

Интеграция планшетов в корпоративную среду

Обзор особенностей новой версии решения *MobileSputnik 1.5* (развивается компанией “МобилитиЛаб”, входит в ГК “АйТи”), позволяющего обеспечить требования безопасности периметра при использовании мобильных устройств в составе публичных каналов связи, а также приближающего интерфейс взаимодействия с офисными приложениями на планшетах/смартфонах к уровню, реализованному на ноутбуках и ПК.



Сергей Орлик — директор Центра корпоративной мобильности “АйТи”, генеральный директор компании “МобилитиЛаб”.

Введение

Появившиеся всего несколько лет назад мобильные планшетные устройства стали играть все возрастающую роль (за счет компактности, легкости использования, мгновенного включения, расширенных возможностей для коммуникации и т.п.) для корпоративного пользователя (который проводит часть рабочего времени вне своего стационарного рабочего места), позволяя вывести эффективность бизнеса на качественно новый уровень. И если смартфоны, в основном, продолжают использоваться в качестве корпоративных коммуникаторов, то планшеты во все большей степени отводятся роль мобильного рабочего места. Хотя ноутбуки остаются наиболее полнофункциональными переносными устройствами, смартфоны и планшеты играют уже серьезную роль в жизни сотрудников, что требует соответствующего внимания и поддержки со стороны корпоративных ИТ- и ИБ-служб.

По результатам проведенного опроса (анкетирование на 3-й ежегодной конференции — “День Корпоративной Мобильности 2013”), выявлено, что:

- большинство (71%) компаний считают внедрение мобильных технологий инструментом, повышающим продуктивность работы и оперативность коммуникаций сотрудников;
- более двух третей организаций используют мобильные устройства для реализации новых сценариев работы сотрудников и оптимизации существующих бизнес-процессов;
- практически все (95%) опрошенные компании планируют до конца 2014 г. обес-

печатить мобильный доступ к корпоративной почте;

- мобильный доступ к корпоративным файловым ресурсам (общие папки Windows и библиотеки документов SharePoint) стал фактически столь же востребованным (90%), как и доступ к почте;
- внедрение мобильных решений для отображения ключевых показателей имеет значение для 77% организаций и планируется или обсуждается к внедрению в 59% из них.

При этом мобильные платформы на базе iOS и Android контролируют подавляющую часть рынка и не имеют серьезных конкурентов в лице других игроков (рис. 1). Платформы Symbian и BlackBerry практически исчезают из корпоративного сектора (<5%), а устройства на Windows еще не стали заметным игроком в мобильном секторе.

В связи с возрастающей ролью планшетов возник ряд задач:

- обеспечение безопасной работы с офисными документами, осуществляемой с использованием “домашних” мобильных устройств сотрудников при доступе к корпоративному контенту (поддержка концепции BYOD);
- устранение ряда функциональных ограничений, свойственных планшетным приложениям, которые они унаследовали от смартфонов.

Во многом эти ограничения удалось снять при разработке программного сервера *MobileSputnik™*, поставляемого вместе с мобильными клиентами-приложениями для iPad и Android-планшетов, для организации мобильных рабочих мест.



Рис. 1. Использование мобильных платформ (планшетов) в России (основаны на данных опросов последних трех лет).

Основная идея при разработке нашего решения была в том, чтобы перенести на планшет с учетом его специфики (прежде всего, с учетом особенностей touch-интерфейса) привычные для офисного пользователя сценарии при работе с файлами/документами, системами почтовых сообщений и др., одновременно существенно расширяя возможности традиционных смартфонов, используемых в качестве корпоративных коммуникаторов. Многие из существующих сегодня на рынке хорошо зарекомендовавших себя решений изначально создавались для смартфонов, вследствие чего для делового человека являются до некоторой степени примитивными и недостаточно функциональными, в частности, например, позволяя работать только с одним информационным объектом (файл, письмо, документ, презентация и т.п.).

Что нам удалось реализовать (для Android и iOS) и что нас выделяет среди аналогичных решений, представленных на международном и российском рынках? Это:

- обеспечить безопасное (в соответствии с корпоративными требованиями) хранение и обработку информации, “растягивая” периметр безопасности до уровня мобильных устройств, подключаемых по 3G, Wi-Fi, IP-каналам и др. публичному доступу. При этом не требуется вносить каких-либо изменений в сетевую топологию, SharePoint и т.д.;
- встроить в мобильные приложения *MobileSputnik* на планшетах ядро одного из наиболее распространенных мобильных офисных пакетов — *Polaris Office* корейской компании *INFRAWARE*, что позволяет осуществлять просмотр и редактирование офисных документов, не покидая мобильного приложения, т.е. выполнять все операции в рамках защищенного контейнера в соответствии с заданными политиками и в рамках установленных регламентов;
- создать уникальный пользовательский интерфейс с поддержкой многоэкранности для работы с несколькими файлами одновременно “в одно касание”;
- создать древовидную навигацию по всем подключенным корпоративным файловым ресурсам с возможностью предпросмотра выбранных файлов в трехпанельном представлении “а ля Outlook”, чего нет в стандартных почтовых клиентах или потребительских сервисах класса *dropbox*, изначально ориентированных на

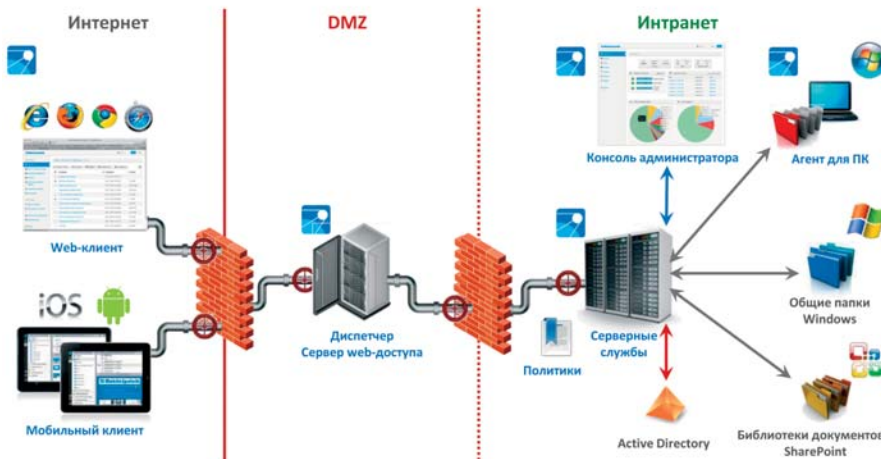


Рис. 2. Общая архитектура решения MobileSputnik.

упрощенные сценарии работы “домашних” пользователей;

- обеспечить поддержку архивов, операций копирования/перемещения на множестве корпоративных ресурсов;
- обеспечить поддержку не только просмотра и редактирования документов, но их создания непосредственно на планшете;
- обеспечить поддержку автоматической синхронизации пользовательских файлов на ПК с сервером MobileSputnik за счет применения интеллектуальных “агентов” без использования каких-либо дополнительных приложений и хранения данных вне контролируемого периметра (например, в облаке);
- обеспечить возможность присоединения и отправки с планшетов сразу нескольких файлов в одном письме;
- обеспечить уникальные возможности прямого кросс-платформенного обмена файлами между планшетами iPad и Android по WI-Fi.

MobileSputnik 1.5: корпоративное мобильное рабочее место

Архитектура

Общая архитектура решения MobileSputnik, развертываемого в ЦОД, DMZ и на мобильных устройствах, представлена на рис. 2. MobileSputnik позволяет органично встраивать мобильные клиентские устройства (с соблюдением всех корпоративных политик безопасности) в имеющийся у заказчика ИТ-ландшафт. Это достигается поддержкой гибких сценариев развертывания серверной части MobileSputnik в корпоративной сети с возможностью разнесения соответствующих компонентов доступа и обработки информации между DMZ и интранет-сегментами, а также ее тесной интеграцией с корпоративной службой каталогов Active Directory (AD).

Архитектура сервера изначально допускает его горизонтальное масштабирование и применение сетевых средств балансировки нагрузки (NLB), а, значит, объем необходимых ИТ-ресурсов практически линейно зависит от числа обслуживаемых мобильных пользователей и интенсивности их работы с планшетами.

*) Если разрешено соответствующими политиками для пользователя на уровне сервера MobileSputnik.

Веб-клиент MobileSputnik реализован с использованием адаптивного веб-дизайна на базе технологий HTML 5, что позволяет использовать его во всех современных веб-браузерах на любых платформах и размерах экранов, включая ПК под управлением Windows, Mac OS X и Linux и смартфоны.

MobileSputnik обеспечивает легкий и безопасный доступ к корпоративным файловым ресурсам Windows и SharePoint и файлам на ПК в любое время и в любом месте:

- мобильные клиенты превращают iPad и Android-планшеты в настоящие мобильные рабочие места, перенося с ПК привычные возможности проводника Windows и Microsoft Office для управления и редактирования офисных документов;
- веб-клиент обеспечивает доступ к файлам с любого устройства – от современных смартфонов до ПК на Windows, Mac OS X и Linux.

MobileSputnik предоставляет:

- управляемый безопасный доступ к iPad и Android планшетов к общим папкам Windows (shared folders) и библиотекам документов SharePoint (document libraries);

- просмотр на мобильных устройствах широкого спектра форматов файлов – Microsoft Word, Excel, Powerpoint, Adobe Acrobat PDF, JPG, GIF, PNG, многостраничные TIFF, аудио MP3 и видео MPG/MP4 и др.;
- возможность одновременного редактирования множества офисных документов непосредственно на планшетах с помощью многоэкранного интерфейса (рис. 3);
- синхронизацию файлов с корпоративными ПК с использованием Windows-агентов*) в стиле dropbox (в случае изменения одного и того же файла несколькими пользователями или одним и тем же пользователем с разных конечных устройств; мобильные клиенты MobileSputnik предоставляют пользователю возможность выбора необходимой версии файла или документа на основе месторасположения и даты/времени модификации документа);
- веб-клиент*) для доступа к подключенным корпоративным файловым ресурсам, функционирующий в браузерах на любом устройстве, – от MacBook Air до Windows Phone (средства самообслуживания позволяют пользователям в дополнение к групповым источникам добавлять собственные избранные корпоративные файловые ресурсы для мобильного и веб-доступа; доступность веб-клиента для пользователей определяется на уровне профиля политик, заданного для соответствующей группы);
- возможность развертывания отказоустойчивой кластерной конфигурации MobileSputnik, совместимой с контроллером доставки приложений Citrix NetScaler.

MobileSputnik имеет встроенный офисный пакет от мирового лидера мобильных офисных пакетов Polaris Office, позволяющий осуществлять редактирование документов форматов Word, Excel, Powerpoint непосредственно в мобильных клиентах MobileSputnik без необходимости загрузки в сторонние приложения.



Рис. 3. Иллюстрация возможностей многоэкранного интерфейса MobileSputnik при работе с множеством файлов “в одно касание”.

В конце февраля 2014 г. в составе мобильных клиентов появилась функция MobileSputnik Direct File Sharing™, которая предоставляет корпоративным пользователям принципиально новые возможности прямого обмена файлами между мобильными устройствами по Wi-Fi — MobileSputnik Direct File Sharing™, не требующие использования Bluetooth. Совместная работа пользователей с файлами документов на предприятии обычно основана на использовании корпоративных файловых ресурсов в интранет, из которых наиболее распространенными являются общие папки Windows и библиотеки документов SharePoint. Однако мобильные пользователи планшетов, находящиеся не просто за пределами стационарного рабочего места, но и на внешних встречах или в командировках, часто работают в автономном режиме. MobileSputnik создан с учетом таких сценариев работы и позволяет работать с документами непосредственно на мобильном устройстве, в том числе создавать и редактировать офисные документы форматов Microsoft Office с помощью встроенной лицензированной технологии одного из ведущих мобильных офисных пакетов Polaris Office.

Новые функции MobileSputnik Direct File Sharing позволяют корпоративным пользователям в любом месте и в любое время использовать сеть Wi-Fi (внешнюю или запущенную на одном из мобильных устройств) для мгновенного и безопасного «перекидывания» и показа файлов друг другу. Функции прямого обмена MobileSputnik обеспечивают безопасный обмен документами для корпоративных пользователей, находящихся в одной сети Wi-Fi.

Доступность функций прямого обмена для пользователей управляется на уровне профилей политик, определяемых на сервере MobileSputnik для соответствующей группы пользователей. Возможность отправки, получения и автоматического открытия полученных документов сразу группой пользователей качественно повышает продуктивность проведения встреч, совещаний и повседневной совместной работы руководителей и сотрудников всех уровней.

Безопасность данных

Как уже было сказано, основной вклад в обеспечение безопасности корпоративных данных, обрабатываемых на планшетах под управлением MobileSputnik, вносит технология контейнеризации. Они расширяются решениями класса mobile application management (MAM), обеспечивающими дополнительную изоляцию мобильных приложений и их данных, а также осуществляющими обмен информацией только между разрешенными приложениями. Лидеры в области MAM: Goog Technology, Citrix и Symantec с соответствующими MAM-платформами — Good Dynamics, Citrix Works и Symantec AppCenter. Мы, в настоящее время, являемся первой российской компанией, которая интегрировала (и, соответственно, лицензировала) разработанные приложения в рамках проекта MobileSputnik с вышеуказанными платформами Good Technology, Citrix и Symantec, став т.о. частью экосистемы этих корпоративных прило-

жений. Кроме как таковой интеграции в соответствующие экосистемы приложений, это означает подтвержденный высокий уровень качества и защищенности самого решения MobileSputnik. Например, для официального включения MobileSputnik в каталог сертифицированных приложений Good Marketplace, мы успешно прошли независимое тестирование в компании Veracode по уровню VL 4, соответствующему требованиям NIST для высококритичных для бизнеса приложений (High Business Critical, 4-й уровень из 5 возможных, где 5-й уровень — безопасность/критичность для жизни).

Отметим некоторые особенности в обеспечении безопасности данных:

- мобильные приложения, агенты и веб-клиент MobileSputnik обеспечивают безопасный доступ ко всем подключенным файловым ресурсам с использованием SSL, а использование HTTP позволяет обойтись без применения VPN на мобильных устройствах. При необходимости ИТ-департаменты имеют возможность выбрать сценарий развертывания веб-клиента и портала самообслуживания, позволяющий ограничить веб-доступ периметром корпоративной сети. Политики сервера MobileSputnik позволяют разрешать использование веб-клиента на уровне отдельных групп пользователей MobileSputnik;
- интеграция с Active Directory качественно упрощает задачу аутентификации мобильных пользователей — для подключения к MobileSputnik и получения доступа к информационным источникам они вводят те же логин и пароль, которые используют на своем рабочем ПК для входа в AD. Фактически, при получении запроса от мобильного устройства на выполнение операции идентификационные данные пользователя сверяются с зарегистрированными в AD, и только в случае их совпадения и отсутствия блокировки устройства или пользователя на сервере MobileSputnik от его же имени проверяется доступ к запрашиваемым ресурсам, т. е. с соблюдением тех же прав, которые ему предоставлены на рабочем ПК, общей папке Windows или корпоративном SharePoint в рамках действующих политик безопасности;
- в случае возникновения ИБ-инцидентов (например, при потере планшета) администратор может заблокировать доступ к корпоративным ресурсам с дискредитированного устройства с помощью специально разработанной для него Web-консоли с поддержкой мобильных браузеров. Помимо управления пользователями, группами пользователей, устройствами и ресурсами (они могут быть привязаны как к отдельным пользователям, так и к группам), администратор имеет возможность контролировать в реальном времени все происходящее в инфраструктуре MobileSputnik через встроенную в Web-консоль панель оперативного мониторинга, а также разбирать имевшие место инциденты и конфликты по сохраненным записям

в журналах системных и пользовательских событий.

С середины января 2014 г. стал доступен комплект решений “MobileSputnik + ViPNet” (от компаний “АйТи” и “ИнфоТекс”, позволяющий обеспечить защищенный доступ к корпоративным данным с мобильных устройств под управлением iOS или Android с применением сертифицированных СКЗИ, реализующих стандарт шифрования ГОСТ.

Комплект поставки “MobileSputnik + ViPNet” включает базовый набор средств для организации защищенной VPN-среды ViPNet и защищенных корпоративных мобильных рабочих мест.

Продукты семейства ViPNet Client для Android или iOS, включенные в комплект “MobileSputnik + ViPNet”, предназначены для защиты мобильных устройств от сетевых атак и организации мобильного доступа к ресурсам корпоративной сети с помощью VPN-туннеля, защищенного технологиями ViPNet. Технологии ViPNet перехватывают любой IP-трафик, идущий от мобильного устройства и к нему, а также обеспечивают его шифрование и невозможность перехвата из сети интернет. При этом процедура шифрования прозрачна для приложений, применяемых пользователем, и не нарушает его привычную работу с данными приложениями. В качестве сети передачи данных могут использоваться как корпоративные сети Wi-Fi, так и публичные хот-споты и сети 3G. Благодаря использованию защищенных корпоративных прокси-серверов, доступных через VPN-туннель, обеспечивается эффективная многоуровневая защита мобильного устройства, антивирусная защита и фильтрация контента, не требующая установки дополнительного антивирусного программного обеспечения на само мобильное устройство. Для управления функциями ViPNet Client for iOS/Android используется простой и удобный графический интерфейс, дизайн которого выполнен в стандартах соответствующих операционных систем.

Продукты ViPNet Client for iOS и ViPNet Client for Android имеют сертификаты ФСБ России на соответствие требованиям к средствам криптографической защиты информации (СКЗИ) класса КС1 и реализуют стандарт шифрования передаваемых данных ГОСТ 28147-89 на ключах длиной 256 бит.

Вместо заключения

MobileSputnik уже реально внедрен и используется в ряде крупных российских банков, финансовых и производственных компаниях. Идущие в настоящее время проекты внедрения и пилотные проекты в России и за рубежом показывают не только интерес корпоративного сектора к данному классу решений, но и высокую оценку предлагаемого MobileSputnik функционала. Можно с уверенностью сказать, что в России создан еще один уникальный тиражный программный продукт, способный удовлетворить самого взыскательного корпоративного пользователя и в России, и в мире.

Сергей Орлик,
ГК “АйТи”