Круглый стол

Плюсы, минусы и перспективы концепции BYOD

В круглом столе принимают участие

Сергей КОРОЛЬКОВ,
технический директор, «ДиалогНаука»

Дмитрий КОСТРОВ,
директор департамента информационно-телекоммуникационных технологий, NVision Group

Анна КРАВЦОВА,
ведущий специалист по продажам IBM Worklight, IBM в России и СНГ

Максим ЛУНГУ,
начальник отдела решений по контролю и защите контента, «ЭЛВИС-ПЛЮС»

Кирилл МЕЩЕРЯКОВ,
руководитель направления по работе с технологическими партнерами, компания «Актив»

Алексей ПАТРИКЕЕВ,
ведущий эксперт практики инфраструктурных решений, «Астерос Информационная безопасность» (группа «Астерос»)

Руслан ПЕРМЯКОВ,
заместитель директора по развитию, ООО СИБ

Анатолий ТРЕТЬЯКОВ,
менеджер по маркетингу сервисных продуктов, Fujitsu

Тема BYOD давно и активно обсуждается на страницах специализированных изданий. Каково положение дел на практике? Каковы реальные масштабы вовлечения личных мобильных устройств в «деловой оборот» на российском рынке?

Сергей КОРОЛЬКОВ

По данным Deloitte, 66% жителей России владеют смартфонами и 41% – планшетами. Чтобы включиться в концепцию BYOD, нужно всего лишь «принести» эти устройства, а точнее, подключить к корпоративным ресурсам. В опросе IDC около 70% респондентов заявили о наличии возможности удаленного доступа к электронной почте. При этом уровень использования решений MDM крайне низок и едва ли превышает 10%. Следовательно, мы на 90% находимся в ситуации, которая называется «unmanaged BYOD». Не нужно забывать и про данные опроса, который показал, что 17% сотрудников уничтожали ценные документы, чтобы навредить работодателю, 13% использовали служебные материалы на новом месте работы, а 4% пользовались информационной системой с прежней работы.

По мнению руководства компаний, возможность работы с личного устройства ускоряет взаимодействие сотрудников и повышает их продуктивность, иными словами, высший менеджмент считает ситуацию прекрасной и перспективной. С точки зрения руководства ИТ, ситуация управляема. А с точки зрения ответственного за обеспечение ИБ, существующее положение создает массу рисков информационной безопасности и будущее BYOD неоднозначно.

Дмитрий КОСТРОВ

Стоит отметить, что использование людьми собственных мобильных устройств только увеличивается. Компаниям выгоден такой подход: сотрудник сам покупает устройство, постоянно его модернизирует, ремонтирует

и т. д. При этом многие компании даже не используют системы MDM, считая, что за все проблемы с безопасностью отвечает сам работник. Размытие периметра безопасности усложняет процесс обеспечения безопасности информации, но решения существуют.

Анна КРАВЦОВА

По масштабам применения BYOD Россия пока отстает от западных стран, однако положительная динамика хорошо прослеживается. Если года два назад большинство российских компаний игнорировали BYOD, то сегодня многие начинают внедрять этот подход или задумываются о его внедрении. BYOD следует тенденциям современного общества, особенно в развивающихся странах, где границы между рабочим и личным временем размыты. Согласно данным аналитических опросов, сотрудники более 70% российских компаний предпочитают иметь доступ к рабочим приложениям в свободное время и использовать для этого личное устройство, которое подходит именно им. Руководство, как правило, тоже видит в BYOD источник конкурентного преимущества. Основные проблемы, связанные с BYOD, во всех странах похожи: это «головная боль» ИТ-департаментов, связанная с необходимостью поддержки бизнес-приложений на нескольких разных платформах, новые угрозы информационной безопасности и сложность обеспечения комплексной защиты устройств, используемых за пределами корпоративной сети. Пока не более половины ИТ-подразделений в России поощряют BYOD, и еще меньше компаний внедряют четкие политики реализации BYOD. Однако очевидно, что уже скоро ИТ-директорам придется поддерживать BYOD.

Максим ЛУНГУ

Действительно, тему BYOD сегодня не затронул, наверное, только ленивый. Практически в каждом номере тематических изданий BYOD освещается в том или ином аспекте. Об этой концепции много говорят на специализированных мероприятиях – делятся опытом, иногда претендуя на «истину в последней инстанции».

От всего этого иногда создается двойственное впечатление: то ли рынок зрелый, все всё понимают и знают что делать, то ли поставщики товаров и услуг пытаются насильно рынок «взорвать», продвигая, а иногда и навязывая подходы, методы и средства. На российском рынке происходит скорее второе – его пытаются «взорвать», и уже не один год. Причины понятны: личная мобильность сотрудников растет, а ее управляемость практически в каждой компании остается на «минус первом» уровне. Это так называемый BYOD по умолчанию – де-юре такую концепцию мало кто вводит, а де-факто она повсюду. BYOD де-юре означает, что сотруднику не просто разрешили пользоваться личным мобильным устройством в служебных целях, но и, как минимум, обеспечили управляемый и контролируемый доступ к корпоративным ресурсам. В случае BYOD де-факто руководство в большинстве случаев закрывает глаза на неконтролируемость доступа к корпоративным ресурсам с персональных устройств. Причины тому разные: неосознание масштаба возможных проблем, лень, отсутствие в компании человека, способного заниматься новым направлением, или попросту отсутствие проблем.

Сложно найти компанию, сотрудники которой, придя на работу, отключают личный смартфон или планшет, но при этом компания ждет постоянной доступности сотрудника и надеется на повышение его эффективности. Масштабы вовлеченности в работу личных мобильных устройств на российском рынке велики. Но говорить о зрелости модели и ориентированности именно на BYOD (что подразумевает внедрение целого направления в корпоративную ИТ/ИБ-культуру и инфраструктуру), наверное, рано. И перспективность данного направления в России оценить сложно, учитывая, что до сих пор случаи использования BYOD в нашей стране носят единичный характер. Возможно, без BYOD гораздо проще и бизнес не видит особых проблем?

Кирилл МЕЩЕРЯКОВ

Российский деловой рынок BYOD стоит разделить на две части: госсектор и частные коммерческие компании. В частных компаниях большинство сотрудников сейчас используют личные устройства для рабочих целей. Это удобно для сотрудника и экономически выгодно для компании-работодателя, так как не приходится покупать дополнительные мобильные устройства. Например, чтение корпоративной почты с личных мобильных устройств стало уже привычным явлением почти во всех частных компаниях. Именно с этим повсеместным распространением концепции BYOD и связано повышение интереса к темам обеспечения информационной безопасности для мобильных устройств.

Что касается госсектора, то там существуют законодательные ограничения, в силу которых использование информации жестко регламентировано. Понятия «мобильное рабочее место» в государственных компаниях обычно не существует. Но с недавних пор и для госсектора

стали разрабатываться специальные проекты корпоративной мобильности. Они предлагают систему управления мобильными устройствами через специальные приложения и систему защиты этих устройств.

Алексей ПАТРИКЕЕВ

В последние годы использование личных мобильных устройств в корпоративном сегменте неуклонно растет, и думаю, что направление будет и дальше набирать популярность. Развитию концепции способствуют повышение доступности мобильных устройств, постоянное развитие информационных систем компаний и непопулярность у работодателей решений по предоставлению сотрудникам корпоративных устройств (в силу экономии). Вчера можно было повсеместно наблюдать чтение рабочей почты со смартфона, а также видеть сотрудников, выполняющих свою работу с использованием различных гаджетов. Сегодня концепция Mobility вышла на уровень коммерчески оправданных проектов. Развитие интерактивных мобильных сервисов – отдельная перспективная ниша на этом рынке.

Руслан ПЕРМЯКОВ

Личные устройства в бизнесе применяются довольно широко. Собственные мобильные телефоны лет десять назад, а сегодня смартфоны и свои флешки – практически деловой стандарт. И что особенно важно, эти устройства приносят все – от рядового клерка до директора компании. Руководство компаний приносит свои ноутбуки. Планшеты в деловой среде пока не завоевали свою нишу, но скоро это случится. Появление на рынке дешевых и функционально стабильных планшетов неизбежно приведет к тому, что они появятся в компаниях.

Анатолий ТРЕТЬЯКОВ

Для людей, активно использующих всевозможные средства связи, мобильные устройства давно стали незаменимыми помощниками. Функциями записных книжек, органайзеров, телефонных справочников, будильников не пользуются разве что совсем пожилые люди или дети, хотя как раз последние в будущем и сформируют основную массу потребителей подобных услуг. Корпоративная и личная электронная почта, социальные сети и удаленный доступ к корпоративным системам, как показывает практика, могут успешно сосуществовать на широком спектре личных мобильных устройств при условии должного управления. Кстати, одно из европейских подразделений Fujitsu предоставляет услуги управления мобильными устройствами для своих клиентов, и это направление не такое уж молодое – оно существует с момента появления первых смартфонов на Symbian, т. е. более десяти лет.

Если говорить о масштабах вовлечения мобильных устройств в деловой оборот на российском рынке, то среди активной части населения больших городов такие устройства распространились практически молниеносно. Сегодня в общественном транспорте или других общественных местах сложно встретить человека без «карманного помощника». А проверка сообщений на своем телефоне, после того как это сделал кто-то другой, – это уже современный рефлекс.

Личное устройство на работе – новая угроза информационной безопасности компании, а в сегодняшних условиях – угроза неизбежная. Какими основными техническими средствами (первое, второе, третье) компания может обезопасить ценную корпоративную информацию? Что может считаться необходимым минимумом?

Сергей КОРОЛЬКОВ

Наверное, одним из самых эффективных способов обеспечения информационной безопасности является организация безопасного терминального доступа с мобильного устройства к ресурсам информационной системы. Но на этом преимущества данного способа заканчиваются.

Минимальный уровень безопасности при использовании BYOD обеспечивается применением технологии ActiveSync, доступной, например, в широко распространенном почтовом сервере MS Exchange. Не все знают, что применение ActiveSync позволяет реализовать на мобильном устройстве минимальный набор политик безопасности: управление парольной политикой, удаленное стирание информации с устройства, управление блокировкой устройства и др.

Оптимальным вариантом следует считать средства класса MDM,

позволяющие организовать на устройстве сотрудника «корпоративную область» данных и программ, управляемую в соответствии с корпоративными политиками безопасности.

Дмитрий КОСТРОВ

Личное устройство – это, конечно, угроза. Если руководство компании считает, что обрабатываемая на устройстве (доступная с устройства) корпоративная информация очень важна и конфиденциальна, есть возможность применить в «жесткой» форме принцип GOCD (Get Our Corporate Device), когда компания выдает сотруднику корпоративный гаджет.

Применение собственного устройства работника – это приемлемый риск при условии выполнения необходимых и достаточных требований безопасности. Нужно внедрять MDM-системы и облачные услуги для СМБ. Это тот минимум, который позволит защитить/контролировать корпоративную информацию.

Анна КРАВЦОВА

Обеспечение информационной безопасности – вопрос комплексный, поэтому решить его универсальным набором из трех технических средств невозможно. Если оставить в стороне политики и стратегию, важно помнить о трех основных объектах контроля – пользователях, данных и устройствах – и связанных с ними векторах атак. Технические средства должны быть направлены на все три участка и обеспечивать уровень безопасности и контроля, адекватный требованиям конкретной компании. В частности, это означает необходимость аутентификации (проверки подлинности) и пользователя, и приложений, и устройств, а также поддержки сквозной аутентификации (SSO). Данные личных приложений на устройстве должны быть отделены от корпоративных и зашифрованы (для чего, как правило, используется контейнеризация), а при передаче – защищены туннелированием трафика. Мобильные устройства нередко теряют и крадут, а значит, у ИТ должна быть возможность дистанционно очистить устройство или деактивировать доступ к чувствительной информации. Кроме того, организация должна иметь возможность принудительного обновления определенных приложений при обнаружении в них уязвимостей.

Максим ЛУНГУ

Личное устройство на работе – право или привилегия? Практически каждый второй пользователь корпоративной сети считает своим правом пользоваться личным мобильным устройством. Иногда сотрудника проще уволить, чем запретить ему пользоваться своим гаджетом на рабочем месте, но всегда ли стоит прибегать к радикальным мерам? Можно минимизировать риски организационными, правовыми и техническими мерами.

К техническим мерам относятся:

- выбор технических средств управления мобильными устройствами и безопасностью, связанной с мобильными устройствами;
- корпоративная политика доступа: правила доступа изнутри и извне контура компании; правила шифрования – VPN, криптоконтейнеры, усиленная аутентификация при доступе к корпоративным ресурсам (e-mail, календарь, документы), антивирусная защита, удаленное управление мобильным устройством, принудительное удаление информации на мобильном устройстве.

Кирилл МЕЩЕРЯКОВ

Существуют два вида угроз: внешние и внутренние. Внешние – это люди, которые пытаются украсть информацию с мобильных устройств. В таком случае для защиты следует использовать, во-первых, сложный пароль либо специальное аппаратное средство аутентификации для доступа к телефону или планшету; во-вторых, мобильные приложения, которые шифруют информацию при сохранении в память мобильного устройства, – такие приложения существуют, и их немало. Таким образом, если мобильное устройство попадет к постороннему лицу, вся информация на нем будет защищена от несанкционированного доступа. Слабая сторона – это человеческий фактор, поскольку многие пользователи не ставят сложные пароли для доступа к своему телефону или даже предпочитают вовсе не использовать пароли.

Если же угроза внутренняя (сам пользователь «сливает» секретную информацию), то защититься от этого практически невозможно. Единственное решение – программа, отслеживающая все действия сотрудника, которые он производит на своем мобильном устройстве. Но кто же согласится, чтобы за его личным телефоном постоянно следили?

Алексей ПАТРИКЕЕВ

Естественно, использование личного устройства в информационных процессах компании несет угрозу ИБ. Соответственно для эффективной защиты необходимо применять средства безопасности как на стороне корпоративных ресурсов, так и на стороне самого мобильного устройства. В первом случае речь идет о традиционных средствах контроля доступа и анализа передаваемой информации (МЭ, средства предотвращения вторжения IPS, DLP, DBF, WAF). В свою очередь, устройство пользователя необходимо обеспечить средствами, реализующими антивирусную защиту, защищенную передачу данных, контейнеризацию.

Руслан ПЕРМЯКОВ

Первое – шифрование, второе – система, реализующая политику MDM, третье – антивирус. Это минимум, все зависит от компании и цены ресурсов. Например, если цена корпоративных секретов высока, есть необходимость внедрения DLP-системы.

Анатолий ТРЕТЬЯКОВ

Попробуем составить список основных мер по обеспечению информационной безопасности:

- контроль и управление мобильными устройствами, отслеживание использования запрещенного ПО, сознательно созданных уязвимостей в системном ПО устройств – Jailbreak и root-доступа;

- наличие хотя бы минимальной защиты устройства с помощью пароля или средствами идентификации пользователей;
- удаленное блокирование и очистка устройства от данных в случае его утраты/кражи;
- отслеживание и управление внешними интерфейсами и каналами связи с внешним миром (Wi-Fi, Bluetooth, сотовая сеть, VPN).

Опционально могут использоваться программные средства блокирования свободного обмена информацией между различными приложениями внутри устройства и т. д.

Эти и дополнительные услуги могут быть предоставлены клиентам в виде готового сервиса на базе инфраструктуры ЦОД Fujitsu в Европе.

Какую дополнительную ценность может привнести в бизнес использование сотрудниками личных устройств – для крупного бизнеса, для сегмента СМБ?

Сергей КОРОЛЬКОВ

Применение личных мобильных устройств дает возможность вовлечь сотрудника в работу за пределами рабочего места и вне рабочего времени с минимальными затратами на изменение ИТ-инфраструктуры. Малый размер затрат является одним из важнейших факторов, влияющих на распространение технологий BYOD в СМБ.

В настоящее время наиболее «модные» и передовые технологии и ПО начинают распространяться именно на мобильных платформах. Бурно развивающиеся облачные сервисы глубоко интегрированы в мобильные платформы. Эти два фактора, а точнее, использование указанных технологий, могут принести дополнительные маркетинговые преимущества представителям сегмента СМБ.

В некоторых случаях, как ни странно, применение BYOD может повысить непрерывность бизнеса.

Дмитрий КОСТРОВ

Снижение затрат работодателя в СМБ. Но если серьезно, сейчас нет смысла говорить о дополнительных ценностях – использование собственных устройств в работе уже реальность, и к этому надо относиться как к совершившемуся факту.

Анна КРАВЦОВА

В СМБ-секторе применение BYOD началось даже раньше, чем в больших компаниях. Это объясняется в основном привлекательностью концепции для предприятий с ограниченными возможностями финансирования и маленькими ИТ-департаментами. Однако с развитием бизнес-приложений и самих мобильных устройств стал проявляться основной потенциал BYOD, привлекательный для компаний любого размера, – возможность сотрудников работать тогда и там, где их посещает вдохновение, реагировать на изменения и срочные вопросы максимально оперативно, получать удовольствие от работы на любимых устройствах без необходимости носить с собой дополнительные телефоны и планшеты. Помимо дополнительной мотивации сотрудников – отсутствие необходимости покупать устройства, вести их учет, обслуживать и списывать означает еще и сокращение расходов.

Максим ЛУНГУ

Ценность для бизнеса – повышение его эффективности. BYOD в его классическом виде по определению призван сделать бизнес эффективнее. Для компании это означает увеличение продуктивности сотрудника, экономию на средствах связи для персонала, мобильность и доступность сотрудника, его лояльность. Для сотрудника – право выбора личного устройства, независимость от корпоративных стандартов, мобильность, баланс между личной жизнью и работой.

Кирилл МЕЩЕРЯКОВ

Польза от применения сотрудниками мобильных устройств очевидна. Сотрудник всегда доступен, «всегда на работе», продлевается рабочий день. Даже если сотрудник болеет или уезжает на встречу/мероприятие, все равно он имеет возможность не отрываться от рабочего процесса. Если сотрудник использует для работы личное мобильное устройство, компания выигрывает экономически. Кроме того, дополнительная ценность для компаний – разработчиков софта или приложений может заключаться в том, что появляется возможность тестировать сервисы в «боевых» условиях на различных устройствах.

Алексей ПАТРИКЕЕВ

В условиях высокой конкуренции на нашем рынке использование BYOD приносит компаниям реальное конкурентное преимущество. Ведь личное мобильное устройство сотрудника почти всегда при нем в отличие от рабочего места и аналогичного корпоративного устройства. Это дает ряд преимуществ – от оптимизации бизнес-процессов до сокращения времени на принятие управленческих решений. Кроме того, сокращаются затраты на дополнительное оборудование, что особенно актуально для СМБ.

Руслан ПЕРМЯКОВ

Первое, что приходит на ум, – эффективность сотрудника. Его пребывание в привычном информационном окружении повышает эффективность при решении практически всех задач, особенно рутинных. Я предполагаю, что на современном рынке это решающий момент.

Анатолий ТРЕТЬЯКОВ

В первую очередь грамотно организованное управление мобильными устройствами может повысить удовлетворенность и продуктивность пользователей. Для некоторых отраслей существенным фактором может стать практически безграничная мобильность сотрудников и рабочих мест. Кроме того, значительно увеличивается скорость распространения и упрощается обмен информацией.

Какими способами удается разграничить на мобильном устройстве область персональной информации и корпоративной? Что представляет собой рынок специализированного ПО для смартфонов в рамках концепции BYOD?

Дмитрий КОСТРОВ

Уже придуман подход к разделению информации на мобильных устройствах на свою и корпоративную. Это создание «песочниц», в которых ведется работа с чувствительной информацией. Такой подход и должен применяться в дальнейшем.

Анна КРАВЦОВА

Основное техническое решение для разделения информации – создание зашифрованных областей (контейнеров), в которых хранится корпоративная информация. Контейнеры создают как сами производители мобильных устройств и сервисов, например Samsung, Google (после приобретения Divide), так и сторонние производители, в частности IBM, VMware, Citrix и т. д. Есть и аналогичные российские разработки. В рамках защищенного контейнера, как правило, предоставляются почтовый клиент, защищенный браузер, календарь, контакты, работа с документами и возможность управления настройками контейнера и мобильного устройства, задание политик безопасности и т. д. Как обязательное средство предоставляется SDK для разработки собственных программных продуктов, совместимых с контейнером. Сегодня программное обеспечение для контейнеризации – это коммерческие продукты. Однако с учетом таких фактов, как покупка компании Divide корпорацией Google, подписание соглашения между IBM и Apple, сохранение тренда BYOD, можно ожидать, что в скором времени появятся бесплатные аналоги минимального «корпоративного набора» для разделения корпоративных и личных данных на мобильных устройствах.

Максим ЛУНГУ

В общем случае можно рассмотреть два варианта: первый – на мобильное устройство не устанавливается никаких дополнительных средств защиты, второй – на мобильное устройство устанавливается специализированное программное обеспечение.

При первом варианте можно обойтись технологией VDI (Virtual Desktop Infrastructure). Такой сценарий подразумевает, что на устройстве не хранится никакой корпоративной информации. Она хранится и обрабатывается внутри периметра корпоративной сети, все приложения запускаются исключительно изнутри периметра. Доступ к приложениям и информации осуществляется через виртуальный рабочий стол. Перенос информации в обе стороны – на мобильное устройство и в корпоративную сеть – ограничен политикой безопасности.

Второй вариант подразумевает установку на мобильное устройство специализированного ПО, которое позволит контролировать контент, управлять приложениями и самим устройством. Для разграничения корпоративной и личной информации на мобильном устройстве создается отдельный контейнер – защищенная область. При этом данные, хранящиеся в защищенной области, зашифрованы; политикой безопасности определены доступные для пользователя корпоративные приложения; доступ к корпоративным ресурсам – строго по защищенному каналу; все содержимое на мобильном устройстве может быть в любой момент удалено из центра – по расписанию или принудительно. Перенос информации в обе стороны, как и в первом варианте, ограничен политикой безопасности.

Какой вариант выбрать? Если компания смотрит в сторону защищенной корпоративной мобильности, то сначала нужно опираться на те вендорские решения, которые уже есть в компании, и постараться их масштабировать на мобильные устройства. Такой подход позволит сэкономить и сделает комфортным переход на корпоративную мобильность в рамках BYOD.

Рынок ПО, в том числе российский, очень разнообразен. Есть отечественные и зарубежные решения. Разработчики предлагают бесчисленное множество функциональных возможностей, соответствие разного рода требованиям, в том числе регуляторных. Но все-таки проникновение специализированного ПО в России невелико, и связано это в первую очередь с низкой популярностью концепции BYOD.

При выборе корпоративных средств управления мобильными устройствами в рамках концепции BYOD необходимо исходить из задач и не верить на слово поставщику ПО. Нужно определить значимые критерии выбора и несколько доступных средств, провести тестирование и только тогда принимать решение.

Кирилл МЕЩЕРЯКОВ

Разграничение областей персональной и корпоративной информации производится либо на уровне отдельных приложений, либо на уровне системы. На уровне приложений все довольно просто и понятно. Например, в одном приложении сотрудник просматривает личную почту, а в другом (защищенном) – корпоративную. Это разделение удобно и легко реализуемо. Единственное требование – специальные приложения для рабочих целей должны быть качественными и удобными, чтобы у сотрудников не возникало проблем с их использованием.

Другой подход – разграничение на уровне системы. На данный момент такой подход разработала компания Samsung – это решение Samsung KNOX. Решение позволяет внутри одного устройства выделить две зоны. В личной зоне сотрудник может делать что угодно, устанавливать любые приложения. В рабочую зону уже установлены специальные корпоративные приложения, которые предоставила компания. Больше туда ничего поставить

нельзя, зона используется только для работы. Минус в том, что это решение применимо только для устройств Samsung. А концепция BYOD предполагает наличие у сотрудников мобильных устройств разных производителей.

Алексей ПАТРИКЕЕВ

В рамках концепции BYOD основным решением является MDM. Оно позволяет реализовывать защиту только части приложений, шифруя используемые ими данные. Есть ряд производителей подобных средств, у которых реализованы такие элементы защиты устройства, как контроль программной среды, организация защищенной передачи данных, контейнеризация, контроль доступа, «сброс» устройства в случае его утери.

Руслан ПЕРМЯКОВ

Способы традиционные – «разделяй и властвуй»: внедрение мандатного управления данными, классификация хранилищ в устройстве, шифрование хранилища и трафика.

Рынок такого рода программного обеспечения только оформился, и пространства для развития пока хватает. Сейчас для него открывается государственный сектор. Чего-то особенного для BYOD пока нет, все способы могут применяться и для корпоративных устройств

Какая аббревиатура (термин) придет на смену BYOD в обозримой перспективе – в контексте использования личных устройств на работе?

Дмитрий КОСТРОВ

Use All That Is At Hand – сейчас любое устройство должно помогать работе. Для работодателя важно, чтобы работник был доступен в режиме 24×7×365, да и самому сотруднику (если он заинтересован в работе) хотелось бы получать доступ к информации везде. Проблема с безопасностью? Да. Но есть понятие «риск-аппетит», и каждый руководитель должен либо принимать риск, либо нивелировать его.

Максим ЛУНГУ

Сложно предсказать, какая аббревиатура станет следующей. Сначала была BYOD, потом появилась CYOD… Что будет дальше? Возможно, BYOD как самостоятельное направление уйдет с рынка и будет рассматриваться как часть других комплексных решений.

Кирилл МЕЩЕРЯКОВ

Точную аббревиатуру назвать не смогу. По моему мнению, в ближайшие несколько лет понятие стационарного рабочего места исчезнет совсем, подавляющее большинство сотрудников перейдет на работу с мобильных устройств. Будут это личные или предоставленные компанией устройства, будет зависеть, скорее всего, от политики каждой конкретной компании.

Руслан ПЕРМЯКОВ

Если пофантазировать, можно представить что-то вроде Create Your Own Digital Environment (CYODE). Очевидно, что количество сервисов, приходящих в информационную среду предприятия, будет только расти. Ведь включая в среду устройство на базе Android, iOS, Windows, мы включаем в корпоративную сеть соответствующее облако. Использование голосовых команд тоже «цепляет» соответствующий облачный сервис. Поэтому можно говорить о создании уникальной пользовательской среды.

Анатолий ТРЕТЬЯКОВ

Например, «Услуги управления мобильными устройствами» (Managed Mobile Services) или «Управление взаимодействием с помощью мобильных устройств» (Managed Mobile Collaboration Service). ■

ПО для создания ГИС-приложений

Компания Esri CIS (официальный дистрибьютор в странах СНГ компании Esri, поставщика геоинформационных технологий, http://www.esri-cis.ru/) объявила о выходе первой официальной версии программного обеспечения ArcGIS Runtime SDK for .NET. Это ПО позволяет создавать готовые ГИС-приложения для настольных компьютеров и телефонов, работающих на ОС Windows, а также приложения для размещения в Windows Store. Скачать ArcGIS Runtime SDK for .NET 10.2.4 можно бесплатно на сайте Esri для разработчиков https://developers.arcgis.com/net/. На этапе создания современной высокопроизводительной ArcGIS Runtime SDK for .NET разработчики сосредоточились в первую очередь на адаптации опыта выпуска нативных приложений для .NET. Подход Esri заключается в построении нового общего API для нативных платформ, продвигаемых Microsoft. В частности, было составлено руководство для разработчиков на WPF, облегчающее переход от популярного ArcGIS Runtime SDK for WPF к новому SDK. Отметим, что ArcGIS Runtime SDK for .NET поддерживает работу офлайн-приложений, синхронизацию сервисов объектов, шейп-файлов, изменений на стороне клиента и многое другое. Компания Esri благодарит всех, кто участвовал в программе бета-тестирования ArcGIS Runtime SDK for .NET (более 3 тыс. разработчиков). Несмотря на то что бета-тестирование завершилось, на странице бета-сообщества по-прежнему доступны документация и статусы сообщений об исправлении выявленных ошибок.

www.esri-cis.ru