

Живи — работай:

концепция BYOD



Алексей ШАЛАГИНОВ,
директор по решениям
Huawei Enterprise Business Group

Мир телекоммуникаций стремительно «мобилизуется». 2011 год стал переломным на рынке персональных устройств — поставки смартфонов и планшетов впервые превысили поставки ПК и ноутбуков.

По данным IDC, поставки планшетов за 2012 год возросли на 66%, а смартфонов — на 32%. В текущем году число сотрудников, работающих вне офиса, составило 1,2 млрд человек, достигнув почти 35% от общего числа офисных сотрудников в мире (рис. 1).

По словам Боба О’Доннелла (Bob O’Donnell), вице-президента IDC, «потребители и коммерческие покупатели начинают рассматривать смартфоны, планшеты и ПК как единый континуум интернет-устройств, отличающихся лишь размером экрана».

BYOD = Развлечение + Работа

Все более популярной становится концепция BYOD (Bring Your Own Device — букв. «принеси свое устройство») — новый режим работы сотрудников, позволяющий использовать их собственные мобильные устройства как для личных целей, так и для работы.

Менеджеры различного уровня в своей повседневной работе не всегда имеют возможность вовремя читать почту, особенно при разъездном характере работы, не всегда успевают утверждать контрольные точки бизнес-процессов, и в результате они затягиваются.

Таблица. 1
Рейтинг технологий в среде ИТ-директоров в 2008–2012 годах

Рейтинг	2012	2011	2010	2009	2008
Аналитика и Business Intelligence	1	5	5	1	1
Технологии мобильности	2	3	6	12	12
Cloud Computing (SaaS, IaaS, PaaS)	3	1	2	16	*
Технологии коллективной работы (Collaboration)	4	8	11	5	3
Виртуализация рабочих мест	5	2	1	3	3
Модернизация имеющихся систем	6	7	15	*	*
IT менеджмент	7	4	10	*	*
Управление отношениями с заказчиками (CRM)	8	18	*	*	*
Планирование ресурсов предприятия (ERP)	9	13	14	2	2
Безопасность	10	12	9	8	5
Социальные сети/Web 2.0	11	10	3	15	15

Источник: Gartner, Rankings of technologies CIOs selected as one of their top five priorities in 2012

ваются. Их графики могут меняться, и они должны использовать подручные устройства для подключения к удаленной конференции. Поэтому решения по мобильному доступу к услугам корпоративной сети предприятия как никогда актуальны для работников любого уровня.

Компания Gartner отмечает, что приоритет технологий мобильности необычайно вырос в среде ИТ-директоров предприятий, заняв второе по важности место, уступив только аналитике и Business Intelligence (табл. 1).

Gartner прогнозирует, что в 2015 году продажи планшетов превысят 326 млн шт., смартфонов — 1 млрд (50% продаж мобильных телефонов), а основной абонентской базой этих устройств будут корпоративные пользователи, использующие мобильные терминалы для офисных целей.

Стиль поведения пользователей в сети также стремительно меняется. Диаграмма (рис. 2) показывает, как выглядят основные пять целей использования мобильных устройств.

Аналитики Gartner полагают, что услуги местоположения LBS (Location Based Service) стимулируют рост контекстных услуг. Например, проходя мимо супермаркета, вы можете получить на смартфон извещение о скидках — почему бы не зайти и не купить то, что вы давно искали, но откладывали покупку из-за высокой цены? Мобильный поиск становится вторым по величине приложением, более 50% местного поиска делается при помощи мобильных устройств. Услуга «унифицированных коммуникаций» (UC) позволяет превращать обычный

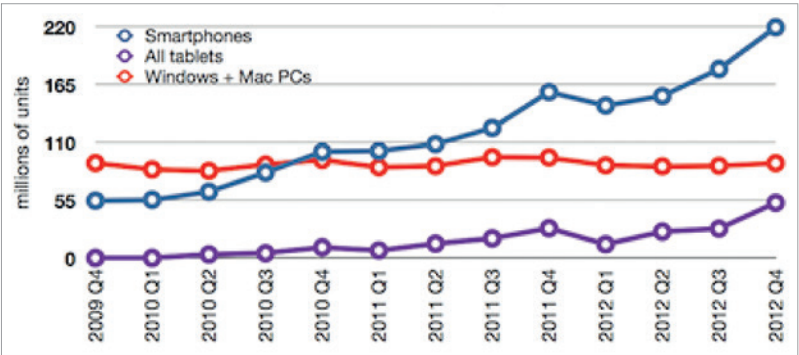


Рис. 1. Изменение поставок смартфонов, планшетов и ПК в 2009–2012 годах

речевой вызов в видеоконференцию с использованием «белой доски», совместным просмотром документов и обменом мгновенными сообщениями IM (Instant Messaging). Мобильный банкинг и оплата проезда в транспорте уже скоро станут привычными услугами. Услуга «быстрого отклика» QR (Quick Response) широко используется на мобильных телефонах. При работе над проектами сотрудники используют мобильные устройства для фото- и видеосъемки с размещением на сайтах фото- и видеохостинга, чтобы быстро послать отчеты о проделанной работе.

По данным Citrix Systems, 92% ИТ-организаций знают, что сотрудники используют свои собственные устройства на рабочем месте, и 94% из них планируют к середине 2013 года иметь свою политику по BYOD (сейчас 44%).

Выгоды BYOD

Исследования практической реализации BYOD показывают, что в среднем каждый сотрудник может сэкономить на передвижениях два часа в день, используя терминал BYOD, то есть 520 часов в год. В среднем эффективность использования рабочего времени возрастает на 15%. Для крупного предприятия, где работает несколько тысяч сотрудников, экономия может составить 15--20% накладных расходов. С меньшей физической нагрузкой и эмоциональным напряжением растет как качество работы, так и качество жизни каждого сотрудника.

Исследования показали, что использование BYOD на предприятии помогает привлечению и удержанию талантливых сотрудников, увеличению производительности и мобильности работников, повышению их удовлетворенности, и в то же время помогает сократить ИТ-затраты.

Архитектура решения BYOD

Несмотря на очевидную привлекательность концепции BYOD с точки зрения бизнеса, она вызывает немалые опасения у «начальников транспортного цеха», а именно ИТ-директоров предприятий, в первую очередь по соображениям безопасности информации, в частности из-за возможности доступа к конфиденциальной



► Рис. 2. Использование мобильных устройств

информации предприятия с личных устройств и ее утечки за пределы организации.

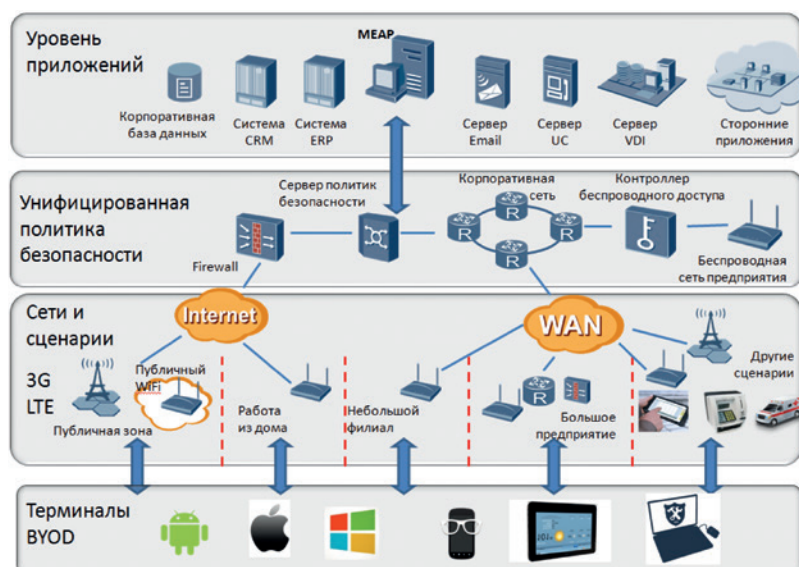
Однако сама по себе концепция BYOD здесь ни при чем. У сотрудников десятилетиями был и есть доступ к конфиденциальной информации, а наличие компакт-дисков, USB, пересылки по электронной почте, камер на мобильных телефонах, копировальных аппаратов, и даже ручек и бумаги всегда делали возможной утечку информации. Компании, дорожащие конфиденциальной информацией, всегда с этим боролись, закрывая доступ к записи на внешние носители с рабочих компьютеров. А как это сделать, если сотрудники используют свои собственные устройства?

Политика безопасности BYOD должна быть понятной, требования к сотрудникам должны быть ясно опи-

саны, и обязанности организации в отношении личных устройств сотрудника четко определены. Тогда вопросы, связанные с безопасностью, будут мало отличаться от обычных, связанных с корпоративными компьютерными устройствами.

Можно определить четырехуровневую архитектуру решения BYOD с учетом требований к безопасности (рис. 3).

Все системы приложений предприятия, необходимые для повседневной работы, находятся на уровне приложений, и доступ к ним осуществляется через сервер политики безопасности, находящийся в корпоративной сети предприятия. Сюда могут входить широко используемые системы отношений с заказчиком (CRM), планирования ресурсов предприятия (ERP), сервер корпоративной почты, сервер унифи-



► Рис. 3. Архитектура решения BYOD, учитывающая требования безопасности

цированных коммуникаций UC, сервер виртуализации рабочих мест VDI (Virtual Desktop Infrastructure), а также корпоративная база данных сотрудников (каталог предприятия). Очень важна платформа мобильных приложений предприятия MEAP (Mobile Enterprise Application Platform), осуществляющая взаимодействие со всеми приложениями предприятия с учетом политики безопасности.

Предназначение MEAP — кроссплатформенная интеграция многих мобильных приложений и типов смартфонов в единой системе. Основные функции MEAP следующие:

- MEAP способна поддерживать несколько типов мобильных устройств и операционных систем без необходимости оперирования с различными наборами программных кодов;
- MEAP поддерживает коннективность, безопасность и администрирование приложений;
- MEAP облегчает разработку и внедрение собственных мобильных приложений на предприятии при помощи технологии 4GL, которая не требует написания исходных кодов, эти приложения могут быть использованы на любых типах мобильных устройств и ОС;
- интеграция с различными типами исходных данных серверов с поддержкой SOAP;

- MDM (Mobile Device Management) — централизованное администрирование мобильных приложений на различных типах устройств;
- MEAP повышает эффективность использования различных бизнес-платформ (CRM, ERP и пр.), поскольку доступ к ним становится возможным с любых мобильных устройств, из любого места, где есть доступ к Интернету;
- MEAP может работать в облаке, то есть предприятию не обязательно разворачивать свою платформу MEAP, напротив, ее можно арендовать у поставщика облачных приложений.

Централизованная политика безопасности обычно осуществляется из корпоративной сети в центральном офисе предприятия. Пользователи могут подключаться к ней при помощи различных сетей и по различным сценариям. Становится возможной работа в публичной сети 3G или Wi-Fi. Например, менеджер, проводя трудные переговоры с заказчиком в его офисе, зашел в ближайшее кафе, чтобы за чашкой кофе тут же написать боссу отчет о проведенных переговорах. Поскольку переговоры были конфиденциальными и передаваемая информация является критичной для бизнеса, идентификация устройства менеджера может быть осуществлена при помощи распознавания IMEI и

введения логина и пароля пользователя в корпоративной сети. После этого передача данных будет осуществляться через защищенный канал VPN.

Становится возможной работа из дома, чтобы не тратить время на дорогу в офис, в случае если на сегодня не запланированы встречи или презентации, а намечается лишь работа с документами.

Небольшие филиалы и крупные предприятия могут подключаться к центральному офису при помощи собственной или арендованной сети передачи данных WAN.

Возможны также и другие сценарии с использованием специализированных отраслевых терминалов. Например, это может быть мобильный кардиограф или аппарат УЗИ в карете скорой помощи, который сразу передает результаты исследования пациента в базу данных медицинского учреждения, где их быстро рассмотрит лечащий врач или соберется консилиум узких специалистов.

Консьюмеризация ИТ-систем предприятий становится реальностью сегодняшнего дня, поэтому специалисты ИТ-служб больше не могут просто прятать голову в песок. Вопрос в том, как плодотворно использовать те возможности, которые BYOD может дать бизнесу предприятия, при сохранении полного контроля над бизнес-процессами и безопасностью корпоративных данных. Для ИТ-служб предприятия это может стать непростой, но интересной и творческой задачей, над решением которой должны работать не только они, но и все сотрудники предприятия. Как выбрать и эксплуатировать состав устройств, с которыми сотрудник будет выполнять работу везде, а не только на рабочем месте, с максимальным удобством для себя и пользой для бизнеса, и как при этом не нарушить правила корпоративной безопасности? Эта задача не решается нажатием клавиши Enter. Она требует командной работы и творческого подхода. Знания и компетенция ИТ-специалистов и бизнес-менеджеров должны образовать синергетический прорыв, чтобы концепция BYOD радикально изменила бизнес-горизонт предприятия.

Но и результаты будут впечатляющими. 