЫЕ МОДЕЛИ ПРЕДОСТАВЛЕНИЯ МОБИЛЬНЫХ УСЛУГ

Данный раздел не относится напрямую к мобильным услугам, «домашнее», внешнее и облачное модели предоставления услуг также характерны и для всех других приложений, информационных технологий и услуг. Однако стремительное развитие мобильных технологий и их специфика делает выбор модели предоставления услуг актуальной задачей.

Основные модели управления мобильными устройствами:

1. Самостоятельное (или внутреннее) управление (in-home):

- Управление мобильной инфраструктурой, находящейся внутри организации, силами работников самой организации;
- Внешнее управление мобильной инфраструктурой, находящейся внутри организации, силами сторонней сервисной компании (outsourcing). Например, система управления входит в инфраструктуру организации, но ее администрирование осуществляет внешняя компания на основе соответствующего договора.

2. Облачное (cloud) управление.

Облачный сервис – это ресурс, находящийся вне организации, доступ или использование которого обеспечивается через Интернет или другую публичную или частную сеть. Существуют различные способы предоставления облачных услуг, основные из которых следующие.

– BaaS (Backend as a Service).

Мобильный Backend as a Service или просто Backend as a Service (BaaS) – это вычислительная архитектура, связывающая мобильное приложение с облачными сервисами.

Являясь альтернативой мобильному промежуточному программному обеспечению (middleware), подход BaaS использует унифицированные интерфейсы прикладных программ (API) и средств разработки программного обеспечения (SDK) для доступа мобильных приложений к облачному хранилищу. Традиционное мобильное промежуточное программное обеспечение интегрирует серверные услуги, реализованные на физическом сервере, с приложением. BaaS, с другой стороны, интегрирует серверные услуги с облачной инфраструктурой.

– SaaS (Software as a Service).

Software as a Service (SaaS) – это модель распространения программного обеспечения, при которой приложение расположено у производителя или поставщика услуг и доступно для клиента посредством сетевого доступа, обычно Интернет.

SaaS становится наиболее распространенной моделью доставки как базовая технология, поддерживающая сложившиеся Web-сервисы и сервис-ориентированная архитектура (SOA), а также новые подходы к разработке, такие как Ajax, становящиеся все более популярными. При этом услуги широкополосного доступа становятся доступными в различных регионах мира.

– PaaS (Platform as a Service).

Platform as a Service (PaaS) – это способ аренды оборудования, операционных систем, хранилищ данных и ресурсов сети посредством доступа к ним через Интернет или другую сеть (публичную, корпоративную, ведомственную и др.). Модель доставки услуг позволяет клиенту арендовать виртуальные серверы и связанные с ними услуги для выполнения существующих приложений или разработки и тестирования новых. PaaS – это развитие SaaS и имеет ряд преимуществ для разработчиков.

– IaaS (Infrastructure as a Service).

Infrastructure as a Service (IaaS) – это модель обеспечения, в которой организация привлекает внешнее оборудование для выполнения операций, включая хранилища данных, аппаратное обеспечение, серверные и сетевые компоненты. Поставщик услуг является владельцем оборудования и отвечает за его размещение, функционирование и поддержку. IaaS иногда называют Hardware as a Service (HaaS).

Существует ряд других способов реализации облачных сервисов, но, по сути, они схожи с уже перечисленными. Часто все способы вместе обозначают как XaaS с расшифровкой «Everything as a Service» (что-то вроде «все, что как сервис»).

Необходимо учитывать, что чем больше ресурсов организации передается в «облачное» управление, тем выше риски безопасности.

4. КЛАССИФИКАЦИЯ УГРОЗ

Выбор методов и средств защиты при использовании мобильных технологий и устройств в корпоративной среде необходимо осуществлять с учетом возможных угроз безопасности и источников их возникновения. Все они, как правило, в той или иной степени применимы и к стационарным компьютерам. Однако существуют специфичные угрозы, а «стандартные» имеют свои особенности. Специфичность эта обусловлена размерами, портативностью, используемыми услугами и уникальностью архитектуры мобильных устройств. В зависимости от используемых или активированных сервисов, эти специфичные угрозы повышают уязвимость мобильных устройств.

Различные источники по-разному классифицируют и описывают угрозы мобильным устройствам. Одна из наиболее полных моделей угроз приведена в документе «Mobile Security Reference Architecture»[5], подготовленном Федеральным советом руководителей информационных служб (Federal CIO[6] Council) США и Министерством внутренней безопасности США (май 2013 г.). Каждый регулятор, ведомство или отдельная организация может по-своему интерпретировать приведенный в данной публикации перечень в соответствии со своими требованиями и стандартами, а также с учетом соответствующих рисков и требований безопасности.

4.1 Программные угрозы

Функционал мобильных устройств обеспечивается системным программным обеспечением и его расширениями, а также приложениями, которые пользователь может загрузить и установить. Однако некоторые из таких приложений и расширений могут быть изначально злонамеренными. Эти угрозы имеют высокий уровень риска и аналогичны для стационарных компьютеров.

4.1.1 Вредоносное программное обеспечение

Разновидность предыдущей угрозы. Такое программное обеспечение создается с целью выполнения несанкционированных действий на мобильном устройстве. Оно может

[5] *https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf*
[6] *Chief Information Officers.*

быть прикреплено к мгновенному сообщению или сообщению электронной почты, а также загружено вместе с инфицированным файлом или встроено в приложение. Вредоносное программное обеспечение может оказывать разрушительное воздействие на мобильную ОС, компрометировать данные или результаты работы приложений.

4.2 Ипользование уязвимых мобильных ОС и приложений

Уязвимости в мобильных ОС и приложениях аналогичны таким же уязвимостям для стационарных компьютеров. Такие уязвимости, как в стационарных, так и в мобильных ОС и приложениях обнаруживаются регулярно. Уязвимости ОС представляют более значительную угрозу, поскольку процессы ОС выполняются с более высоким приоритетом, чем приложения. Мобильные приложения, как и приложения для других устройств, также могут быть безграмотно составлены и уязвимы для атак и использования «дыр». Многие приложения уязвимы по причине ошибок разработки или программирования, или же некорректно сконфигурированы или настроены с точки зрения безопасности.

Одна из самых ранних и опасных атак заключается в отключении злоумышленниками встроенных средств защиты (процесс, известный как «jailbreaking» для Apple iOS или «rooting» для Google Android). Отключение встроенных средств защиты ОС позволяет пользователям устанавливать приложения и системные расширения, которые запрещены политикой безопасности. Такие установки могут привести к умышленному или случайному внедрению вредоносного кода. Как правило, процесс обхода (взлома) средств защиты ОС и приложений занимает дни или даже часы после выхода новой версии с исправленными ошибками предыдущей. Такие угрозы имеют высокий уровень риска.

4.3 Web-угрозы

Все больше устройств имеют доступ к Интернет и, соответственно, растет количество и изощренность Web-угроз. При этом целями, в том числе, являются смартфоны, планшеты и специализированные устройства и сервисы (например, Интернет, телевидение, радио и др.)[7].

4.3.1 Мобильный код

Это активный контент, получаемый по сети и который может быть выполнен на мобильном устройстве. Мобильный код может быть доставлен посредством HTML5, JavaScript, Adobe Flash и другими приложениями, поддерживающими интерпретируемые языки.

4.3.2 Загрузка «на лету»

Данная угроза заключается в автоматическом получении вредоносного кода и является результатом посещения пользователем инфицированного web-сайта. Многие легальные сайты могут содержать вредоносный код, поскольку ранее были инфицированы. Загрузка «на лету» чрезвычайно опасна, поскольку цель атаки (пользователь) не был уязвим до посещения такого сайта.

---

[7] *Многие из перечисленных угроз характерны и для стационарных устройств. Однако в данной публикации будут рассматриваться угрозы для мобильных устройств, даже если они универсальны.*

4.3.3 Использование уязвимого браузера

Уязвимый браузер – это специфичный случай уязвимого приложения по нескольким причинам. Во-первых, браузер мобильного устройства – это приложение, которое используется, как правило, достаточно часто, и поэтому с большей вероятностью подвержен угрозе для пользователя. Во-вторых, есть множество примеров вредоносного web-контента, только и ожидающего на сайтах Интернет, как бы использовать «преимущества» уязвимого браузера. И, в-третьих, пользователи могут устанавливать и использовать сторонние браузеры, которые не управляются или должным образом не защищены со стороны администраторов организации, увеличивая тем самым зону охвата уязвимостей браузера.

4.4 Сетевые угрозы

Сетевые угрозы безопасности – это угрозы, где потенциальным источником является использование уязвимостей через сеть оператора связи на прикладном уровне или внутри приложений, файлов или данных (в плане данные/ услуга), также как и в плане контроля, отвечающего за конфигурацию и управление устройством. Сетевые угрозы безопасности осуществляются через сеть оператора связи или сетевые протоколы, а также устройства, приложения и данные, постоянно использующие сеть. Устройства, использующие для связи сети Wi-Fi и сотовые, более доступны и уязвимы, чем устройства, использующие только проводные сети. Эти угрозы имеют высокий уровень риска и специфичны исключительно для мобильных устройств.

4.4.1 Съем голоса/ данных «по воздуху»

Мобильные устройства для взаимодействия используют различные беспроводные протоколы, в которых передаваемые данные могут быть перехвачены или скомпрометированы. Большинство устройств поддерживают сотовые протоколы, а также Wi-Fi и Bluetooth. Угрозы данного класса относятся к воздействиям в канале связи от пользователя мобильного устройства до базовой станции оператора связи.

Wi-Fi

Мобильные устройства используют, в частности, Wi-Fi – беспроводной способ взаимодействия на основе семейства стандартов IEEE 802.11a/b/g/n. Такие устройства могут подключаться к любой мобильной, персональной или корпоративной точке доступа или другому подобному устройству для взаимодействия «точка – точка». Устройства, использующие Wi-Fi, уязвимы для перехвата другим Wi-Fi-устройством, беспроводным программным инструментарием, а также анализатором сигналов. Неконтролируемые точки доступа (несанкционированная точка внутри административно контролируемого домена) – также потенциальная угроза, подвергающая мобильное устройство опасности атаки посредника или «человек посередине» (man-in-the-middle).

Сотовая связь

Мобильные устройства могут взаимодействовать с использованием сотовых сетей различных технологий (GSM, EDGE, LTE и др.). Некоторые операторы связи могут предоставлять криптографические способы защиты (см. раздел 5). Данные и голос в сетях сотовой связи могут быть перехвачены, а также конфигурация и ключевые компоненты устройства могут быть скомпрометированы по каналам управления.

Bluetooth

Bluetooth – это маломощная беспроводная технология ближнего действия, обеспечивающая взаимодействие мобильных устройств по стандартизованному протоколу. Bluetooth используется для передачи данных между устройствами внутри персональной сети (personal area network, PAN), а также для передачи команд и голосового взаимодействия между устройством и гарнитурой. Bluetooth имеет встроенные механизмы шифрования и аутентификации, однако известны уязвимости и «дыры» этой технологии, такие, как перехват ключей при инициализации сеанса.

Инфракрасное взаимодействие

Инфракрасное взаимодействие – это маломощная беспроводная технология ближнего действия в инфракрасном диапазоне, обеспечивающая взаимодействие мобильных устройств по стандартизованному протоколу (RC-5, SIRC). Инфракрасное взаимодействие, как и Bluetooth, используется для передачи данных между устройствами внутри персональной сети (personal area network, PAN), а также для односторонней передачи команд. Инфракрасное взаимодействие не имеет механизмов шифрования и аутентификации, и поэтому уязвимо. Большинство уязвимостей специфичны и зависят от производителя, такие как переполнение буфера при получении инфракрасного кода взаимодействия.

Near Field Communication

Near Field Communication (NFC) – это набор стандартов для маломощного, сверхближнего беспроводного способа взаимодействия «точка – точка». Эта технология используется для идентификационных карт и транзакций с банковскими картами в 1-м квартале 2012 г. Реализации NFC в первую очередь являются объектами атак физического уровня, таких, как перехват и навязывание сигнала, однако специфические реализации могут содержать дополнительные уязвимости.

4.4.2 Съем голоса/ данных по сети

В сети может осуществляться электронное прослушивание. Все взаимодействия будут маршрутизированы через беспроводные сети (Wi-Fi или сотовые) и Интернет до точки назначения. Взаимодействия могут быть перехвачены в промежуточной точке маршрутизации или с помощью различных подслушивающих устройств. Угрозы данного класса относятся к воздействиям в канале связи от базовой станции оператора связи до точки доступа пользователя мобильного устройства в публичной, ведомственной, корпоративной или другой сети.

4.4.3 Манипуляции с данными при передаче

Данные и голос при передаче могут быть изменены, подтасованы или избирательно блокированы с целью компрометации соединения. Одна из отличительных особенностей мобильных устройств – это то, что они часто переключаются между механизмами средств и операторов связи, перескакивая от одной базовой станции сотовой связи к другой или переключаясь с сотовой связи на Wi-Fi. Также мобильные устройства имеют сравнительно малые вычислительные мощности и объемы памяти по сравнению с ПК и серверами. Эти особенности приводят к тому, что многие мобильные приложения обращаются к удаленным хранилищам данных (не размещенным на мобильном устройстве), разгружая тем самым вычислительные мощности мобильного устройства для повышения функциональности. Таким образом, мобильные устройства увеличивают объемы данных, передаваемые через не доверенные механизмы средств связи. Кроме того, облачные сервисы от производителя устройства или третьей стороны предлагают услуги хранения файлов, обработки приложений и данных, а также функции управления в распределенной среде, что снижает ограничения на внутреннюю память устройства при увеличении объема данных, передаваемых между облаком и мобильным устройством. Увеличение потока обмениваемыми данными предоставляет противнику большее поле для нападения, целью которого являются передаваемые данные. В результате критичные данные могут быть непреднамеренно раскрыты или скомпрометированы по причине слабостей архитектуры облака, некорректной реализации или злонамеренных действий, что может привести к значительному ущербу. Данная угроза сопряжена с высоким риском и специфична для беспроводных и облачных технологий.

4.4.4 Раскрытие данных за счет побочных электромагнитных излучений и наводок

Большинство вычислительных устройств порождают побочные электромагнитные излучения и наводки (ПЭМИН) за счет переключения отдельных электрических компонент внутри устройства, не считая излучения, порождаемого сигналом сотовой связи, Bluetooth, NFC или Wi-Fi. Это излучение специфично внутри радиочастотного спектра и может быть перехвачено и декодировано, поскольку устройство и излучаемые данные не защищены.

Практически в любом вычислительном устройстве обрабатываемые данные не защищены, и поэтому уязвимы для прослушивания как вблизи, так и на значительном расстоянии (до 100 м) с использованием усиливающей антенны, радиочастотного приемника, промежуточного частотного усилителя, выборочного конвертера и вычислительного устройства. Такая конфигурация недорога в производстве и невелика по размерам. Данная уязвимость специфична, в основном, для беспроводных устройств, но связанный с ней риск относительно невелик.

4.4.5 Соединение с не доверенным сервисом

Пользователи мобильных устройств, использующие тот или иной сетевой сервис, могут неумышленно обратиться к не доверенному сервису. При этом легальный сервис мог быть

ранее скомпрометирован. Или же пользователь умышленно обратился к сервису, к которому не обращался ранее, и надежность которого не подтверждена. В результате критичная информация может быть раскрыта или скомпрометирована. Также существует риск нарушения целостности или доступности данных.

4.4.6 Затор (Jamming)

Затор – это угроза, которая мешает получению или передаче при беспроводном соединении. Другими словами, затор – это постановка или использование помех. Любой беспроводной протокол, используемый мобильным устройством, подвержен помехам, включая сотовые соединения, GPS/ГЛОНАСС, Wi-Fi и Bluetooth.

4.4.7 Затопление (Flooding)

Атака затопления переполняет систему данными, объем которых больше, чем система может обработать. Любой беспроводной протокол, используемый мобильным устройством, подвержен затоплению, включая сотовые соединения, GPS/ГЛОНАСС, Wi-Fi и Bluetooth. Результатом атаки является обычно отказ в обслуживании. Данной угрозе подвержены пользователи любых устройств, проводных и беспроводных.

4.4.8 GPS/ Геолокация

Почти все мобильные устройства обеспечивают для своих приложений тот или иной уровень службы геолокации. Такие приложения могут использовать эту службу для отображения текущего местоположения устройства на карте, определять местонахождение ближайших ресурсов, осуществлять трассировку маршрута пользователя и даже выполнять популярную у пользователей функцию навигации маршрута передвижения. Вместе с тем эта служба имеет потенциальную возможность раскрытия местонахождения устройства или выводить некорректную информацию о местонахождении пользователя за счет внешних помех или манипуляций. Эта угроза характерна исключительно для мобильных устройств.

Источники данных геолокации

Сбор данных позиционирования от различных источников – это пассивный процесс: источники периодически рассылают информацию о местонахождении в широковещательном режиме. Поскольку процесс сбора пассивен, двусторонняя аутентификация отсутствует и, таким образом, целостность данных позиционирования не гарантирована. При этом используются различные источники данных позиционирования (сигнатуры соты 2/3/4G мобильного устройства, сигнатуры Wi-Fi, внутренний приемник A-GPS).

Триангуляция

Путем комбинирования двух и более источников данных позиционирования и, используя технику триангуляции, приложения мобильного устройства могут значительно повысить точность определения своего местонахождения, обеспечивая данными зависимые службы, если один и более их собственных источников недоступен.

Трассировка (Tracking)

Трассировка с использованием службы геолокации мобильного устройства полезна для решения многих штатных задач, таких как обнаружение утерянного устройства. Однако эта же служба может использоваться для сбора информации и создания нештатных ситуаций для организации или пользователя. Незаконная трассировка может быть выполнена путем извлечения данных (data mining) и просмотра «гео-маркированных» (geotagged) записей, изображений или других данных.

«Гео-маркировка» (Geotagging)

Гео-маркировка – это процесс добавления географических идентификационных метаданных к фото, видео и другим данным. Извлечение данных из «гео-маркированных» изображений и других данных, записанных мобильным устройством – это метод, позволяющий отслеживать местоположение устройства, как в легальных, так и в незаконных целях.

Подмена местонахождения (Location Spoofing)

Для передачи некорректной информации местонахождения может использоваться ретрансляция скрытых сигналов GPS, а также ложная информация местонахождения от вышек сотовой связи и «горячих точек» Wi-Fi. Такие атаки могут привести к тому, что мобильное устройство будет оперировать ошибочной информацией местонахождения, что может привести к некорректному функционированию приложений, которым необходимы точные данные местонахождения.

4.5 Физические угрозы

Не все угрозы безопасности исходят от злоумышленников, намеревающихся скомпрометировать или украсть критичные данные. Некоторые угрозы, такие, как находящееся не на месте устройство, возникают без всякого злого умысла. Тем не менее, физические угрозы становятся все более распространенными в среде, становящейся все более мобильной. При этом мобильные устройства становятся все меньше и все больше проникают во все сферы деятельности общества.

4.5.1 Утеря устройства

Утеря мобильного устройства ставит под угрозу конфиденциальность, целостность и доступность информации, хранящейся на нем. Более того, устройство может содержать контрольную информацию (полномочия) для доступа к корпоративным ресурсам, тем самым увеличивая риск для организации. Наконец, данные на устройстве могут быть утеряны, если вовремя не было проведено резервное копирование.

Данные, восстановленные несанкционированной стороной

Если мобильное устройство утеряно или им физически обладает не его законный пользователь, возможно, что данные, информация о конфигурации, а также контрольная информация (полномочия), хранимые на устройстве, могут быть восстановлены и использованы нелегально.

Несанкционированное использование контрольной информации (полномочий)

Данная угроза означает, что идентификация устройства как такового – это слабость аутентификации, поскольку утерянное или украденное устройство может получить доступ к корпоративным ресурсам. Клонирование – это еще одна уязвимость, поскольку злоумышленник может сконфигурировать другое устройство как точную копию законного устройства, сделав его аутентичным в корпоративной системе. Наконец, контрольная информация (полномочия) может быть украдена или незаконно присвоена, что приведет к угрозе для корпоративной сети в целом.

4.5.2 Ущерб от физического доступа

Существует возможность, что тот, кто имеет физический доступ к мобильному устройству, может установить вредоносное программное или аппаратное обеспечение, которое может собирать или искажать данные, как на уровне устройства, так и на уровне организации, повышая тем самым уязвимость организации в целом. Злоумышленник может использовать внешние интерфейсы для подключения мобильного устройства к USB/Bluetooth и удерживать его «на привязи». Наконец, злоумышленник может, при определенных обстоятельствах, подключить компьютер или внешний накопитель для клонирования, копирования, искажения или уничтожения содержимого устройства.

4.5.3 Специфические функции устройства

Встроенные функции мобильного устройства, такие как камера и микрофон, могут представлять собой угрозу, предоставляя возможность сбора критичных изображений и разговоров. В некоторых случаях третья сторона или преступники могут включать микрофон устройства, даже если считается, что он отключен.

4.5.4 Цепь поставки

Цепь поставки компонент мобильных устройств, их сборки, а также принадлежностей к ним предоставляют возможность физически вмешаться в комплектацию устройства до его доставки, что может сделать его потенциально уязвимым.

4.5.5 Внешнее оборудование

Оборудование, физически взаимодействующее или расширяющее возможности мобильных устройств, также влечет, хоть и чрезвычайно малую, степень риска. Док-станции, беспроводные периферийные устройства и др. могут быть потенциально использованы злоумышленником для получения доступа к мобильному устройству. Например, существует потенциальная возможность съема информации с мобильного устройства, подключенного к док-станции, через электрическую сеть или посредством использования ПЭМИН. Или же пользователь может использовать инфицированную ранее флэш-карту.

4.6 Угрозы мобильных устройств для организации

Ресурсы организации могут быть скомпрометированы, если мобильное устройство должным образом не защищено или не управляется. Эти угрозы могут распространяться

и на компьютеры пользователей, переносные компьютеры, серверы (включая web), базы данных и устройства хранения данных, что может привести к несанкционированному доступу к ресурсам организации. В контексте данного рассмотрения эта угроза характерна для мобильных устройств.

4.6.1 Доступ к ресурсам организации

Утерянное или украденное устройство, или же скомпрометированная контрольная информация (полномочия) могут привести к полному доступу к критичной информации и ресурсам в информационной системе организации. Такой доступ может привести к компрометации данных организации или несанкционированным действиям, выполняемым посредством доступа с мобильного устройства к корпоративным данным и сетям. Кроме того, критичная информация, не переведенная в цифровой вид (документы на бумажных носителях, проецируемая на экран информация, переговоры), могут быть легко оцифрованы, перехвачены и перенаправлены с помощью скрытого индивидуального устройства. По причине малого размера, достаточной вычислительной мощности и наличия встроенных записывающих и передающих устройств (камера, микрофон, акселерометр, GPS, Wi-Fi, Bluetooth) мобильное устройство является важным инструментом (промышленного) шпионажа, а также угрозой со стороны инсайдеров.

4.7 Пользовательские угрозы

Такие угрозы общего характера могут быть использованы внутренними пользователями организации. Они могут быть умышленными или неумышленными. Злоупотребление полномочиями и мошенничество относятся к умышленным угрозам. Ошибки пользователей и халатность – это неумышленные внутренние угрозы (например, разглашение критичной информации как результат попытки «социальной инженерии»).

4.7.1 «Социальная инженерия» (Social Engineering)

Социальная инженерия – это искусство манипулирования людьми с целью убедить их выполнить определенные действия или разгласить конфиденциальную информацию. «Фишинг» (phishing) – одна из наиболее популярных атак социальной инженерии, которая заключается в направлении пользователю сообщения, которое выглядит как законное, и призывает его выполнить те или иные несанкционированные действия.

4.7.2 Инциденты безопасности, связанные с мобильными устройствами

Т.е., мобильное устройство является источником или целью такого инцидента. Такая угроза является общей, расследование таких инцидентов должно проводиться в соответствии с общей политикой безопасности организации.

4.7.3 Пользовательские устройства

Организации, разрешающие использование не доверенных пользовательских устройств, подвержены дополнительному риску. Пользователи неумышленно могут приобрести устройство, не являющееся оригинальным, а клон может не обладать теми же свой-

ствами безопасности, что и оригинальное устройство. Более того, критичные данные, как персонально опознаваемая информация, может быть уязвима, поскольку пользователь собственного устройства может устанавливать приложения без ограничений, включая те из них, которые могут размещать критичную информацию на сторонних серверах. Возможны другие варианты вредоносного кода на не доверенных устройствах. Использование пользовательских устройств также повышает риск, связанный с конфиденциальными или критичными данными, утечкой информации и соответствующими потерями.

4.7.4 «Вредоносный инсайдер» (Malicious Insider)

Инсайдер – это любой работник организации с соответствующими полномочиями и знанием информационных систем, сервисов и операций. Вредоносный инсайдер может умышленно нанести ущерб организации путем выполнения действий, не выходящих за рамки его полномочий, которые могут нанести физический ущерб оборудованию или скомпрометировать конфиденциальность, целостность или доступность корпоративных данных.

4.8 Угрозы со стороны поставщика услуг

Угрозы данного класса могут быть реализованы со стороны оператора мобильной связи, целью которых являются как сами данные, так и управление мобильным устройством. Это может быть доступ к сети управления оператора для реконфигурации мобильного устройства, перехвата критичных данных на конечном устройстве или кэшированных у оператора. Также угрозы могут быть реализованы в других каналах передачи данных, помимо традиционного IP-транспорта (такие, как MMS/SMS или канал управление/контроль), и которые могут использоваться для передачи вредоносного кода.

Специфические для ОС свойства и функции, предоставляемые и управляемые производителем ОС – еще один канал реализации данной угрозы путем вставки уязвимости или перехвата критичных данных. Например, пользователь может ненамеренно подписаться на услугу резервного копирования, которая предоставляет транспорт для передачи критичных данных в облако производителя. Некоторые производители требуют шифрования пользовательских данных, при этом неизвестно качество шифрования или каков процесс удаления данных у производителя, если пользователь в итоге решит отказаться от этой услуги.

Существует множество типов диагностических данных, которые в совокупности могут использоваться для определения характеристик пользователя и/или организации. Некоторые производители применяют стороннее программное обеспечение и сервисы, комбинируя данные геолокации с SSID[8] для определения местонахождения определенных беспроводных сетей, которые совместно используются их клиентами. При этом неизвестно, пересылаются эти данные производителю ОС или третьей стороне. Другое стороннее программное обеспечение, устанавливаемое производителем ОС, может ис-

[8] *SSID (Service Set Identifier) – идентификатор, позволяющий различать отдельные беспроводные сети, которые могут действовать в одном и том же месте или области.*

пользоваться, например, для трассировки режима работы пользователя и измерения его производительности. Эти данные могут пересылаться производителю ОС или третьей стороне.

Еще один источник угрозы – поставщик услуг по установке мобильного программного обеспечения. Примером может служить «витрина», внешне выглядящая почти как настоящая, но содержащая инфицированное программное обеспечение. Такая «дыра» может быть непосредственно встроена в приложение или неумышленно реконфигурировать мобильное устройство (напрямую или опосредованно), напрямую или через третью сторону может предоставить явно не указанный сервис, такой как чат.

4.8.1 Отслеживание местоположения

В течение долгого времени операторы связи отслеживали местоположение путем пассивного перехвата сигнатуры мобильного устройства от сотового узла и сопоставляя ее с физическим местоположением этого узла. Сопоставляя сигнатуру мобильного устройства с местонахождением нескольких узлов и используя метод триангуляции, сервис определения местонахождения становится значительно более точным. А используя эти данные совместно с локальным приемником GPS/ ГЛОНАСС мобильного устройства и с данными местонахождения Wi-Fi, точность определения местонахождения мобильного устройства еще более возрастает.

Управление данными местонахождения является важной функцией, поскольку она защищает критичную информацию о местонахождении владельца мобильного устройства, так же, как и, возможно, историю предыдущих и последующих его передвижений. Операторы связи являются владельцами данных о размещении сотовых узлов и управляют ими, поэтому достаточно сложно установить их политику и практику в этой области, не говоря уж об анализе и аудите. Используя GPS/ ГЛОНАСС и Wi-Fi, разработчики мобильных ОС и приложений генерируют данные местонахождения непосредственно на устройстве, что, в основном, упрощает их использование и контроль.

Если эти данные будут скрытно направлены несанкционированному адресату, это может быть очень опасно как для организации, так и для владельца мобильного устройства. Источники угрозы: производители мобильных устройств, ОС и приложений, поставщики мобильных приложений, операторы связи, администраторы мобильных устройств.

4.8.2 Отслеживание действий пользователей через приложения

Некоторые сторонние приложения, установленные оператором связи, ОС или самим пользователем, позволяют отслеживать определенные события, происходящие на устройстве. Вот примеры отслеживаемых типов событий:

- Записи о нажимаемых кнопках при наборе номера, что позволяет определить номер другого абонента;
- Данные местонахождения GPS/ ГЛОНАСС (в некоторых случаях);

• Записи о посещаемых URL (включая ресурсы HTTPS), но без содержимого этих страниц или других данных HTTP.

Источники угрозы: производители и поставщики мобильных приложений, операторы связи, администраторы мобильных устройств.

4.8.3 Маршрутизация/ переадресация

При отсутствии Соглашения о качестве предоставляемых услуг (Service Layer Agreement, SLA) с оператором связи чрезвычайно сложно установить точный путь прохождения информации от мобильного устройства через его инфраструктуру. И почти невозможно установить путь до получателя, поскольку он может включать несколько операторов связи. При мониторинге IP-сети это возможно с использованием вариаций команды traceroute, мониторинг голосовых данных и сообщений MMS/ SMS практически невозможен. Путь данных оператора связи обусловлен деловыми интересами, и может меняться в соответствии с договорными отношениями между операторами связи, экономическими связями или путями, используемыми при сбоях, отказах и восстановлении. Более того, при трансграничной передаче данных важно, обеспечивает ли путь один и тот же оператор связи, или разные, имеющие другие политику и практику обеспечения безопасности и конфиденциальности.

Учитывая неопределенность правил маршрутизации/ переадресации, следует считать все взаимодействия мобильного устройства как проходящие через несколько не доверенных сетей. Применяемые криптографические методы и протоколы должны использовать принцип «точка-точка» так, чтобы весь трафик оставался зашифрованным до того, как он будет безопасно доставлен получателю, и при этом реализовывать разрешенные криптографические алгоритмы.

4.8.4 Владение и хранение данных

Операторы связи управляют и являются владельцами различных типов данных мобильных устройств. Эти типы данных включают, в том числе, информацию о местонахождении, записи о вызовах, записи об IP-потоках, конфигурацию, идентификационные данные устройства, сообщения MMS/ SMS, электронную почту и пр. При этом достаточно сложно установить политику и практику управления операторов связи, не говоря уж об анализе и аудите.

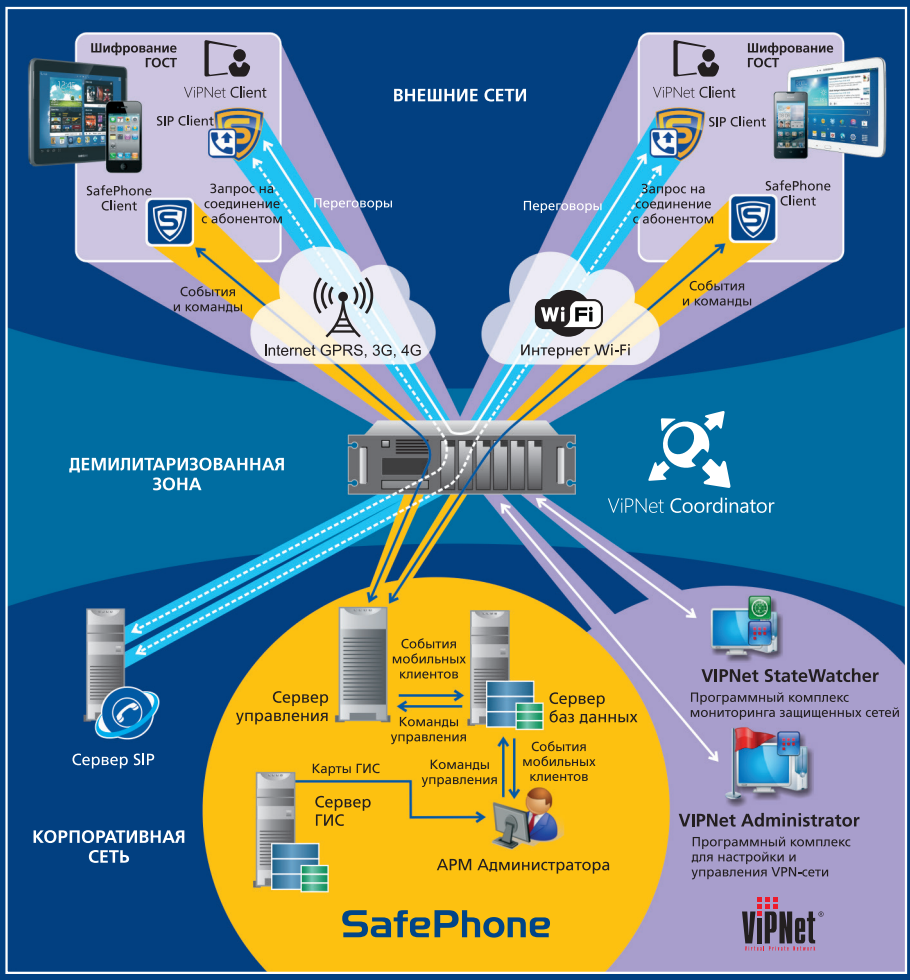
Даже если возможно заключение Соглашения о качестве предоставляемых услуг с оператором связи (что вряд ли) в части определения правил владения и хранения данных, установить, выполняется ли данное Соглашение оператором связи, практически невозможно.

4.9 Статистика угроз

Обзор «BYOD & Mobile Security Report» (2014 г.) на основе опроса 1 100 респондентов приводит статистику наиболее опасных проблем, связанных с использованием мобильных устройств (Рисунок 2).

Решение SafePhone PLUS для создания защищенных мобильных рабочих мест

- Обеспечение безопасности телефонных переговоров
- Защита мобильного устройства и информации на нем
- Защищенный доступ к корпоративным ресурсам
- Конфиденциальный обмен данными
- Безопасная мобильная видеоконференцсвязь
- Интеграция с корпоративной АТС



Экосистема решения SafePhone для обеспечения мобильной безопасности

- MDM-решение с наиболее надежной архитектурой защиты
- Дополнительные модули повышают эффект использования продукта
- Интеграция продуктами ИБ позволяет создать экосистему мобильной безопасности современного предприятия

СТАТИСТИКА НАИБОЛЕЕ ОПАСНЫХ ПРОБЛЕМ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ

5. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ

Ниже перечислены наиболее часто применяющиеся меры обеспечения безопасности мобильных вычислений.

В сотовых сетях GSM/ GPRS/ 3G (и аналогичные) и WiFi, а также в протоколе Bluetooth используются следующие стандартные криптографические алгоритмы:

1.Алгоритм аутентификации A3, алгоритмы шифрования A5/0, A5/1, A5/2, GEA1 и GEA2, A5/3, GEA3 и UEA1, алгоритм распределения ключей A8.

2.Алгоритмы, используемые для аутентификации, шифрования и генерации ключей в протоколах стандарта Wi-Fi 802.11 b/g/n: RC4 (с длиной ключа 40 и 104 бит) в протоколе WEP, RC4 (с длиной ключа 128 бит) в протоколе WPA, AES (с длиной ключа 128 бит) в протоколе WPA2.

3. Алгоритмы аутентификации и генерации ключей, используемые протоколом Bluetooth: E1, E21, E22 на базе алгоритма SAFER+ с длиной ключа 128 бит (для полноты картины безопасности беспроводных технологий).

Другие меры обеспечения безопасности мобильных коммуникаций реализуются средствами ОС мобильных платформ и/ или средствами их управления. В их числе:

1.Аутентификация, включая усиленный PIN (парольная защита устройства, приложений и данных), в т.ч. двухфакторная.

2. Шифрование данных на устройстве.

3. Удаленное управление мобильным устройством: удаление данных на устройстве, блокировка устройства, контроль, установка и удаление приложений, контроль настроек мобильного устройства.

4. Защита от вредоносного кода.

5. VPN для удаленного доступа (на уровне устройства и/или приложений).

6. Настройка и установка политики безопасности в соответствии с требованиями организации.

7. Ведение черных/ белых списков приложений и сайтов.

8.Определение и защита от взлома устройства («jailbreak» для Apple iOS или «rooting» для Google Android).

9.Трассировка с использованием GPS/ ГЛОНАСС.

Уже упоминавшийся обзор «BYOD & Mobile Security Report» (2014 г.) приводит статистику мер, направленных на минимизацию рисков, связанных с использованием мобильных устройств (Рисунок 3).

СТАТИСТИКА МЕР, НАПРАВЛЕННЫХ НА МИНИМИЗАЦИЮ РИСКОВ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ

Также следует отметить, что Агентство по информационной безопасности Министерства обороны США (Defense Information Security Agency, DISA) разработало требования по безопасности (Security Requirements Guide, SRG) для основных мобильных ОС: Apple iOS, Google Android, Windows Phone, BlackBerry при их использовании Министерством обороны США[9]. Агентство национальной безопасности США разработало Рекомендации по конфигурации безопасности для устройств Apple iOS версии 5[10].

[9] *http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html*
[10] *http://www.nsa.gov/ia/_files/os/applemac/Apple_iOS_5_Guide.pdf*

Однако возможность реализации этих рекомендаций в коммерческой сфере является проблематичной по причине их жесткости.

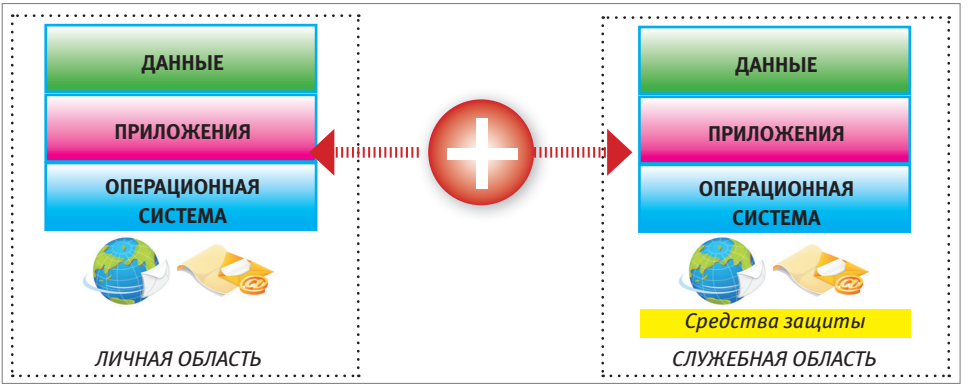
6. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ОС

6.1 Контейнер (container) или «песочница» (sandboxing).

«Песочница» или контейнер приложений – это метод разработки и/или размещения и управления мобильными приложениями, который ограничивает среду выполнения определенного кода. Цель контейнера – усилить безопасность путем изоляции приложения для предотвращения проникновения вредоносного кода, злоумышленника, а также взаимодействия защищенного приложения с системными ресурсами и другими приложениями. Термин «песочница» появился в результате аналогии с детской песочницей, где песок и игрушки находятся внутри небольшого контейнера или огороженной площадки.

«Песочница» приложений является неоднозначным решением, поскольку его полнота и надежность может создать проблемы безопасности, особенно для приложений сторонних производителей, которые это решение должно бы устранять. «Песочница» должна содержать все файлы, которые требуются для выполнения приложения, что может создать сложности для других приложений, которые должны взаимодействовать между собой. Кроме того, «песочница» использует интерфейс своего разработчика вместо оригинального интерфейса приложения, заключенного в ней. Например, если разработчик создал приложение, которое должно использовать список контактов, контейнер может стать причиной потери важной функциональности. Для предотвращения таких конфликтов разработчики решений создают дубликаты приложений и данных (список контактов, браузер, почтовый клиент и др.) для закрытой и открытой областей. Схема «песочницы» представлена на рисунке 4.

СХЕМА «ПЕСОЧНИЦЫ»



Некоторые мобильные ОС имеют встроенные средства защиты, включая контейнер, но их эффективность различна. Контейнерные приложения существуют для ОС Android, iOS, BlackBerry и Windows Phone, при этом BlackBerry предлагает приложения Secure Work Space для iOS и Android, а также BlackBerry Balance для собственных устройств BlackBerry.

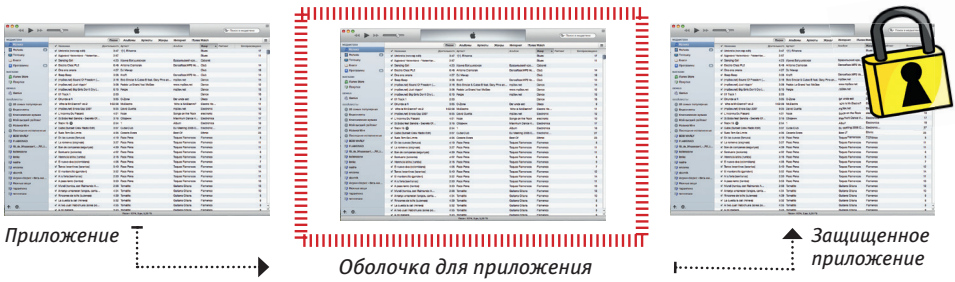
Samsung предлагает KNOX, AT&T – Toggle, а VMware предлагает контейнеры для Android от Horizon Mobile в пакете Horizon Suite.

6.2 Упаковка приложений (app wrapping).

Упаковка приложений (или оболочка для приложений) – это метод применения уровня управления к мобильному приложению без каких-либо изменений к базовому нижележащему приложению. Фактически, данный способ представляет собой «заплатку» на приложение, накладываемую библиотекой безопасности, и определяющую, как приложение и его данные должны использоваться, храниться, обрабатываться и передаваться.

Упаковка приложений позволяет администратору устанавливать специфические элементы политики к приложению или группе приложений. Элементы политики могут включать такие установки, как наличие или отсутствие аутентификации пользователя для отдельных приложений, данных, связанных с конкретным приложением и которые могут храниться на устройстве и специфических API, таких, как копирование и вставка или совместное использование данных. Упаковка приложений позволяет с каждым отдельным приложением связать определенные настройки безопасности и управления и разместить их как единую, упакованную в контейнер программу, в корпоративном хранилище приложений. Схема упаковки приложения представлена на рисунке 5.

СХЕМА УПАКОВКИ ПРИЛОЖЕНИЯ



Данный метод используют, как правило, независимые разработчики решений для управления мобильными приложениями, например: Good Technology или AirWatch (которая в январе 2014 г. была приобретена компанией VMware).

6.3 Виртуализация (virtualization).

Существует два метода виртуализации[11]: виртуализация устройств и виртуализация приложений. Изначально разработанный для настольных компьютеров, этот способ, являющийся относительно молодым для мобильных устройств, обеспечивает высокий уровень безопасности с точки зрения изоляции данных.

Виртуализация мобильного устройства – это метод его управления, при котором две виртуальные платформы установлены на одном беспроводном устройстве. Платформа – это ни-

[11]Виртуализация – предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию вычислительных процессов, выполняемых на одном физическом ресурсе (Винипедия).

железащая вычислительная система, в которой могут выполняться приложения. Например, смартфон может иметь одну виртуальную среду для служебных задач, и одну – для личных. Приложения и данные в двух средах остаются изолированными, защищая корпоративные данные. Также виртуализация мобильного устройства может позволять одному устройству функционировать под управлением двух различных ОС, что, в свою очередь, дает возможность выполнять на нем, например, приложения как для BlackBerry, так и для Android.

Виртуализация мобильных приложений по своей сути аналогична виртуальной машине для настольного компьютера. Приложение выполняется на сервере, в центре обработки данных или в облаке, при этом от клиентского устройства пересылаются необходимые данные, и на нем отображаются результаты обработки. При централизации данных вероятность их потери существенно ниже, особенно в случае, когда управление данными соответствует установленной политике безопасности. При данном способе администраторы могут создавать политики безопасности мобильных данных, позволяющие управлять устройством даже в случае его компрометации.

Виртуализация мобильных приложений может быть оптимальным решением для многих организаций, обеспечивает преимущества обработки и достижение необходимого уровня безопасности мобильных данных. Недостатком способа виртуализации является существенно более высокая загрузка канала связи, чем при использовании любых других способов. Кроме того, существенным требованием для сохранения необходимого уровня безопасности является доверие к центру обработки данных, где исполняются приложения.

Ряд производителей, таких, как VMware, Citrix, IBM и ряд других предлагают решения и услуги, помогающие администраторам «виртуализировать» корпоративные приложения.

6.4«Двойной профиль» (Dual persona).

Двойной профиль в контексте управления мобильными устройствами – это обеспечение и поддержка двух отдельных и независимых пользовательских сред на одном мобильном устройстве. Как правило, одна среда предназначена для обработки и хранения личных данных, другая – для служебных.

Цель использования двойного профиля – создать метод раздельного и защищенного хранения корпоративных приложений и данных на мобильных устройствах (как личных, так и корпоративных) работников. Для обеспечения личной конфиденциальности пользователя администраторы организации могут видеть и управлять только ресурсами в служебной среде. В случае увольнения работника служебная область может быть очищена полностью, при этом все приложения и данные в личной среде останутся в неприкосновенности. Как правило, двойной профиль предназначен для обеспечения защиты корпоративных приложений и данных и сохранения конфиденциальности личных данных при реализации стратегии BYOD.

Двойной профиль не является самостоятельным методом обеспечения безопасности мобильного устройства, скорее, это концепция реализации перечисленных выше способов. Одним из методов реализации двойного профиля является виртуализация мобильно-

го устройства с использованием «гипервизора» (hypervisor) для разделения аппаратных ресурсов между двумя ОС на одном мобильном устройстве. VMware Horizon Mobile для Android – это пример продукта, обеспечивающего виртуализацию мобильного устройства.

Другой метод реализации двойного профиля – создание контейнера («песочницы») для служебной среды путем установки клиента или с использованием возможностей самой ОС. Контейнер, функционирующий как обычное приложение или процесс ОС, позволяет администраторам устанавливать политики безопасности для служебной среды, которые при этом никак не взаимодействуют с личной средой мобильного устройства. Примерами таких политик безопасности являются парольная защита, удаленное стирание данных, установка времени доступа к корпоративным данным. Подобный метод реализован, например, в BlackBerry OS приложением BlackBerry Balance (входит в состав ОС).

7. ТЕХНОЛОГИИ И ФУНКЦИИ УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ И ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ

7.1 Управление мобильными устройствами (Mobile Device Management, MDM)

Управление мобильными устройствами (MDM) – это способ администрирования, включающий внедрение, обеспечение безопасности, мониторинг, интеграцию с корпоративными ресурсами и управление мобильными устройствами. Назначение MDM – оптимизировать функциональность и безопасность мобильных устройств в корпоративной информационной инфраструктуре, обеспечивая также при этом защиту корпоративной системы от угроз, связанных с использованием мобильных устройств.

Программное обеспечение для управления мобильными устройствами позволяет распространять приложения, данные, настройки конфигурации, политики и «заплатки» на мобильные устройства. Кроме того, MDM предоставляет возможность администраторам наблюдать и контролировать мобильные устройства так же, как настольные компьютеры, а также обеспечивать баланс между оптимальной производительностью для пользователя и обеспечением безопасности. Инструментарий MDM, как правило, включает управление приложениями, синхронизацию и совместное использование файлов, средства обеспечения безопасности, а также поддержку принятой в организации стратегии использования мобильных устройств (COPE, BYOD или другой).

MDM может стать полезным инструментом для бизнеса, обеспечивающим контроль и управление смартфонами и другими портативными устройствами, находящимися у работников. В качестве первого шага необходимо четко определить цели и задачи системы MDM, соответствующие политике безопасности организации (которая должна быть принята ранее). Ниже приведен перечень функций и возможностей MDM, который поможет определить те из них, которые наиболее критичны для организации.

1. *Учет мобильных устройств и их параметров.*

MDM должна поддерживать список контролируемых устройств. Необходимо определить способы и методы учета устройств и актуализации их перечня.

Учет устройств: какие физические параметры необходимо отслеживать? Помимо базовых (ID устройства, аппаратная модель, версия ОС) MDM может учитывать и другие параметры, как-то: беспроводной адаптер, внешняя память и др.;

Классификация: каким образом сгруппированы мобильные устройства? Например, MDM может автоматически классифицировать устройства по типу, версии ОС или состоянию (неизвестно, авторизовано, инициировано, списано);

Поддержка: каким образом осуществляется обновление устройств и отражаются дополнения, изменения, удаления? MDM может использоваться для периодического опроса устройств, проверки изменений при наличии подключения или проведения внепланового аудита;

Физическая трассировка: необходимо ли знать не только владельца портативного устройства, но и его точное физическое местоположение? Многие смартфоны оснащены функцией GPS/ ГЛОНАСС, поэтому MDM имеют возможность геопозиционирования устройства;

Интеграция с базами данных: имеются ли системы учета других ресурсов (настольных компьютеров, серверов и др.)? Если да, то есть возможность интеграции записей об учтенных мобильных устройствах с общими репозиторями путем экспорта записей или отчетов.

2. Инициализация мобильных устройств.

Управление жизненным циклом устройства начинается с его активации и инициализации. Каким образом каждое новое устройство становится авторизованным и пригодным к использованию в парке портативных устройств и в информационной инфраструктуре организации в целом?

Поддерживаемые платформы: какие платформы (например, Apple iOS, Google Android, BlackBerry OS, Microsoft Windows Phone) и минимально разрешенные модель/ версия (например, Samsung SAFE с версией Android 4 и выше) должны поддерживаться? Управление устройствами зависит от множества характеристик, включая ОС и связку «производитель – модель – версия». Следует использовать независимое от устройства управление, если это возможно, за исключением специфичных для конкретных устройств функций (например, удаленное удаление данных);

Регистрация устройства: как планируется регистрировать устройство? MDM могут разрешить только администратору регистрировать служебные устройства, позволить пользователю регистрировать собственное устройство или реализовать комбинацию этих функций;

Активация агента: каким образом программное обеспечение MDM будет установлено и активировано на каждом новом устройстве? Некоторые мобильные устрой-

ства могут использоваться с «родными» MDM (например, Apple iOS, BlackBerry OS), другие могут требовать обращения к хранилищу приложений для загрузки и установки агента MDM. В последнем случае активация, как правило, завершается при получении каждым устройством сообщения, содержащего ссылку для установки агента «по воздуху»;

Конфигурация устройства: каким образом настройки по умолчанию от производителя или провайдера будут переопределены в соответствии с требованиями организации? Например, может быть необходима установка парольной защиты, добавление ключа реестра или перезапись меню для удаления неслужебных приложений. MDM может применить заранее подготовленную «стандартную конфигурацию» к каждому устройству после первичной активации или аппаратной перезагрузки.

3. Распространение мобильного программного обеспечения.

Многие MDM имеют гораздо больше функций, чем просто учет и конфигурация устройств, включая доставку и обновление мобильных приложений. Это не является основной задачей (это, скорее, задача MAM, см. ниже), но такая возможность достаточно важна.

Пакеты программного обеспечения: как предполагается упаковывать необходимые приложения для их конфигурации и доставки? MDM может определять и развертывать эти пакеты с учетом платформы, объема памяти и зависимости одного приложения от другого;

Распространение приложений: приложения и обновления предполагается загружать с общедоступных хранилищ (например, Apple iTunes, Google Play), доставлять с корпоративного хранилища или использовать комбинацию этих или других способов? Каждая мобильная ОС использует собственные правила в зависимости от полномочий пользователя, необходимых для установки и обновления приложений, однако MDM могут автоматизировать соответствующие процессы (например, запрашивать пользователей при установке необходимого общедоступного приложения);

Оптимизация: организация должна использовать доверенные или общие глобальные сети? Некоторые MDM обеспечивают сжатие, поэтапное обновление и управление пропускной способностью канала (например, разрешая установку только при наличии «быстрого» канала связи);

Контроль изменений: как часто мобильные приложения должны обновляться, или проверяться на наличие «заплат»? Необходимо определить способы тестирования обновлений и «заплат» для того, чтобы их применение не заблокировало приложение или устройство.

4. Управление мобильной безопасностью.

Для портативных устройств процессы управления самими устройствами и их безопасностью неотделимы. Многие системы MDM предоставляют функции управления безопас-

ностью, которые отсутствуют в мобильных ОС или необходимы для обеспечения задач, решаемых на устройстве.

Аутентификация пользователя (в т.ч. двухфакторная): как необходимо аутентифицировать пользователя для предоставления доступа к мобильному устройству? Необходима ли двухфакторная аутентификация и если да, то какого типа? Некоторые MDM могут быть интегрированы с корпоративными каталогами, и доступ к мобильному устройству и/или приложению может регламентироваться общими правилами;

Применение парольной политики: сколько попыток доступа разрешено до блокировки или перезагрузки устройства? Каковы требования к качеству пароля? Разрешено ли совершать экстренные вызовы в обход аутентификации? Многие агенты MDM могут применять эти и другие парольные политики, помимо встроенных в ОС (как правило, это просто PIN);

Удаленная очистка устройства: необходима ли возможность полной удаленной очистки мобильного устройства? Например, многие MDM позволяют удалить данные или вернуться к настройкам по умолчанию на утерянном устройстве при его подключении к сети или с помощью SMS типа «kill pill»;

Белые/ черные списки и ограничения на устройство: MDM, имеющие возможность управлять приложениями (или MAM) могут разрешать установку одних приложений и запрещать установку других. Также MDM могут контролировать настройки устройства и блокировать потенциально опасные интерфейсы и другие опции (например, Wi-Fi, Bluetooth, GPS/ ГЛОНАСС, камера и др.);

Защищенные коммуникации: насколько критичен трафик MDM (например, изменение конфигурации, установка приложений)? Некоторые MDM обеспечивают защищенный с использованием криптографических средств канал (VPN[12]) своими средствами, отличными от средств ОС или сторонних приложений. Также MDM/ MAM своими средствами или средствами сторонних приложений могут обеспечивать корпоративный VPN-канал на уровне «устройство – шлюз сети» или «приложение – сервер».

5. Защита мобильных данных

На мобильном портативном устройстве наиболее критичным активом организации зачастую являются именно данные. MDM (как и другие средства управления) могут обеспечить сохранность и защиту мобильных данных.

---

[12] *VPN (Virtual Private Network – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений). В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть (Википедия).*

Шифрование данных: необходимо ли применять политику аппаратного или программного шифрования для предотвращения несанкционированного доступа к данным на мобильном устройстве? Многие современные мобильные устройства реализуют функцию аппаратного шифрования, другие позволяют реализовать политику шифрования путем установки или активации сторонних криптографических приложений (например, внутри контейнера или корпоративного приложения);

Резервное копирование и восстановление: как предотвратить потерю данных, если мобильное устройство украдено или повреждено? Большинство мобильных устройств поддерживает для авторизованных пользователей плановое резервное копирование определенных настроек и данных в облачную службу резервного копирования «по воздуху». Следует определить необходимость и объекты резервного копирования;

Трассировка данных: есть ли необходимость ведения системного журнала, регистрирующего перемещения данных с мобильного устройства и на него? Некоторые MDM позволяют контролировать и регистрировать перемещение критичных данных на съемный носитель или на другие устройства при синхронизации, в т.ч. «по воздуху».

6.Мониторинг и служба поддержки

Некоторые функции MDM могут хотя бы частично оправдать собственную стоимость за счет уменьшения стоимости поддержки управляемых устройств.

Самопомощь: некоторые MDM предоставляют порталы, разрешающие пользователям самостоятельную регистрацию устройства, восстановление или изменение пароля, загрузку приложений, резервное копирование и восстановление данных. Необходимо определить, насколько эти возможности согласуются с корпоративной политикой безопасности;

Диагностика: что должна видеть служба поддержки, когда возникает проблема? MDM может сыграть важную роль не только обеспечивая необходимые настройки, но предоставляя информацию о статусе и текущих параметрах устройства в реальном времени;

Удаленный контроль: что делает служба поддержки, когда удаленный пользователь нуждается в помощи? Многие MDM имеют функции удаленного контроля, которые позволяют персоналу взаимодействовать со сторонними устройствами в режиме реального времени;

Аудит и контроль соответствия: соответствует ли мобильное устройство утвержденной корпоративной политике и/ или другим нормативным и распорядительным документам? MDM может автоматически удаленно осуществлять оценку и корректировку настроек устройства, а также сообщать об их соответствии утвержденной политике;

Отчет об операциях: насколько важна отчетность о действиях мобильных пользователей, включая взаимодействие с корпоративными сетями и серверами или внешними ресурсами? Большинство MDM обеспечивают регистрацию событий, генерируемых мобильными устройствами, которые могут быть использованы для ретроспективного анализа. Важно только, чтобы система регистрировала действительно необходимые события.

Вряд ли какая-либо корпоративная система нуждается в реализации всех перечисленных функций, так же, как и какая-либо отдельная MDM предоставляет их все. Некоторые из перечисленных функций – это вариации аналогичных функций для настольных компьютеров, некоторые специфичны для мобильных устройств. Необходимо четко определить ключевые и дополнительные функции, подобрать MDM, наиболее полно и корректно реализующую их, и затем зафиксировать функции, настройки, условия в политике безопасности (раздел 8).

С административной точки зрения желательно, чтобы система управления мобильными устройствами обладала следующими свойствами:

- Совместимость с используемыми в организации мобильными ОС, платформами и приложениями;
- Возможность функционирования с различными поставщиками услуг;
- Возможность взаимодействия с различными мобильными устройствами непосредственно «по воздуху» и в реальном времени;
- Возможность быстрого внедрения мобильных платформ, ОС и приложений следующего поколения;
- Возможность быстрого добавления и удаления устройств из системы для обеспечения эффективности функционирования и безопасности корпоративной системы.

Обзор «BYOD & Mobile Security Report» (2014 г.) приводит следующую статистику наиболее важных функций систем MDM (Рисунок 6).

СТАТИСТИКА НАИБОЛЕЕ ВАЖНЫХ ФУНКЦИЙ СИСТЕМ MDM

7.2 Управление мобильными приложениями (Mobile Application Management, MAM)

Управление мобильными приложениями – это совокупность процессов распространения и администрирования программного обеспечения на корпоративных смартфонах и планшетах конечных пользователей. В отличие от систем управления мобильными устройствами (MDM), которые сосредоточены на активации, регистрации и обеспечении функционирования и безопасности мобильных устройств, системы управления мобильными приложениями сфокусированы на распространении, лицензировании, настройке, поддержке, контроле использования и применении политик для мобильного программного обеспечения.

Многие системы управления мобильными приложениями имеют возможность сравнивать тип мобильного устройства, владельца, пользователя и группу с определенными администратором политиками, определяя при этом, какие мобильные приложения могут быть установлены на новом устройстве при его активации. Важное требование к системам управления мобильными приложениями – это возможность удаления администратором корпоративных приложений и данных с устройства конечного пользователя, а также предотвращение дальнейшего доступа к корпоративным приложениям и данным в случае отсутствия физического контакта с устройством.

MAM использует контейнеры и упаковку приложений для защиты корпоративных данных, хранящихся в мобильных приложениях, вне зависимости от того, это сторонние промышленные или собственные приложения. Изоляция служебных приложений от личных, а также упаковка корпоративных приложений на уровне защищенного кода позволяет администратору управлять только служебными приложениями, оставляя личные без внимания.

Одна из главных задач при распространении корпоративных приложений – какое доверенное хранилище приложений выбрать или создать? Доверенное хранилище приложений, которые могут использоваться в служебных целях – это одна из основ безопасного использования мобильных устройств организацией. Существует несколько подходов к решению данной задачи.

Один из них – создание собственного, корпоративного хранилища приложений. При решении задачи о целесообразности создания собственного хранилища следует получить ответы на следующие вопросы:

- Существуют ли в вашей компании реалистичные цели создания корпоративного хранилища приложений?
- Каким образом предполагается убедиться, что корпоративное хранилище приложений достигнет указанных целей?
- Каким образом предполагается наполнять корпоративное хранилище приложений и быть уверенным в том, что их можно считать доверенными?
- Осознает ли организация, что создание корпоративного хранилища приложений влечет решение дополнительных задач, таких, как установка строгой политики использования приложений (особенно при использовании концепции BYOD) или требование о контроле использования приложений на мобильных устройствах работников?

Лучшими основаниями для создания корпоративного хранилища приложений являются обеспечение безопасности и соответствие корпоративным (ведомственным) стандартам и требованиям. Две основные проблемы безопасности, которые может решить данный подход – это возможность заражения корпоративных приложений вредоносным кодом через небезопасные каналы распространения приложений, и неумышленное раскрытие конфиденциальной информации сторонним лицам. Возможность ограничения доступа работников к потенциально небезопасным приложениям и/или каналам их распространения значительно снизит риски безопасности организации.

Другая цель, оправдывающая создание корпоративного хранилища приложений – это размещение собственных, разработанных в организации приложений. Делая такие приложения столь же доступными, как и другие, многие компании отмечают, что работники предпочитают именно их. Кроме того, затраты на загрузку и поддержку собственных приложений могут быть сравнимы с аналогичными затратами для сторонних приложений.

Вместе с тем, необходимо отметить, что создание корпоративного хранилища приложений требует разовых временных и финансовых затрат, и для их администрирования и поддержки нужен высококвалифицированный, именно в данной области, персонал.

Корпоративное хранилище приложений обеспечивает платформу доставки мобильных приложений, с помощью которой работники организации могут просматривать и загружать разрешенные к использованию приложения. Однако такое хранилище – это гораздо больше, чем просто каталог. Как правило, это часть глобальной стратегии MAM, которая помогает службе ИТ контролировать безопасность приложений и следить за их соответствием определенным стандартам и требованиям, обеспечивать достоверность данных, массовую закупку и лицензирование.

У организаций есть несколько возможных способов реализации корпоративного хранилища приложений. Один из них – создать собственное хранилище с использованием средств разработки типа StrongNode или Titanium Studio. С их помощью можно установить хранилище внутри организации или у поставщика облачных услуг, предоставляющего сервис PaaS.

С другой стороны, организация может приобрести готовую систему MAM и также либо установить хранилище внутри организации, либо у поставщика услуг PaaS. Такие компании, как Symantec, MobileIron и App47 предлагают решения MAM как программные комплексы. Кроме того, эти и ряд других компаний сами предоставляют облачные сервисы, позволяющие организациям реализовать виртуальное частное корпоративное хранилища приложений (private enterprise app store, VPEAS). Такие услуги предоставляют многие компании, например, Apperian, BMC, FullArmor и Salesforce.

Другой подход – использование для нужд организации существующих потребительских сервисов, таких, как Dropbox для хранения и распространения файлов. В этом случае работники могут просто обратиться к Google Play, Apple's App Store или любому другому общедоступному хранилищу для загрузки приложений Dropbox на свои мобильные устройства. Проблема этого подхода в том, что компания подвергает риску свои критичные данные и открывает возможность использования приложений в неслужебных целях при

сложности контроля и мониторинга приложений. Некоторые потребительские сервисы предлагают корпоративные альтернативы, например, Dropbox for Business, однако даже при их использовании риски и проблемы безопасности и администрирования остаются.

Учитывая это, многие организации опробуют другие методы распространения и управления мобильными приложениями и услугами, включая реализацию корпоративного хранилища приложений, доступ к мобильным сервисам посредством частных облаков, разработку Web-ориентированных приложений или реализацию виртуальной мобильной машины.

Таким образом, существуют различные подходы к созданию корпоративного хранилища мобильных приложений. При этом между граничными способами (только внутреннее хранилище, полностью внешнее хранилище) можно выбрать промежуточные, некоторые из которых описаны выше. Также существует возможность использования корпоративного хранилища или «доверенной третьей стороны» (trusted third-party), например, оператора мобильной связи.

При выборе способа создания корпоративного хранилища мобильных приложений необходимо ориентироваться на баланс выгоды и риска. С одной стороны – безопасность, контролируемость, минимизация риска при существенных затратах. С другой стороны – простота и удобство использования при увеличении рисков и снижении общего уровня безопасности.

7.3 Управление мобильными данными (Mobile Information Management, MIM)

На английском языке это понятие корректнее называть Mobile Data Management, однако тогда его аббревиатура, MDM, будет совпадать с уже устоявшимся понятием Mobile Device Management. Иногда MIM обозначают как Mobile Content Management (MCM).

MIM – это независимая от устройства стратегия безопасности, обеспечивающая хранение критичных данных в зашифрованном виде и позволяющая только доверенным приложениям их обработку и передачу.

Несмотря на перспективы, развитие систем управления мобильными данными встречает определенные сложности при продвижении на рынке систем управления корпоративной мобильностью. Главная трудность состоит в интеграции, поставщики таких систем должны проектировать стандарты или становиться партнерами производителей и разработчиков с тем, чтобы устройства и приложения последних могли считывать и обрабатывать установленную на данных защиту. Как правило, в контексте безопасности MIM связывается с MDM и MAM, т.е. управление данными обычно является одной из функций или опций систем управления устройствами (путем создания контейнера для критичных данных) и/или приложениями (путем установки политики для приложений, обрабатывающих или передающих критичные данные). Например, система управления мобильными устройствами BlackBerry Enterprise Server 10, управляющая ОС BlackBerry OS, Google Android, Windows Phone и Apple iOS, имеет некоторые возможности управления мобильными данными.

В совокупности эти три способа (MDM, MAM и MIM) иногда обозначают как MxM.

8. КОРПОРАТИВНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ МОБИЛЬНЫХ ТЕХНОЛОГИЙ

Корпоративная политика безопасности мобильных технологий – это набор правил, определяющих использование и обеспечение безопасности мобильных устройств в корпоративной сети. Она обязательна к применению, должна быть доведена до сведения всех работников, использующих мобильные устройства, основываться на корпоративной модели угроз и должна включать, как минимум, следующие разделы:

1. Цели и задачи. Любая организационная политика вряд ли достигнет целей, диктуемых бизнесом, если назначение политики четко и ясно не соотносится с целями бизнеса. Необходимо кратко обосновать, почему безопасность мобильных устройств важна для бизнеса – будь то соответствие нормативным и другим требованиям, снижение затрат или защита клиентов – а также описать, как политика способствует достижению этих целей.

2.Область применения. Необходимо охарактеризовать, какие устройства подпадают в область применения политики, и какие – нет. Например, необходимо указать, затрагивает ли политика личные и/или служебные устройства, а также перечислить их типы (например, смартфоны, планшеты или другие) или даже указать разрешенные и запрещенные модели.

3. Допустимая область применения мобильных устройств. Укажите условия, разрешающие доступ и/или хранение служебных данных на мобильных устройствах. Например, должны ли работники давать согласие на мониторинг, управление, очистку и физическое изъятие устройства, или же это определено изначально и работники только должны быть ознакомлены с этими правилами? Какими данными может владеть работник, какие при этом полномочия назначены пользователю мобильного устройства в соответствии с данной политикой? Также целесообразно определить явно запрещенные области применения мобильных устройств в организации.

4. Применяемые политики (безопасности). Необходимо определить требования защиты мобильных устройств (в т.ч. мобильных данных), включая обязательные и рекомендуемые меры. Например, необходимо определить требования по использованию PIN устройства, требования по парольной защите, включая минимальную длину, сложность, частоту смены и период неактивности. Также необходимо определить допустимые криптографические методы и алгоритмы для хранимых и передаваемых данных, включая характеристики данных, к которым они должны быть применены. В зависимости от типа используемых устройств и функций системы управления могут использоваться различные методы, перечисленные в разделе 5.

5. Обеспечение исполнения. Необходимо определить, как организация будет контролировать использование и настройки мобильных устройств, какие шаги будут предприняты для обеспечения соответствия политике. А также, какие юридические

меры и организационно-штатные меры со стороны подразделений кадров и безопасности будут предприняты в случае неправомерного использования мобильных устройств.

6. Ответственность. Определите задачи, которые должны решать руководство и работники организации в отношении защиты мобильных данных. Например, в чьей ответственности находится резервное копирование и восстановление? Какие действия должен предпринять работник для немедленного стирания данных?

7. Определения. Не следует думать, что пользователи понимают сленг мобильных технологий или безопасности. Политика часто использует технические термины, поэтому желательно определить, что они означают в контексте данной политики.

При составлении политики безопасности необходимо иметь предварительно утвержденную модель угроз, а затем целесообразно сформулировать ответы на следующие вопросы:

- Какие корпоративные данные и ресурсы наиболее значимы и/или критичны?
- Как организация может обеспечить наилучший баланс между выгодой и риском при предоставлении мобильным пользователям доступа к корпоративным данным и ресурсам?
- Какие корпоративные данные, как и кем могут быть загружены на мобильное устройство и какие данные должны оставаться внутри корпоративной сети?
- Какие, как, откуда и кем (корпоративные) приложения могут быть установлены на мобильном устройстве, и какие приложения и/или их источники должны быть запрещены?
- Какие типы технологий, решений и средств обеспечения безопасности доступны для мобильных устройств и каковы условия их применения?

Для уменьшения риска утери или компрометации данных в зоне ответственности оператора связи, следует использовать и отразить в политике безопасности организации следующие рекомендации:

- Считать все каналы передачи данных устройства как небезопасные (голос, данные, MMS/ SMS);
- Если возможно, удалите все критичные данные с устройства, если нет – используйте шифрование всех критичных данных (полностью, в контейнере или отдельных файлов);
- Сконфигурируйте устройство с идентификаторами, не относящимися к специфичным для организации;
- Адаптируйте технологии виртуализации и/ или контейнера («песочницы») для хранения критичных данных;

- Тесно взаимодействуйте с оператором связи, который должен понимать аспекты данной проблемы, и, по возможности, заключите с ним Соглашение о качестве предоставляемых услуг, включающее обязательства оператора связи по владению и хранению ваших данных.

Обзор «BYOD & Mobile Security Report» (2014 г.) приводит следующую статистику наиболее важных положений, которые должны быть отражены в политике безопасности мобильных устройств (Рисунок 7).

СТАТИСТИКА НАИБОЛЕЕ ВАЖНЫХ ПОЛОЖЕНИЙ В ПОЛИТИКЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ

9. ПРОЕКТИРОВАНИЕ МОБИЛЬНОГО БИЗНЕСА И ОБЕСПЕЧЕНИЕ ЕГО БЕЗОПАСНОСТИ

Построение или развитие мобильного бизнеса целесообразно осуществлять поэтапно, от ключевых организационных положений к конкретной технической реализации.

1. *Обследование.*
   - Определение мобильных бизнес-процессов;
   - Определение парка мобильных устройств;
   - Определение парка мобильных приложений;
   - Определение технологий подключения к корпоративной сети;
   - Определение существующих систем типа MDM/ MAM/ MIM (MxM) – при их наличии.
2. *Анализ рисков, разработка модели угроз и модели нарушителей.*

3. Разработка политики безопасности мобильного бизнеса.

4. Проектирование системы обеспечения (безопасности) мобильного бизнеса.

- Выбор или адаптация существующей системы управления типа MxM, разработка параметров их настройки;
- Выбор из существующих или разработка доверенного хранилища мобильных приложений и данных;
- Выбор и/или разработка средств и методов обеспечения безопасности мобильных бизнес-процессов, устройств, приложений и данных (из перечня доступных);
- Разработка конкретных политик и настроек для мобильных устройств и приложений.

5. Реализация системы обеспечения мобильного бизнеса.

- Приобретение и/или настройка системы управления типа MxM в соответствии с разработанной политикой и параметрами;
- Применение разработанных политик и реализация способов и методов обеспечения безопасности мобильных устройств, приложений и данных;
- Регистрация (перерегистрация) мобильных устройств и приложений;
- Разработка эксплуатационной и нормативно-распорядительной документации.

6. Подбор и обучение обслуживающего персонала и/ или выбор партнера для внешнего (включая облачное) управления и обслуживания.

7. Испытания и опытная эксплуатация.

8. Ввод в промышленную эксплуатацию, техническая поддержка и сопровождение.

ЗАКЛЮЧЕНИЕ

В настоящее время во многих организациях планируется или уже реализовано использование мобильных технологий в бизнес-процессах. Но при этом зачастую отсутствуют знание или понимание возможностей, подводных камней, опасностей и других нюансов этих технологий. Получение служебной электронной почты на мобильное устройство реализовано во многих организациях, но даже такой простой процесс может быть уязвим, если в почте содержатся критичные для организации данные, а само мобильное устройство не имеет дополнительных средств или настроек безопасности, или же вообще не управляется централизованно.

Данная публикация – это попытка (общая, но далеко не полная) описать возможности мобильных технологий для корпоративного использования с основными «pro» и «contra». Многие бизнес-процессы организации могут быть усовершенствованы с использованием мобильных технологий. Главное – понимать, какие бизнес-процессы можно «мобилизировать», для чего это нужно (цель?) и каков ожидаемый результат.

Примеры:

- Корпоративная электронная почта;
- Корпоративный электронный документооборот;
- Международные и российские информационные и информационно-финансовые системы (Reuters, Bloomberg и др.);
- Корпоративные информационные, кадровые, бухгалтерские и другие системы;
- Системы «Клиент – Банк» и пр.

Важный для планирования мобильного бизнеса вопрос: передачу данных предполагается осуществлять только в части обмена информацией мобильного пользователя с корпоративной системой или еще и для совершения, например, финансовых транзакций или других критичных операций, которые могут нанести реальный финансовый ущерб? В последнем случае риски возрастают многократно. При этом необходимо сформулировать четкие ответы на вопросы «как это сделать?» и «чем это грозит?». Есть ли персонал, способный решать эти вопросы? Во всем этом следует разобраться досконально, иначе возможны проблемы, многие из которых здесь описаны.

В заключение следует отметить, что если способы и процедуры обеспечения информационной безопасности для классических, не мобильных, систем хорошо известны, правильно реализованы и даже во многом стандартизованы, то область безопасности мобильных технологий – пока во многом «terra incognita». Отсутствуют «работоспособные» российские стандарты или рекомендации, а специалистов пока просто мало. В России еще только формируются специалисты и даже организации, специализирующиеся на практических вопросах обеспечения ИБ при применении мобильных технологий в бизнесе. Но еще предстоит большая работа, поскольку область применения мобильных технологий в организациях для облегчения или совершенствования бизнес-процессов весьма перспективна.

Также следует отметить, что перечисленные средства и методы применимы не только для обеспечения безопасности мобильных технологий при взаимодействии работника организации – пользователя мобильного устройства с публичной, ведомственной, корпоративной или другой системой, но и для обеспечения безопасности при межмашинном взаимодействии[13]. Более подробно технологии M2M, средства и методы обеспечения их безопасности будут рассмотрены в следующих версиях данной публикации.

---

[13] Межмашинное взаимодействие (машинно-машинное взаимодействие, Machine-to-Machine, M2M) – общее название технологий, которые позволяют машинам обмениваться информацией друг с другом, или же передавать ее в одностороннем порядке. Это могут быть проводные и беспроводные системы мониторинга датчиков или каких-либо параметров устройств (температура, уровень запасов, местоположение и т. д.). К примеру, банкоматы или платежные терминалы могут автоматически передавать информацию по GSM-сетям, а также, если у них закончилась чековая бумага или наличность, или же наоборот, что наличности слишком много и требуется приезд инкассаторов. M2M также активно используется в системах безопасности и охраны, вендинге, системах здравоохранения, промышленных телеметрических системах (производство, энергетика, ЖКХ и др.) и системах позиционирования подвижных объектов на основе систем GPS/ ГЛОНАСС. Одним из подклассов M2M является межмашинное взаимодействие с использованием мобильных решений, для него также может использоваться аббревиатура M2M (Mobile-to-Mobile). Такое определение дает Википедия.

Изложенное является составляющими элементами стратегии Enterprise Mobility Management (EMM) – управление корпоративными мобильными технологиями. EMM – это совокупность персонала, процессов и технологий, предназначенных для управления комплексом мобильных устройств, беспроводных сетей и соответствующих сервисов для обеспечения мобильных операций в интересах бизнеса. При этом обеспечение безопасности – лишь часть EMM. EMM также подразумевает оптимизацию, увеличение производительности, ускорение бизнес-процессов с использованием мобильных технологий.

В свою очередь, EMM является частью стратегии Endpoint (Security) Management, т.е., управление (безопасностью) совокупностью оконечных устройств организации. Она определяет политику и правила управления всеми оконечными устройствами организации, включая мобильные устройства всех типов, ПК, серверы и пр. Было бы логично при планировании EMM организации учитывать устоявшиеся правила, средства и практику управления другими устройствами, а еще лучше – интегрировать EMM в существующую систему управления и инфраструктуру в целом. Это будет способствовать тому, что EMM станет составной работоспособной и неотъемлемой частью обеспечения (безопасности) бизнес-процессов организации, а не очередной модной игрушкой.

Таким образом, использование мобильных технологий в бизнес-процессах организации перспективно и выгодно, но при выполнении следующих условий:

- Определены концепция и стратегия использования мобильных устройств и технологий в организации;
- Определены бизнес-процессы и оценена выгода от использования мобильных технологий в них;
- Проведена оценка угроз и рисков;
- Четко сформулирована и реализована политика безопасности использования мобильных технологий в организации;
- Реализована техническая инфраструктура управления мобильными технологиями, включая хранилище данных и приложений, а также средства и методы обеспечения безопасности, интегрированная с общей информационной инфраструктурой организации.

Грамотно оценить и соотнести перечисленные условия возможно только квалифицированному персоналу или доверенным консультантам. Только тогда «мобилизация» бизнес-процессов принесет выгоду, а не вред.

Есть замечания и/или предложения?
Контакты на сайте АРСИБ: www.aciso.ru.

Ждите следующих версий...

Издание подготовили:

Издатель – Виктор Минин
Автор – Александр Першин
Экспертная группа –
М. Одувалов, Г. Фалькович, Н. Носов, А. Макар, В. Минин.

Распространяется бесплатно.
©АРСИБ, 2015 г.
aciso.ru email: info@aciso.ru