Обеспечение безопасности мобильных устройств на предприятии

Безмалый В.Ф.
MVP Consumer Security
Microsoft Security Trusted Advisor

Сегодняшняя ситуация в мире смартфонов

В последнее время во всем мире наблюдается резкий рост числа смартфонов, используемых как в персональных целях, так и в корпоративных.

Сегодняшние темпы развития и расширение использования мобильных технологий в деловой среде являются факторами, требующим серьезного внимания со стороны корпоративных ИТ. Проникновение потребительских смартфонов и планшетов в корпоративную среду стало носить массовый характер.

“Революция планшетов”, инициированная iPad (см. Morgan Stanley Blue Paper “Tablet demand and disruption. Mobile Users Come of Age.”, февраль 2011), и широкое распространение смартфонов разных ценовых категорий на базе Android (см. Gartner report “Market Share: Mobile Communication Devices by Region and Country, 3Q11”) привели к тому, что мобильные технологии вошли в Top 3 технологических приоритетов CIO в 2011 году (см. Gartner CIO Agenda survey 2011).

Качественное расширение пользовательского опыта (user experience), связанное с расширением спектра доступных форм-факторов смартфонов и планшетов, обеспечило возможность не только ограниченного потребления информации, но и активной “диалоговой” реакции со стороны пользователей мобильных устройств, предполагающей взаимодействие с информационными ресурсами и прикладными системами. Эти мобильные устройства фактически сформировались в новый класс рабочих мест (workplace) -мобильные рабочие места.

Корпоративная мобильность – способность организации предоставить возможность и использовать преимущества повсеместного, безопасного, своевременного (оперативного), удобного мобильного доступа сотрудников к корпоративным информационным ресурсам и системам со смартфонов и планшетов.

Компании и организации стали задумываться о более четкой регламентации использования мобильных устройств (и корпоративных, и личных) и формировании целостного видения в отношении мобильных технологий, предполагающего не только расширение прикладной функциональности, доступной мобильным пользователям, но и возможности оптимизации, а также развития существующих бизнес-процессов с учетом практически постоянной “подключенности” мобильных пользователей.

Согласно опроса, проведенного 13 октября 2011 года Центром корпоративной мобильности АйТи (http:/mobility.it.ru) большинство респондентов отмечают значимость организационных решений в отношении использования мобильных технологий и устройств в компаниях и организациях. При этом 68% из них уже разработали либо планируют разработать стратегию, политики и регламенты корпоративной мобильности, подтверждая насущную необходимость решения задач, связанных с использованием мобильных устройств в организациях.

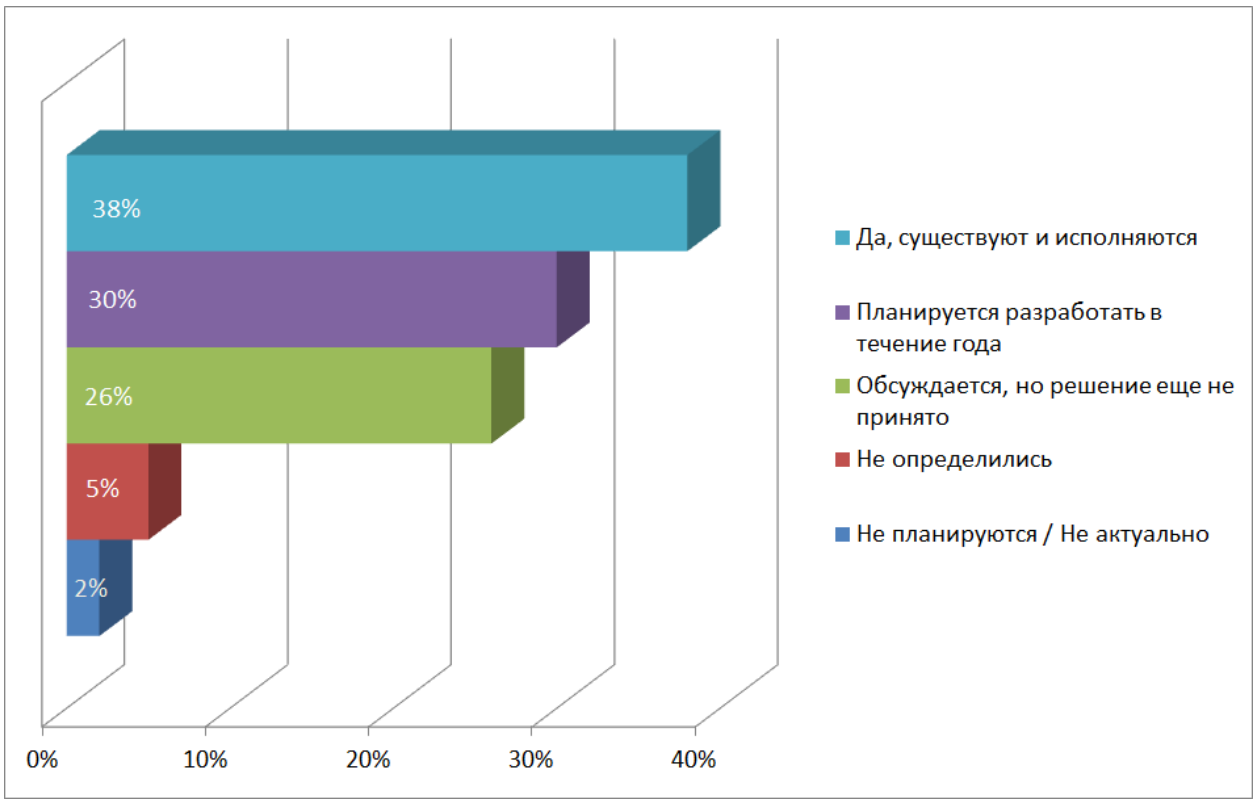

Рисунок 1 Наличие в организациях стратегии, политик и регламентов использования мобильных технологий и устройств (смартфонов и планшетов)

Высокое внимание к мобильным технологиям не связано с модой на iPad в руках руководителя, а является ответом на реальные потребности организаций в улучшении коммуникаций и бизнес-процессов. Важно отметить, что сами сотрудники часто озвучивают такие потребности и инициируют соответствующие запросы, желая использовать преимущества мобильного доступа к корпоративным информационным системам и ресурсам.

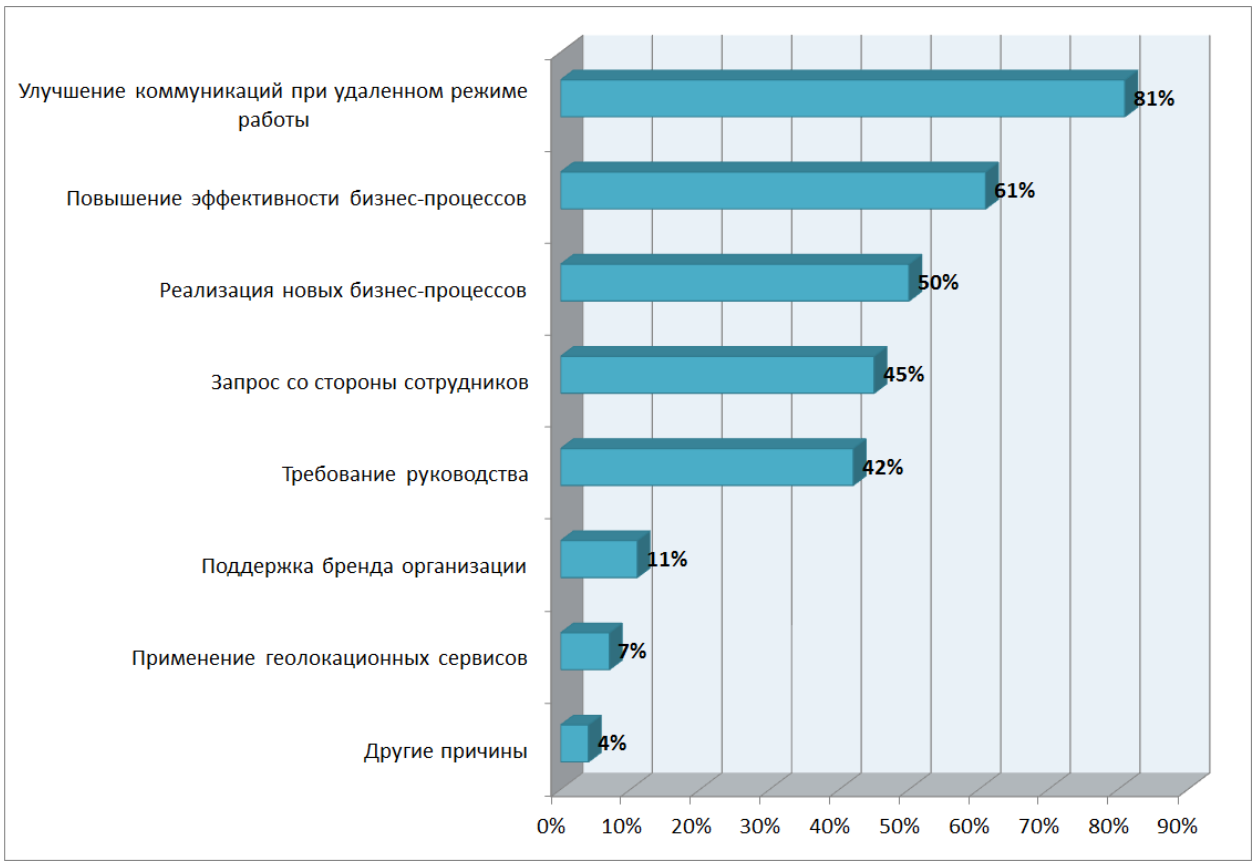

Рисунок 2 Основные причины, по которым организации используют или планирует использовать мобильные технологии

Бизнес-процессы и виды деятельности, в том или ином объеме требующие “мобилизации”, включают как бизнес-коммуникации внутри организации, так и взаимодействие с внешними субъектами -поставщиками и партнерами, а также клиентами и потребителями продуктов и услуг, предоставляемых организацией “вовне”.

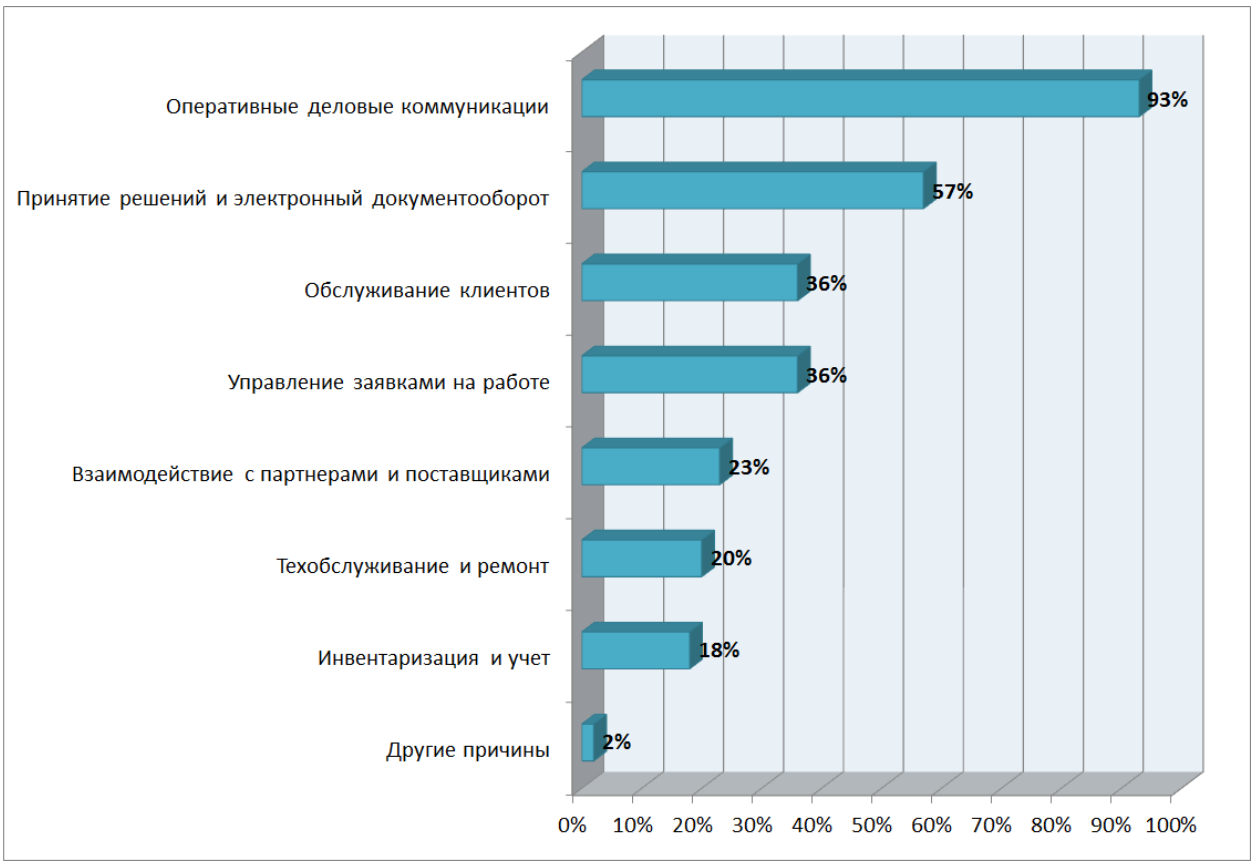

Рисунок 3 Бизнес-процессы в организациях, оптимизируемые за счет использования мобильных технологий

Обеспечение сотрудников мобильными устройствами и средствами доступа к корпоративным информационным ресурсам и системам

Осознавая необходимость обеспечения сотрудников мобильной связью в деловых целях, большая часть организаций выдает корпоративные мобильные устройства различным категориям своих сотрудников. И такая практика, судя по доле организаций, где такой вопрос находится в стадии обсуждения, наверняка будет расширяться.

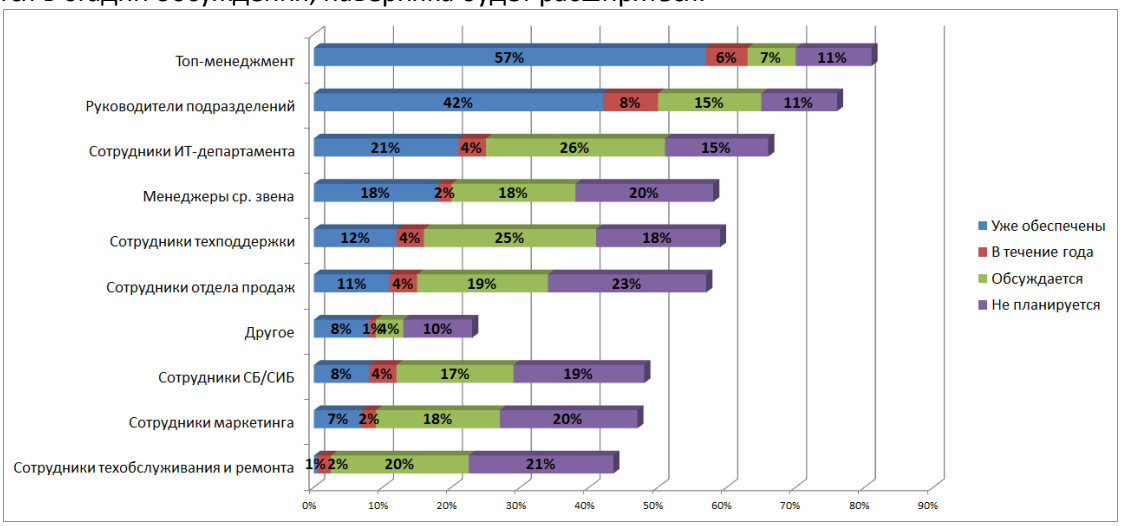

Рисунок 4 Категории пользователей, которым требуется мобильный доступ к информационным ресурсам и системам

При этом внутрикорпоративный охват мобилизацией (количество сотрудников, обеспеченных доступом к корпоративным ресурсам и системам с мобильных устройств) среди опрошенных компаний растет заметно быстрее, чем просто количество организаций, планирующих внедрить элементы корпоративной мобильности. Это косвенно свидетельствует о том, что, попробовав обеспечить сотрудников мобильным рабочим местом, компании утвердились в полезности и выгодности этого начинания и планируют активно расширять

количество сотрудников с мобильным корпоративным доступом. Так, в частности, в разы сокращается количество компаний, где мобильным доступом к корпоративным системам обладают единицы или десятки сотрудников, и в разы увеличивается количество организаций, где сотни и тысячи сотрудников могут работать с корпоративными информационными системами из любого места и с компактных смартфонов/планшетов.

Факторы, ограничивающие эффективное деловое использование мобильных технологий

Наиболее распространенным фактором, сдерживающим эффективное использование мобильных технологий в деловой среде, является отсутствие актуализированных корпоративных стандартов на выдаваемые и поддерживаемые мобильные устройства. До сих пор чувствительная доля корпоративных смартфонов относится к устаревшим поколениям мобильных устройств на базе операционной среды Windows Mobile. При этом менее пятой части респондентов указали стоимость устройств в качестве фактора, тормозящего применение мобильных технологий в их организациях.

Анализ и отбор смартфонов и планшетов в организации должны вестись с учетом потребностей различных категорий пользователей. Стандартизация устройств и, естественно, мобильных операционных систем является одной из важных задач, которые должны быть отражены в концепции и стратегии корпоративной мобильности (это отмечают две трети опрошенных). Такая внутрикорпоративная стандартизация поможет справиться с самой распространенной причиной неиспользования - разнообразием устройств и платформ на рынке. А наличие концепции корпоративной мобильности и содержащихся в ней политик и регламентов пользования поможет согласовать требования служб информационной безопасности, стоящих на страже защиты внутрикорпоративной информации, и желания конечных пользователей и бизнеса шире применять свои мобильные устройства в рабочих целях.

Только 4% респондентов, большинство из которых используют смартфоны на Windows Mobile, указали наличие у них систем управления мобильными устройствами (MDM – Mobile Device Management). Но, в подавляющем большинстве случаев, даже существующие политики и регламенты приняты на организационно-административном уровне и не поддержаны соответствующими техническими средствами.

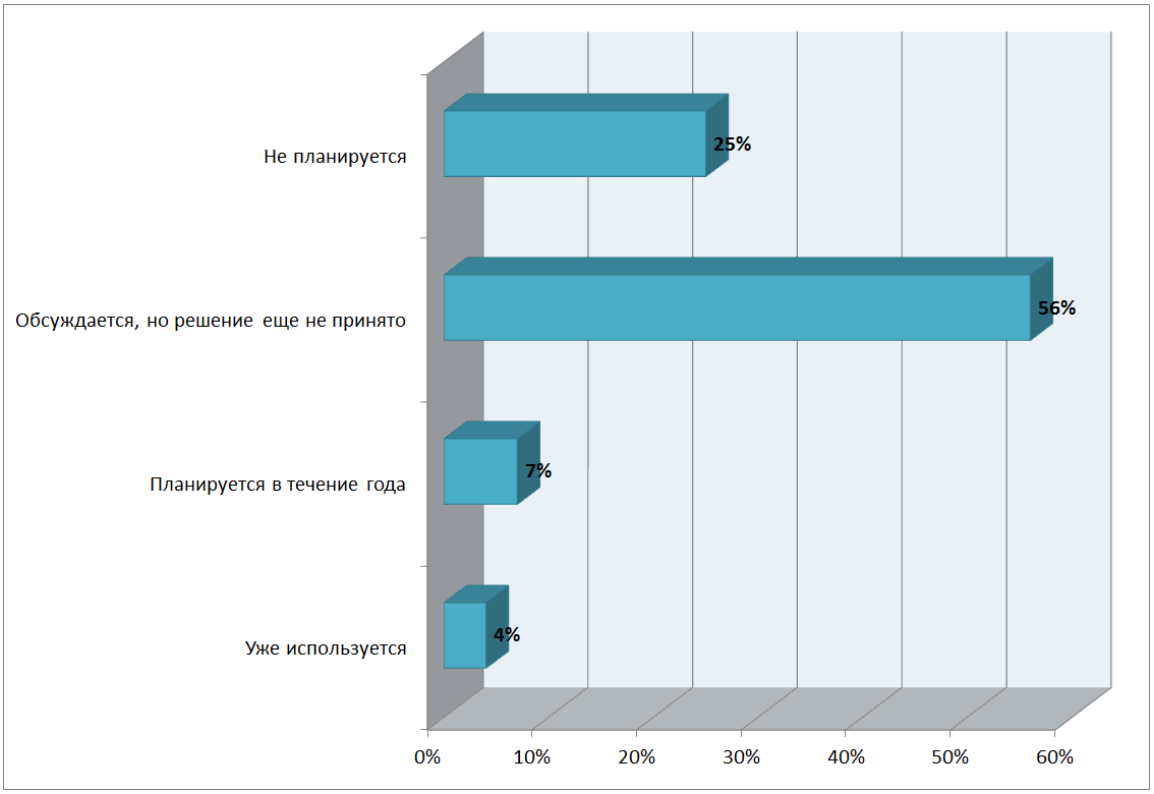

Рисунок 5 Использование средств управления мобильными устройствами в организациях

Лидирующими операционными системами, используемыми в смартфонах и планшетах, являются iOS и Android, представляющие один подход к использованию в обоих типах устройств (смартфоны и планшеты) и одну и ту же операционную систему.

Несмотря на фактическую стандартизацию Windows в качестве платформы традиционных рабочих мест (рабочих станций и ноутбуков) и исторически сильные позиции Windows Mobile на российском рынке, сегодняшняя фрагментация семейства операционных систем Microsoft Windows приводит к смешанному отношению представителей корпоративных ИТ к мобильным устройствам на базе этих операционных систем. Фактически, можно говорить о двух несовместимых поколениях Windows Mobile и Windows Phone для смартфонов предполагающих разную организацию и технологии разработки пользовательского интерфейса “тач”-приложений.

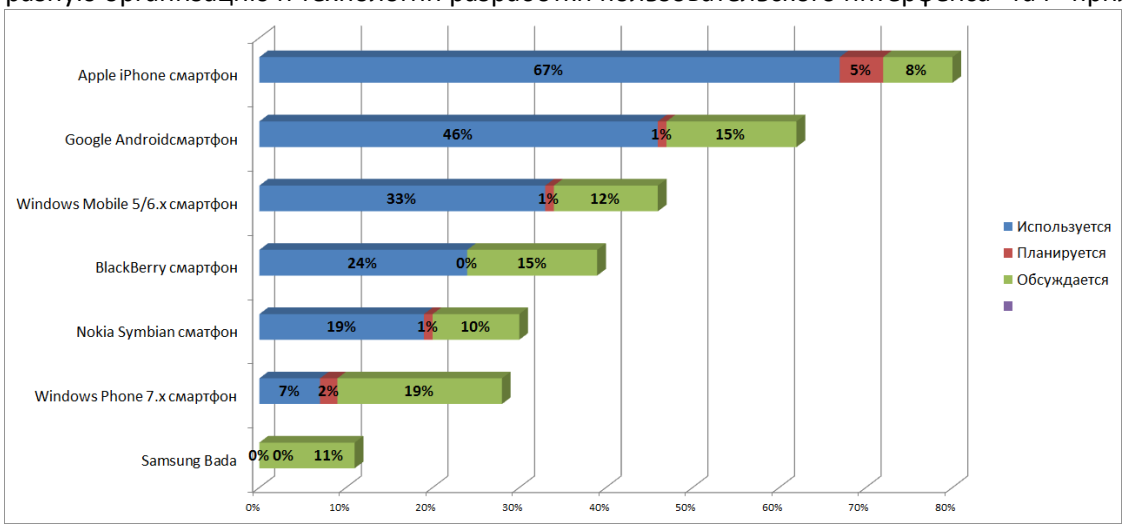

Рисунок 6 Мобильные платформы смартфонов в организациях

В связи с широким распространением смартфонов рассмотрим, какие угрозы появляются при этом.

Сегодняшняя ситуация в мире вредоносного программного обеспечения для смартфонов

Сегодня большая часть вредоносного кода, в том числе разнообразные троянские программы, спам и шпионское программное обеспечение, классические черви, а также методы фишинговых атак разрабатываются специально для «захвата» пользователей мобильных телефонов с целью получения денег незаконным путем. Вредоносный код может быть вложен в почтовое сообщение, встроен в пиратское программное обеспечение (ПО), размещение на веб-страницах, откуда он загружается троянскими программами, заранее установленными на зараженных смартфонах. Важным каналом заражения с появлением OS Android становится Android Market, а также другие площадки, с которых наряду с легальным ПО пользователи могут загрузить и вредоносное.

Все эти факторы приводят к тому, что обеспечение антивирусной защитой становится все более и более сложной задачей.

В то же время, в связи с огромным чистом операционных систем смартфонов и различного антивирусного программного обеспечения для них, что появились на ранке, проблема выбора антивирусного ПО становится все более сложным.

К увеличению количества вредоносных программ для мобильных устройств в частности и к увеличению угроз для безопасности смартфонов в целом ведут следующие тенденции:

1. постоянно растет процент смартфонов среди используемых для мобильной связи устройств. Чем популярнее технология, тем проще и выгоднее ее атаковать;
2. по мере того, как область расширяется, увеличивается и количество квалифицированных специалистов, потенциально способных атаковать ее безопасность;
3. смартфоны становятся все более мощными и функциональными, начиная вытеснять собой карманные компьютеры. Это значит, что у вирусов и вирусописателей появляется все больше возможностей;
4. увеличение функциональности устройства естественным образом ведет к увеличению количества потенциально интересной информации, которая в нем хранится. В отличие от обычного мобильного телефона, содержащего в среднем случае лишь адресную книгу, в памяти смартфона могут храниться любые файлы из тех, которые обычно хранят на диске компьютера. А использование программ для доступа к защищенным паролем онлайн-сервисам (например, ICQ) ставит под угрозу безопасность личных данных.

Исходя из этого возникает необходимость развертывания централизованной антивирусной защиты смартфонов. Рассмотрим создание такой системы защиты на базе Kaspersky WorkSpace Security.

Kaspersky WorkSpace Security

В состав данного продукта входит антивирус для защиты смартфонов Kaspersky Endpoint Security 8 for Smartphone Maintenance Pack 1, который можно загрузить по адресу http://products.kaspersky-labs.com/russian/special/kesmobile/.

Kaspersky Endpoint Security 8 for Smartphone Maintenance Pack 1 включает следующие версии компонентов:

- 8.0.0.37 (Microsoft Windows Mobile);
- 8.1.39 (Symbian OS);
- 8.1.27 (BlackBerry OS);
- 8.1.71 (Android OS);
- 9.0.57.0 (Kaspersky Administration Kit Plugin).

Из впервые реализованных возможностей стоит упомянуть следующие.

- Обеспечена работа программы на устройствах с Android OS; поддерживаются следующие функции для версии программы, которая устанавливается на устройства с Android OS: Антивирус, Анти-Спам, Личные контакты, Анти-Вор.
- Реализована возможность удаленного администрирования устройств с Android OS через Kaspersky Administration Kit.
- Добавлена поддержка устройств Nokia с Symbian 3.
- Добавлена поддержка устройств с BlackBerry OS версии 6.0.

Описание

Комплект Kaspersky Endpoint Security 8 for Smartphone предназначен для обеспечения комплексной защиты мобильных устройств. Возможности программы широки: антивирусная проверка файлов при их открытии, сохранении и запуске (кроме мобильных устройств с BlackBerry OS), а также перехват и проверка всех входящих сообщений MMS и файлов, которые передаются следующими способами: с использованием беспроводных соединений (инфракрасный порт, Bluetooth), при синхронизации с персональным компьютером, при загрузке файлов через веб-браузер или через другие каналы. Реализуется проверка файловой системы устройства по требованию пользователя или по расписанию на наличие вирусов и других вредоносных программ (кроме мобильных устройств с BlackBerry OS), возможность отправлять зараженные файлы в карантин, а также лечить некоторые из них (кроме мобильных устройств с BlackBerry OS). Обновление антивирусных баз программы происходит по требованию пользователя или по расписанию через GPRS-Интернет, Wi-Fi, через Microsoft ActiveSync для устройств с Microsoft Windows Mobile или EDGE (кроме мобильных устройств с BlackBerry OS). Выполняется блокирование нежелательных входящих вызовов и SMS, получение текущего номера телефона при смене SIM-карты, есть возможность дистанционного блокирования устройства в случае его кражи или потери и возможность дистанционного удаления информации пользователя с устройства, плюс к этому возможность дистанционного определения местоположения устройства. Доступна отправка SMS-команд на другие устройства с установленной программой Kaspersky Endpoint Security 8 for Smartphone (или Kaspersky Mobile Security 9) для дистанционного блокирования устройства, удаления данных, определения местоположения устройства, сокрытия конфиденциальной информации пользователя и защиты мобильного устройства от сетевых атак по протоколам TCP/IP (кроме мобильных устройств с BlackBerry OS и Android OS). Файлы хранятся в зашифрованном виде (кроме мобильных устройств с BlackBerry OS и Android OS), а также возможно временно скрыть информацию и события для конфиденциальных номеров, выбранных пользователем (кроме мобильных устройств с BlackBerry OS). Поддерживается работа программы со следующими системами удаленного администрирования: Kaspersky Administration Kit, MS SCMDM, Sybase Afaria. Установка программы на мобильное устройство и ее активация реализуется с помощью систем удаленного администрирования, а также выполняется удаление программы с устройств через Microsoft System Center Mobile Device Manager. Возможна синхронизация устройства с системами удаленного администрирования и настройка параметров работы программы как для нескольких устройств сразу, так и индивидуально для каждого устройства, поддерживается применение политик с помощью систем удаленного администрирования. Отчеты о состоянии защиты мобильных устройств и событиях программы передаются в Kaspersky Administration Kit.

Обращаю ваше внимание на то, что программа устанавливается только в основную память мобильного устройства.

Kaspersky Endpoint Security 8 for Smartphone включает следующие компоненты:

- Антивирус (кроме мобильных устройств с BlackBerry OS);
- Анти-Спам;
- Анти-Вор;
- Сетевой экран (кроме мобильных устройств с BlackBerry OS и Android OS);

- Шифрование (кроме мобильных устройств с BlackBerry OS и Android OS);
- Личные Контакты (кроме мобильных устройств с BlackBerry OS).

Системные требования

Программа предназначена только для тех мобильных устройств, которые поддерживают прием и передачу SMS и работают на следующих операционных системах:

- Symbian OS 9.1, 9.2, 9.3, 9.4 Series 60 UI, Symbian 3 (только мобильные устройства компании Nokia);
- Microsoft Windows Mobile 5.0, 6.0, 6.1, 6.5;
- BlackBerry OS 4.5, 4.6, 4.7, 5.0, 6.0;
- Android OS 1.5, 1.6, 2.0, 2.1, 2.2, 2.3.

Система удаленного администрирования должна удовлетворять следующим минимальным требованиям:

- Kaspersky Administration Kit версии 8.0.2112 и выше;
- Mobile Device Manager Software Distribution Microsoft Corporation Version: 1.0.4050.0000 (SP);
- System Center Mobile Device Manager Microsoft Corporation Version: 1.0.4050.0000;
- Sybase Afaria 6.50.4607.0.

Развертывание Kaspersky Administration Kit не представляет никакого труда, поэтому останавливаться на нем подробно не имеет смысла.

Управление

Управление смартфонами и установленной на них программой Kaspersky Endpoint Security 8.0 for Smartphone (KES) осуществляется аналогично управлению клиентскими компьютерами с установленными на них продуктами «Лаборатории Касперского». Администратор при этом должен сформировать группы, в состав которых он включит мобильные устройства, а после этого создать политику для KES. Особенность KES заключается в том, что все параметры работы программы, включая лицензию, расписание обновления баз и проверки устройств, задаются с помощью политики.

Необходимо учесть, что при установке сервера администрирования для обеспечения управления защитой мобильных устройств через Kaspersky Administration Kit на шаге «Выбор компонентов» обязательно должен быть установлен флажок «Поддержка мобильных устройств». При установке компонента поддержки мобильных устройств создается сертификат сервера администрирования для мобильных устройств. Он используется для аутентификации мобильных устройств при обмене данными с сервером администрирования. Обмен информацией производится с использованием протокола Secure Socket Layer (SSL). Без сертификата для мобильных устройств установить соединение между сервером администрирования и мобильными устройствами невозможно. Средний объем передаваемых при одной синхронизации данных составляет 20–40 Кбайт.

Согласно руководству по внедрению в разделе, посвященном установке модуля управления Kaspersky Endpoint Security 8 for Smartphone, для получения доступа к интерфейсу управления программой при помощи Kaspersky Administration Kit на рабочее место администратора должен быть установлен модуль управления программой Kaspersky Endpoint Security 8 for Smartphone. Чтобы установить модуль управления программой Kaspersky Endpoint Security 8 for Smartphone, скопируйте из дистрибутива программы установочный файл модуля и запустите его на рабочем месте администратора.

Файл модуля входит в состав дистрибутива программы Kaspersky Endpoint Security 8 for Smartphone, но расположен он не в самораспаковывающемся архиве KES8_forAdminKit_ru.exe.

Данный компонент необходимо загрузить с сайта по следующей ссылке: http://www.kaspersky.com/downloads/productupdates/downloads-endpoint-security-smartphone либо http://products.kaspersky-labs.com/russian/special/kesmobile/, скопировать в папку Plugin вашего пакета Administration Kit, а затем установить его на рабочем месте администратора антивирусной системы.

Кроме того, требуется загрузить самораспаковывающийся пакет KES8_forAdminKit_ru.exe по адресу http://www.kaspersky.com/downloads/productupdates/downloads-endpoint-security-smartphone (в документации сказано: «При покупке Kaspersky Endpoint Security 8 for Smartphone в интернет-магазине вы оформляете заказ, по факту оплаты которого вам по электронной почте отправляется письмо, содержащее файл ключа для активации программы и ссылку, по которой можно загрузить дистрибутив программы. За подробной информацией о способах покупки и комплекте вы можете обратиться в отдел продаж по адресу sales@kaspersky.com.»). Но так как в моем случае мне некогда было искать, у кого мы покупали, когда и т. д., я обратился к Интернету.

Следует учесть, что, в отличие от файлов инсталляционного пакета, файлы из дистрибутива являются шаблонами, в которые сервер администрирования при создании инсталляционного пакета прописывает необходимые параметры. Список параметров представлен в документации.

Опытный администратор, прочитав документацию, может внести эти параметры в «шаблоны» вручную и действительно получит инсталляционный пакет. Однако неопытный администратор столкнется с проблемами, которые не сможет решить самостоятельно.

Обновление антивируса

Если ваши смартфоны будут обновляться с серверов «Лаборатории Касперского», то проблем у вас не возникнет никаких. Если же вы хотите, чтобы они обновлялись с внутреннего сервера, придется указать его адрес. Для того чтобы обновления производились с серверов обновлений «Лаборатории Касперского», в поле «Адрес сервера обновлений» введите KLServers. При использовании для обновления баз какого-либо другого сервера обновлений в блоке «Источник обновлений» указывается HTTP-сервер, локальная или сетевая папка. Например, http://domain.com/.

Структура папок в источнике обновлений должна совпадать со структурой на серверах обновлений «Лаборатории Касперского». На самом деле вам необходимо просто скопировать в папку index файлы с http://ftp.kaspersky.com/bases/av/avc/symbian/.

Таким образом, если клиент указывает адрес http://mycompany.com, то KMS будет искать файл http://mycompany.com/index/mobile.xml. Файл mobile.xml должен быть аналогичен вот этому: http://ftp.kaspersky.com/index/mobile.xml.

Если вы используете Windows Mobile, то вам нужен только узел с ComponentID= «KMS90WM». Параметр RelativeSrvPath должен указывать на папку, где лежат базы, относительно адреса, указанного в политике в качестве источника обновлений. Параметр Filename должен указывать на имя файла баз, параметр FileDate должен содержать дату и время.

Как видите, несмотря на то, что задача кажется весьма скромной, на самом деле придется повозиться, однако полученный результат того стоит.