Мобильные технологии в корпоративном сегменте: на волне BYOD

МАКСИМ БЕЛОУС

Зарплатная карта достойного банка из первой пятёрки, корпоративный ноутбук, служебный телефон — привычный для многих сотрудников крупных компаний комплект материальных дополнений к солидному денежному вознаграждению. Однако в последние годы всё явственнее проявляется новая тенденция: личные, приобретённые за собственные деньги мобильные устройства вытесняют с рабочих мест сотрудников те, что достались им в пользование от работодателя бесплатно. Эта тенденция приносить на работу свои устройства (Bring Your Own Device; BYOD) стала реальностью, которую уже невозможно игнорировать или запрещать, приходится с ней както справляться.

ОБЗОРЫ

Свой планшет ближе к телу

Мобильные технологии пришли в бизнес достаточно давно. Собственно, первые сотовые телефоны появились в руках именно у бизнесменов и лишь полтора-два десятилетия спустя стали обыденными предметами обихода пользователей всех социальных слоёв и возрастов. Полноценные же мобильные компьютеры и вовсе до самого недавнего времени считались по-настоящему нужными лишь для работы.

Всё изменило пришествие Web 2.0 и социальных сетей. Миллиардам людей по всему земному шару стало вдруг жизненно необходимо иметь регулярный (а лучше постоянный) и несложно организованный доступ ко Всемирной паутине. Необходимо для того, чтобы с максимальной лёгкостью связываться с родными и близкими, заводить новые знакомства, участвовать в совместных обсуждениях новых фильмов и модных трендов, хвастаться фотографиями и комментировать отпускные снимки коллег — словом, припадать к живительному источнику цифровой социализации.

Вдумчивая интеграция подхода BYOD с действующей корпоративной инфраструктурой требует не только концептуальной смены мировоззрения начальников отделов ИТ и ИБ, но и немалых инвестиций.

Взрывному росту популярности социальных сетей способствовало крайне удачное стечение обстоятельств. Именно под конец первого десятилетия 2000-х, в период самого начала этого роста, на рынке появились первые общедоступные и относительно недорогие мобильные терминалы для выхода в Интернет: сперва нетбуки, затем смартфоны и, наконец, планшеты. К концу нынешнего года, по оценке Cisco, число одних только мобильных телефонов в мире превысит общее количество жителей планеты, включая новорожденных. В 2012-м был зафиксирован 70%-ный рост мобильного трафика. Причём на каждый из 36 млн. планшетов, находившихся тогда на руках у пользователей по всему свету, приходилось в среднем втрое больше переданных и принятых данных, чем на типичный смартфон, а на каждый из 161 млн. ноутбуков — всемеро больше.

Наши современники активно и самостоятельно входят в мир высоких технологий, формируя собственные предпочтения либо следуя модным трендам. Веками отлаженная схема "пришёл на работу — используй предоставленные работодателем инструменты" начала давать сбой на наших глазах именно в той сфере, где заняты "белые воротнички". ИТ-службы по всему миру явно не были готовы к тому, что рядовые сотрудники и менеджеры всех уровней начнут не просто приносить в офис свои мобильные терминалы, но ещё и активно использовать их для рабочих целей.

В США, согласно недавнему исследованию Microsoft, 67% опрошенных предпочитают работать с применением личных ноутбуков, смартфонов и планшетов, не слишком заботясь о тонкостях регулирования BYOD-политики со стороны руководства. Более того, строгий запрет на использование собственных устройств и попытка насильно заставить сотрудников использовать корпоративные мобильные терминалы входит теперь в число важнейших причин, побуждающих "белых воротничков" менять работодателя.

В то же время лишь 23% сотрудников получают на работе хотя бы минимальный инструктаж от ИТ-отделов и служб безопасности относительно возможных рисков интеграции персональных устройств в корпоративную инфраструктуру. Судя по тому, насколько бурно растёт приятие идеологии BYOD работодателями (в особенности из сегмента СМБ, которые уже подсчитывают немалые прибыли от экономии на централизованно приобретаемом "железе"), именно компаниям придётся следовать в данном случае за глобальным трендом и постепенно инкорпорировать эту идеологию в стратегию своего развития. Возникающие же проблемы в областях безопасности, надёжности хранения данных, оперативного ремонта выходящей из строя персональной техники и порядка оплаты мобильного трафика (в том числе в роуминге) работодателям приходится решать по мере поступления, что называется, с колёс.

Оценки аналитических агентств текущего состояния мирового рынка BYOD-решений и сопутствующих услуг заметно разнятся в силу различий применяемых методик. Однако можно с уверенностью утверждать, что объём его измеряется десятками миллиардов долларов, а среднегодовые темпы роста составляют 15—20%. Данные локальных опросов в России свидетельствуют, что уже более половины предприятий (по некоторым оценкам, даже до 75%) так или иначе допускают применение сотрудниками своих мобильных устройств в работе, т. е. тенденция BYOD уже получила широкое распространение и в отечественных компаниях.

Более того, по данным исследований IDC, в то время как российский ИТ-рынок в целом находится на спаде, его BYOD-сегмент — один из немногих, находящихся на подъеме. Вместе с тем использование собственных мобильных устройств несет новые угрозы информационной безопасности компаний, с которыми они раньше в рамках корпоративной инфраструктуры не сталкивались. И всё же число организаций, в которых практика использования личных мобильных устройств поставлена под контроль ИТ- и ИБ-департаментов в соответствии с принятой стратегией и политикой безопасности, крайне невелико, в лучшем случае это единицы процентов.

Презумпция бесконтрольности

Самым серьёзным риском движения в сторону BYOD для любой компании, безусловно, нужно признать повышение вероятности утечек деловой информации, что, в свою очередь, ведёт к различным потерям — финансовым, техническим, репутационным. Следует ли исходя из этого просто запретить использование персональных мобильных устройств для рабочих нужд? Сергей Орлик, директор Центра корпоративной мобильности компании "АйТи", убеждён в бессмысленности такого запрета: никто ведь не отказывается от автомобиля как удобного и быстрого средства передвижения, невзирая на всю его объективную опасность и для водителя, и для пешеходов. В рамках корпоративной мобильности необходимо вводить не менее строгие, чем ПДД, "правила игры", по меньшей мере два из которых должны быть безусловно обязательными: это управление мобильными устройствами (MDM Mobile Device Management), обеспечивающее их конфигурирование в соответствии с заданными политиками, а также разделение личных и деловых данных на мобильных устройствах с использованием соответствующих корпоративных приложений, предназначенных для работы с электронной почтой, файлами и интегрированных с корпоративной службой каталогов.

Бесконтрольное использование мобильных устройств, отметил Юрий Черкас, руководитель направления инфраструктурных ИБ-решений Центра информационной безопасности компании "Инфосистемы Джет", свидетельствует в первую очередь о том, что служба ИБ работает плохо. И основные риски компании связаны именно с этим или с недостаточностью применяемых мер защиты, а отнюдь не с применением личных мобильных устройств.

Оценка рисков в связи с бесконтрольным использованием мобильных устройств — отдельная проблема, которую нужно решать исходя из потенциального урона компании. По наблюдениям технического консультанта Symantec Михаила Савушкина, в компаниях, где понимают данные проблемы и высоко оценивают свои риски, необходимые средства защиты внедряются или уже внедрены. В таких компаниях даже утеря устройства не приведет к получению несанкционированного доступа к информации на телефоне.

Согласно данным исследования компании ЭОС, на которые сослался ее главный специалист по маркетингу мобильных приложений Артём Андреев, около 44% респондентов оценивают риск от потери информации как несущественный, в то же время другие 44% говорят, что это может сказаться на их работе. Основные риски здесь обусловлены сбором злоумышленником информации о мобильном пользователе и о компании, перехватом и искажением информационных потоков от мобильного пользователя в организацию и в обратном направлении, блокированием информации, которую отправляет пользователь/организация, подменой клиента или сервера.

Особенно высоки риски в случае предоставления мобильного доступа к рабочей информации руководителям компании. Чем выше статус и должность человека, тем выше ценность конфиденциальной информации, которой он пользуется в работе, справедливо напоминает Алексей Александров, руководитель направления по работе с технологическими партнёрами в компании "Аладдин Р.Д.". Вместе с тем, как указывает Антон Багров, заместитель директора департамента разработки ПО компании "АстроСофт", мобильный доступ напрямую влияет на качество управления компанией и в конечном счете на эффективность и результативность ее работы. Поэтому важно четко определять перечень возможных угроз и исходя из этого выстраивать политику использования персональных мобильных устройств с разделением уровней доступа.

При выверенном балансе между рисками и преимуществами подход BYOD ▸

Наши эксперты

АЛЕКСЕЙ АЛЕКСАНДРОВ, *руководитель направления по работе с технологическими партнёрами, "Аладдин Р.Д."*

АРТЁМ АНДРЕЕВ, *главный специалист по маркетингу мобильных приложений, ЭОС*

АНТОН БАГРОВ, *заместитель директора департамента разработки ПО, "АстроСофт"*

СЕРГЕЙ ЛАРИН, *специалист по инфраструктурным решениям, Microsoft в России*

РИШАТ МУХАМЕТШИН, *ИТ-аналитик, DIRECTUM*

СЕРГЕЙ ОРЛИК, *директор Центра корпоративной мобильности, "АйТи"*

МИХАИЛ САВУШКИН, *технический консультант, Symantec*

ИЛЬЯ ФЕДОРУШКИН, *руководитель департамента корпоративных продаж мобильных решений, "Самсунг Электроникс" в России*

ЮРИЙ ЧЕРКАС, *руководитель направления инфраструктурных ИБ-решений Центра информационной безопасности, "Инфосистемы Джет"*

может стать новым фактором развития внутрикорпоративных ИТ-коммуникаций. Ришат Мухаметшин, ИТ-аналитик компании DIRECTUM, позитивно воспринимает необходимость контролировать потоки корпоративной информации через личные устройства сотрудников. Скорость внутрикорпоративного взаимодействия вследствие их применения только повышается по сравнению с той, какую обеспечивают традиционные рабочие места с доступом к ИТ-ресурсам (например, к информационной системе, почте и т. п.). Но добиться необходимого баланса в отсутствие специализированных программно-аппаратных средств контроля BYOD невозможно.

Сергей Ларин, специалист по инфраструктурным решениям Microsoft в России, акцентирует внимание на том, что обеспечение доступа личных устройств (включая мобильные) в корпоративную среду в обязательном порядке должно проводиться в рамках согласованной и действующей для всей компании политики безопасности. Ее отсутствие может приводить к печальным последствиям с точки зрения и безопасности, и бизнеса, и репутации. С этим мнением солидарен и Илья Федорушкин, руководитель департамента корпоративных продаж мобильных решений "Самсунг Электроникс" в России: мобильное устройство становится частью ИТ-инфраструктуры предприятия и к нему должны применяться ИТ-политики и политики информационной безопасности, действующие на предприятии, причем модернизированные с учетом фактора мобильности, т. е. использования в любое время и в любом месте.

В целом же, как отмечают наши эксперты, необходим комплексный подход к решению вопросов обеспечения защиты конфиденциальной информации на мобильных устройствах, который совмещал бы и технические, и организационные меры.

Куда всё это BYOD?

Вдумчивая интеграция подхода BYOD с действующей корпоративной инфраструктурой требует не только концептуальной смены мировоззрения начальников отделов ИТ и ИБ, но и немалых инвестиций, пусть даже частично покрываемых экономией на централизованных закупках ноутбуков, планшетов и смартфонов для сотрудников. Начинать столь масштабное преобразование всё-таки лучше постепенно и с малого. Прежде всего, указывает Михаил Савушкин, — предоставить сотрудникам защищенный доступ к электронной почте, а затем уже к документам и корпоративным системам. Хотя сегодня сегмент BYOD на российском рынке ощутимо растёт и рост этот в обозримой перспективе продолжится, у компаний нет понимания того, какие риски ведет за собой бесконтрольное использование мобильных устройств при получении доступа к корпоративным ресурсам.

По данным третьего ежегодного опроса "Корпоративная мобильность в России-2013", проведённого компанией "АйТи", в половине организаций мобильные устройства приобретаются сотрудниками только за свой счет (BYOD) и при этом более трети организаций выдают корпоративные смартфоны и планшеты определенным категориям сотрудников. Доля BYOD в процентном отношении, вероятно, будет расти, полагает Сергей Орлик, с одновременным абсолютным ростом числа корпоративных мобильных устройств.

Илья Федорушкин отметил, что достаточным уровнем безопасности сегодня обладают решения с использованием портальных средств и корпоративных облаков, позволяющих чаще всего работать с корпоративной информацией через браузер и подключение к этим ресурсам посредством VPN. Основной же помехой развитию BYOD в России ему видится дилемма "корпоративная безопасность — личная свобода". Когда компания разрешает подключаться к корпоративной сети только в том случае, если выполняются определенные требования к безопасности, а сотрудник, за свои средства купивший устройство, хочет использовать его без каких-либо ограничений и контроля со стороны организации.

Помимо технологической готовности компании к внедрению BYOD, Сергей Ларин делает акцент на психологической готовности организации к грядущим и неизбежным переменам. В этом отношении особое значение приобретает, по его мнению, поиск иных подходов, нежели применение решений класса MDM, которые получили не слишком широкое распространение в силу своей дороговизны и сложности во внедрении и использовании.

Не стоит забывать и о классических мобильных компьютерах, на это указал Юрий Черкас. По его словам, использование собственных ноутбуков (преимущественно Mac) для работы в офисе находится на втором месте по распространенности после применения личных мобильных устройств. Причём персональные ноутбуки сотрудников не требуют внедрения MDM-системы. Данные опроса, проведённого компанией "ЭОС", свидетельствуют, что уже сейчас порядка 35% организаций готовы предоставить своим сотрудникам ограниченный доступ с личных устройств, вместе с тем около 26% организаций готовы предоставить полный доступ ко всем ресурсам компании, об этом сказал Артём Андреев.

Помимо электронной почты в качестве ещё одного направления актуального проникновения BYOD-подхода на российских предприятиях Ришат Мухаметшин назвал дистанционный доступ к адресной книге. В любом случае рисков в ходе такого внедрения очень много. Поэтому в основном личные устройства могут быть использованы в бизнес-процессах, которые лишь поддерживают основную деятельность предприятия. Это относится к процессам делопроизводства, к обеспечению эффективного взаимодействия на разных уровнях. На незрелом пока ещё рынке поставщики решений для управления корпоративными мобильными устройствами должны предлагать более доступные и понятные решения, разработчики мобильных приложений должны учитывать интересы потребителей их услуг. И наконец, самое важное — покупатели должны понимать и быть готовы к внедрению таких систем. Если ранее BYOD воспринимался только как риск, сейчас уже есть понимание возможностей, которые появляются вслед за интеграцией личных устройств в деловые процессы.

Внедрение без опасности

"Что позволено Юпитеру, не позволено быку" — не то правило, которым должна руководствоваться служба информационной безопасности уважающей себя компании. Подозревать топ-менеджеров в инсайдерстве и промышленном шпионаже, конечно, вряд ли стоит, но планшеты и смартфоны в равной степени склонны терять и CEO, и рядовые клерки. Михаил Савушкин убеждён, что комплексный подход к безопасности (создание нормативной документации, определение ресурсов для доступа и т. д.) должен применяться для всех без исключения сотрудников компании.

Юрий Черкас советует начинать с четкого формирования конкретного сценария BYOD. В первую очередь следует определить: кто, откуда, к каким ресурсам и с каких устройств имеет доступ. Важно учитывать и варианты развития ситуации на перспективу. Зачастую бывает так, что все начинается с организации удаленного доступа к почте, а затем требуется обеспечить доступ уже к массе корпоративных приложений, включая SAP и т. д. После того как сценарий определен, остается адекватно подобрать меры защиты и внедрить соответствующие средства.

Ключевые элементы системы безопасности, по мнению Артёма Андреева, — это криптографическая контейнеризация всего устройства либо отдельных областей его внутренней памяти, использование систем MDM с возможностью удаленного управления устройством, надёжная система взаимной аутентификации всех участников информационного обмена, бесшовная интеграция

Объём рынка BYOD-решений измеряется десятками миллиардов долларов, а среднегодовые темпы роста составляют 15—20%. Данные локальных опросов в России свидетельствуют, что уже более половины предприятий (по некоторым оценкам, даже до 75%) так или иначе допускают применение сотрудниками своих мобильных устройств в работе.

с сервисами и системами безопасности. Антон Багров рекомендует обращать внимание на уже имеющийся на рынке опыт ведущих производителей устройств и предложения по программному обеспечению. Практически все производители уже выпускают те или иные комплексы ПО для реализации взаимодействия личных устройств и корпоративных сервисов. Кроме того, подавляющее большинство западных компаний этот этап уже прошли, всегда можно воспользоваться их практическим опытом.

Огромное значение имеет и организационный аспект, на это указал Сергей Ларин. Необходимо обучать сотрудников, разъяснять корпоративную политику. Иногда даже стоит подписывать дополнительные соглашения к трудовым договорам, в которых должно быть указано, какая информация является коммерческой тайной и не должна быть раскрыта. Осведомленность пользователей зависит от работы ИТ-службы компании, сотрудников, отвечающих за безопасность, и даже от работы HR-отдела. Сотруднику также надо четко объяснить, что делать, например, в случае утери или кражи устройства. В свою очередь, ИТ-службы должны быть готовы к такому развитию событий, чтобы своевременно и эффективно ему противодействовать.

Актуальность текущего момента

Сегодняшние вендоры, лидеры систем управления мобильными устройствами, предоставляют во многом схожие по функциональности продукты. Сергей Орлик считает, что это в определенной степени отражает зрелость соответствующих технологий. В то же время эти вендоры производят не только системы MDM, но и другие технологии и продукты и дифференцируются за счет интеграции с другими своими и внешними решениями. Отличия различных MDM могут состоять в тех или иных возможностях интеграции с корпоративной инфраструктурой управления сертификатами, сетевой инфраструктурой для контроля доступа в беспроводные сети и т. п. В каждом конкретном случае необходимо отталкиваться от корпоративных требований к обеспечению мобильного доступа и существующего в организации ландшафта. Универсальных рецептов нет, подводных камней хватает всегда, но в отношении зрелых продуктов лучшие практики уже накоплены в тех центрах компетенции, которые занимаются не просто поставкой лицензий, а имеют опыт реальных проектов.

К сожалению, в настоящее время ощущается нехватка разработчиков под iOS и Android, а корпоративных — в особенности. Мобильная разработка требует интеграции в корпоративный ландшафт. Если вход на ПК предполагает использование Active Directory, то для мобильного устройства это задача нетривиальная, необходимо решать ее на уровне приложения, вводить серверную составляющую и обеспечивать доставку и обработку специализированных политик на уровне приложения. Для разработчиков, которые имеют опыт создания потребительских приложений и пытаются заниматься корпоративными решениями, это проблема, у них просто нет понимания и навыков использования соответствующих корпоративных технологий.

В мобильной составляющей все более важным становится использование соответствующих платформ контейнеризации и интеграции мобильных приложений. И в серверной, и в мобильной части таких решений необходимо предусматривать возможность автономной работы наравне с онлайн-режимом. Таких требований множество, ряд из них специфичен именно для мобильной работы. Процент корпоративных тиражных систем для мобильной работы существенно выше, чем для традиционных ПК, что связано в большой степени с унификацией сценариев мобильной работы, дополняющей и расширяющей деятельность на рабочем месте. Алексей Александров подчёркнул, что доступ к хранимой на устройстве информации, а также подключение к корпоративным системам должны осуществляться после прохождения процедуры аутентификации.

В "АстроСофт" в качестве основной проблемы при разработке мобильных систем отмечают большое разнообразие самих мобильных устройств. Один из вариантов решения проблемы многообразия устройств — использование веб-интерфейса с гибкой подстройкой под размеры экрана устройства. Однако в этом случае не всегда удается воспользоваться всеми возможностями, предоставляемыми платформой.

Традиционными, с точки зрения Ришата Мухаметшина, можно считать проблемы "зоопарка" ОС, отсутствие дисциплины пользования мобильными устройствами. Отдельно можно назвать завышенные ожидания заказчика и в большинстве случаев необходимость объяснить новые расходы на поддержку функционирования и развития нового решения после внедрения. Часто практика использования корпоративных приложений отличается от однопользовательских, особенно если речь идет об изолированной системе, а не о, скажем, общедоступном облачном сервисе.

На данный момент существует тенденция переноса корпоративных данных в отдельный виртуальный контейнер на устройстве (управление мобильными приложениями) или же сразу виртуальную ОС, об этом сказали и Михаил Савушкин, и Илья Федорушкин, и другие эксперты. Таким образом компания как бы арендует на личном устройстве сотрудника некую область памяти и не затрагивает его личные настройки и данные. Однако и здесь большинство экспертов также единодушны — пока в России практику BYOD чрезвычайно сложно увязать с соблюдением нормативных требований по обеспечению информационной безопасности. В первую очередь из-за проблем, связанных с применением сертифицированной на территории РФ криптографии.