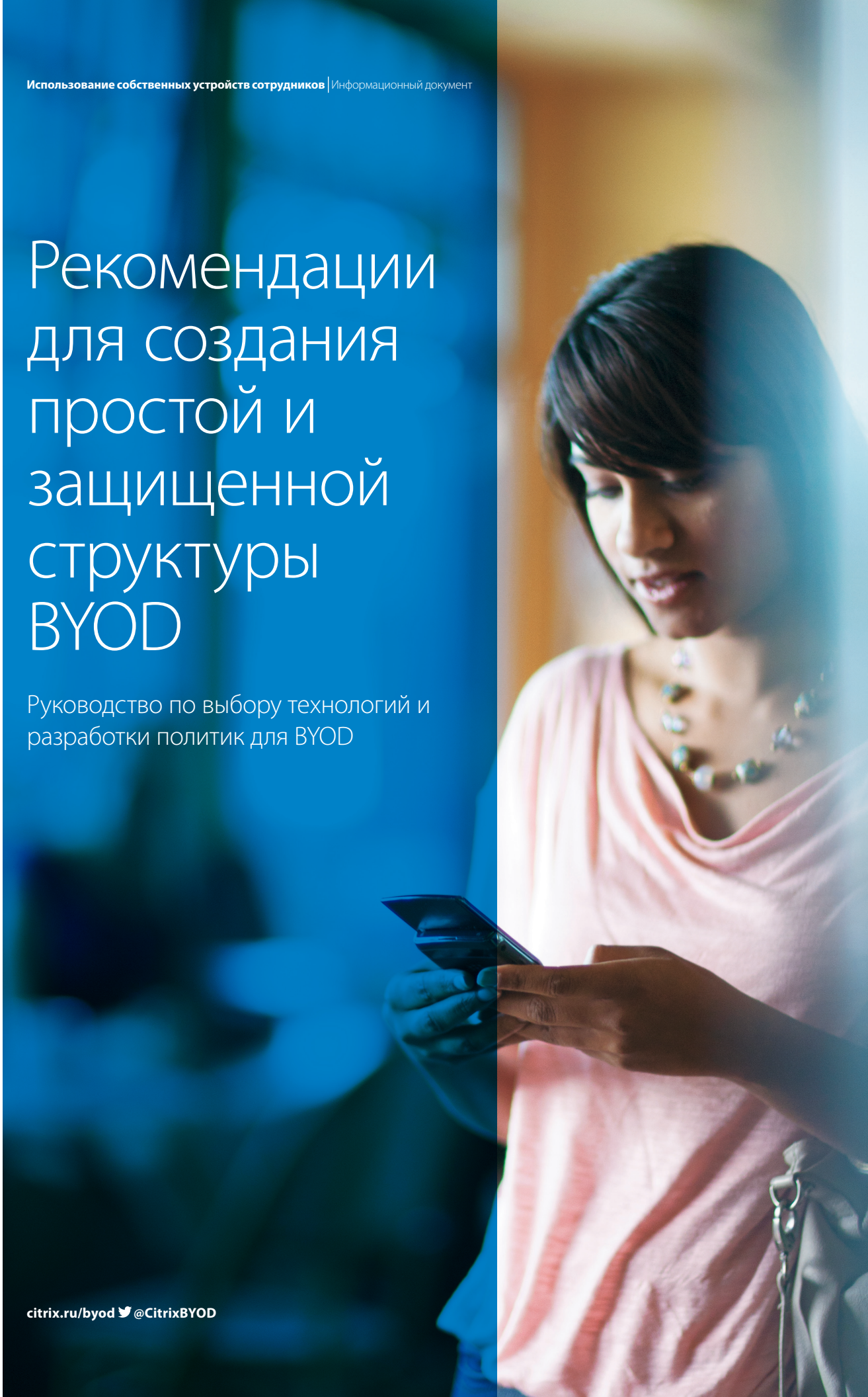
Рекомендации для создания простой и защищенной структуры BYOD

Руководство по выбору технологий и разработки политик для BYOD



CITRIX®

citrix.ru/byod **@CitrixBYOD**

Программы и политики BYOD (использование собственных устройств сотрудников) позволяют выбрать оптимальное устройство для выполнения работы, в том числе личный смартфон, планшет или ноутбук. В этом информационном документе приведены рекомендации по внедрению концепции BYOD, которая поможет сотрудникам стать более мобильными и эффективными, а также подготовит ИТ-инфраструктуру к работе с потребительскими устройствами простым, безопасным и контролируемым образом.

Поскольку ориентированность на потребителя все больше влияет на организацию ИТ-инфраструктуры, организации спешат разработать стратегии, позволяющие полностью реализовать концепцию использования собственных устройств сотрудников (BYOD). Сотрудники, которые могут выбирать оптимальное устройство для выполнения своей работы (ноутбук, смартфон, планшет), становятся более мобильными и эффективными. Более благоприятные условия труда помогают организациям набирать новые и удерживать существующие квалифицированные кадры. Если принадлежат сотрудникам, ИТ-отделу становится проще осуществлять закупки и управление конечными устройствами.

В этом документе приводятся рекомендации для ИТ-администраторов по созданию комплексной стратегии BYOD, обеспечивающей сотрудникам оптимальную свободу выбора. Для ИТ-инфраструктуры это позволяет ориентироваться на пользователя, соблюдая при этом требования к безопасности, простоте и экономии средств. Имея в своей основе технологии управления мобильностью предприятия, виртуализации приложений и десктопов Windows и безопасного общего доступа к файлам, а также зарекомендовавшие себя способы внедрения BYOD, эта стратегия открывает для вашей организации следующие возможности.

- **Расширение возможностей сотрудников** в выборе собственных устройств для улучшения производительности, совместной работы и мобильности.
- **Защита закрытой информации** от потери и хищения, соблюдение нормативных требований к конфиденциальности, соответствие стандартам и управление рисками.
- **Снижение затрат и упрощение управления** путем введения самообслуживания, автоматизированного управления и мониторинга.
- **Упрощение ИТ-инфраструктуры** благодаря наличию единого комплексного решения для защиты данных, приложений и устройств.

BYOD набирает популярность: формализуем ориентированность на потребителя и ставим ее под контроль

В широком смысле к BYOD может быть отнесена практически любая стратегия, которая позволяет сотрудникам использовать собственные устройства для выполнения работы (время от времени, часто или постоянно). Во многих организациях сотрудникам разрешается наряду со служебными компьютерам пользоваться дополнительными устройствами — смартфонами, планшетами, ноутбуками, домашними компьютерами, если это необходимо для достижения оптимальной гибкости, мобильности и эффективности. В некоторых организациях пошли еще дальше и полностью изъяли определенные типы служебных устройств у некоторых работников — тех, кто предпочитает пользоваться собственными устройствами. В некоторых случаях затраты работника на приобретение собственного устройства полностью или частично возмещаются путем выплаты регулярной компенсации. От подрядчиков все чаще требуют использовать собственные устройства вместо предоставляемых из числа оборудования, принадлежащего компании. В идеальном случае, способы реализации концепции BYOD, применяемые в организации, должны быть подробно изложены в виде формальной политики.

На самом деле очень многие сотрудники уже приносят на работу собственные устройства, вне зависимости от наличия или отсутствия политики BYOD на рабочем месте. В настоящий момент среднее число устройств, подключенных к корпоративной сети, составляет 5,18 шт. на одного работника умственного труда и 4,43 шт. на одного из всех работников. Ожидается рост этого показателя почти до 6 устройств к 2020 г.[1] Частично это отражает переход от доминирования традиционных настольных ПК в среде конечных устройств. Этот переход предусматривает более широкий выбор устройств по совокупности следующих параметров — мобильность, производительность, размер и вес — для оптимального выполнения своих задач, будь то ноутбук, планшет или смартфон.

К настоящему моменту во многих организациях BYOD продолжает практиковаться неофициально. В то же время, отсутствие более развитой инфраструктуры BYOD может стать причиной возникновения в организации потенциальных угроз — от несоответствия требованиям безопасности и нормативным стандартам до наращивания сложности ИТ-инфраструктуры. Поскольку ориентированность на потребителя продолжает быстро наступать, необходимо наличие комплексной BYOD-стратегии, охватывающей как политики, так и технологии.

С точки зрения технологий, наиболее очевидной проблемой является обеспечение доступа сотрудников к корпоративным приложениям и бизнес-информации с личных устройств. Простая установка приложений непосредственно на устройство существенно повышает угрозу безопасности, риск утечки конфиденциальной информации и нарушения требований соответствия, приведет к необходимости координации выдачи лицензий и усложнению работы службы поддержки. Такой же эффект дает внедрение BYOD только для устройств под управлением Windows и игнорирование других потребительских устройств. Многие люди также стали использовать для работы неуправляемые приложения других производителей и сетевые службы — ИТ-отделам необходимы средства контроля и управления такого рода деятельностью, а также способы предотвращения угроз безопасности организации из-за использования таких приложений.

Идеальный подход — это реализация вычислений полностью вне устройств с помощью средств управления мобильностью предприятия, виртуализации приложений и десктопов Windows, а также защищенного общего доступа к файлам, вместе со службами сетевого сотрудничества и дистанционной поддержки. Благодаря такому подходу ИТ-отдел сможет обеспечить оптимальную степень свободы для сотрудников с сохранением надлежащего уровня безопасности и контроля. Сотрудники получают безопасный доступ в одно касание ко всем своим Windows, веб-, SaaS- и мобильным приложениям через единый магазин приложений с любого устройства, через любые сети, путем единого входа в систему и при незаметном роуминге сессии при перемещении с места на место, между сетями и с одного устройства на другое. ИТ-отделы получают единую точку управления для быстрого контроля использования приложений любого типа и его отмены, как с целью

Принципы успешной реализации стратегии BYOD

Сотрудники должны иметь полную свободу в выборе устройства для работы, в том числе того же устройства, которым они пользуются в личной жизни, и иметь возможность непрерывно работать на различных устройствах в течение дня.

ИТ-структура должна обеспечивать доставку по запросу файлов, приложений и десктопов на любое устройство везде, через любое соединение, сохраняя единообразие и эффективность защиты, исполнение политик, соответствие стандартам и контроль через единую точку управления.

предоставления новых ресурсов, так и для отключения доступа в случаях, когда он больше не требуется или нежелателен. В большинстве ситуаций бизнес-информация остается под защитой в центрах обработки данных; если она размещается на конечных устройствах, ее защита осуществляется путем изолирования, шифрования и механизмов дистанционного удаления.

Таким образом ИТ-отделы могут упростить управление и снизить затраты, позволяя сотрудникам работать удобно, безопасно и непрерывно на устройстве любого типа вне зависимости от его принадлежности. Использование возможности детального управления данными, сессиями и информацией приложений позволяет обеспечить защищенный доступ к конфиденциальным данным на личных устройствах сотрудников. ИТ-отделы получили возможность контроля использования и управления приложениями, данными и устройствами по уникальным идентификаторам, автоматического отключения учетных записей уволенных сотрудников и избирательного удаления данных на утерянных устройствах.

Используемые политики BYOD могут существенно отличаться в различных организациях в зависимости от выбранных приоритетов и целей, при их создании необходимы консультации с отделом кадров, финансовым, юридическим отделом и службой информационной безопасности. Рекомендации и практические примеры разработки политик приведены в следующем разделе.

Элементы комплексной BYOD-стратегии	
Технология и системы	• Магазин приложений с самообслуживанием, обеспечивающий унифицированный защищенный доступ и единый вход в мобильные, веб-, пользовательские и Windows-приложения с любого устройства через любые сети. • Управление мобильностью предприятия для защиты как мобильных устройств, так и бизнес-информации, к которой с них осуществляется доступ. • Защищенная доставка приложений и десктопов по запросу на любое устройство — личное или служебное — с отслеживанием и мониторингом для обеспечения соответствия стандартам и сохранения конфиденциальности. • Защищенный общий доступ к файлам и синхронизация с любого устройства. • Совместная работа, в том числе сетевые конференции с видеоизображением высокой четкости, а также совместные рабочие пространства, доступ к которым возможен с любого устройства. • Дистанционная поддержка пользователей и технологий независимо от местоположения.
Политики	• Предоставление права. • Разрешенные устройства. • Доступность служб. • Внедрение. • Распределение затрат. • Безопасность. • Поддержка и обслуживание.

Рекомендации и методы внедрения BYOD

Успешная инициатива по реализации BYOD сочетает в себе упрощение работы сотрудников с эффективной защитой, мониторингом и управлением для ИТ-отдела. Несмотря на соблазн для ИТ-отделов разработать отдельную политику для каждой возможной ситуации, в действительности большинство проблем могут быть решены путем применения нескольких простых согласованных между собой принципов. В большинстве случаев ИТ-отдел сможет справиться с управлением и обеспечением сотрудникам безопасного доступа к приложениям, данным и файлам, используя управление на основе ролей, настройку и средства безопасности личных устройств для защиты организации от угроз, потери данных и нарушения требований соответствия.

Приемлемость использования

Организации должны четко обозначить, кому из сотрудников разрешено использовать личные устройства, как на нерегулярной основе в дополнение к корпоративному конечному устройству, так и для постоянного замещения корпоративного устройства, либо каким-либо схожим образом. Предоставление доступа может рассматриваться как привилегия, которую можно заслужить, как реализация требований сотрудников, как требование для ролей определенных типов, как избыточный риск в некоторых случаях или, чаще всего, как сочетание этих подходов. Пол Мартин (Paul Martine), руководитель информационной службы Citrix: «Следуя своей философии "открытого рабочего пространства", компания Citrix позволяет каждому сотруднику приносить с собой любое устройство для работы без ограничений».

Программы, реализующие замену корпоративных конечных устройств личными, часто с выплатой компенсаций работникам, требуют внимания к другим аспектам. Одним из способов определения того, кто обладает правом на участие в программе такого рода, является рассмотрение таких критериев, как род деятельности, частота командировок, эффективность сотрудника и необходимость в автономном доступе к конфиденциальным данным. Шон Геновэй (Shawn Genoway), старший ИТ-директор компании Citrix: «В компании Citrix любой, кому было дано право использовать ноутбук, может участвовать в программе и получить соответствующую компенсацию для замены своего служебного устройства на личное, если у него есть одобрение руководства». Хотя возможность предоставления этого права определяется по самым различным факторам, за руководителями должно всегда оставаться последнее слово в утверждении сотрудников, которые могут стать кандидатами на получение компенсации за замену своего служебного устройства на личное по собственному выбору. Руководителям также целесообразно применять подходы BYOD в контексте других служебных поощрений, привилегий и дисциплинарных мер.

Как правило, подрядчики являются самыми подходящими кандидатами для программы BYOD. В большинстве организаций подрядчики уже должны использовать собственные устройства; более того, это требование нацелено на обеспечение соответствия независимых подрядчиков стандартам.

Разрешенные устройства

В ситуациях, когда приложения устанавливаются непосредственно на конечные устройства, ИТ-отдел должен определять и устанавливать минимальные характеристики устройств для поддержки операционных систем и приложений, обеспечения производительности и других аспектов использования устройств. Виртуализация десктопов устраняет эту необходимость путем обеспечения возможности запуска полнофункционального десктопа и приложений Windows на устройстве любого типа. С помощью решения для управления мобильностью предприятия ИТ-отделы могут регистрировать любое устройство и управлять им, обнаруживать устройства под управлением суперпользователя, а также полностью или выборочно стирать данные с несоответствующих стандартам, утерянных, украденных и принадлежащих уволенным подрядчикам или сотрудникам устройств. В компании Citrix, где работники используют

Работники компании Citrix соблюдают следующие правила BYOD.

1. Подключение через Citrix Receiver.
2. Доступ к предоставленным приложениям через защищенный унифицированный магазин приложений.
3. Совместное использование, синхронизация и защита файлов через Citrix ShareFile.
4. Использование надлежащего антивирусного ПО.
5. Обращение к поставщикам оборудования при возникновении аппаратных проблем.
6. Соблюдение все корпоративных политик, включая контроль за защитой устройства.

Порядок замены работниками Citrix служебного ноутбука на личный.

1. Требуется одобрение руководителя.
2. Выплачивается компенсация в размере 2 100 долларов США (минус соответствующие налоги) за приобретение ноутбука в рамках договора на трехлетнее использование.
3. Компенсация пересчитывается пропорционально, если сотрудник покидает компанию ранее, чем через год.

любые устройства по своему выбору, уже используется более двух тысяч личных ноутбуков и около двух тысяч личных планшетов, а также более четырех тысяч личных смартфонов, в том числе устройства под управлением iOS и Android, которые используются для самых разных целей — от просмотра электронной почты до полного доступу к приложениям через Citrix Receiver.

Участников следует обязать приобретать персональные устройства через обычные розничные сети, а не через отдел закупок организации. Это позволит иметь четкую историю владения, а также обеспечит прямое общение участников программы со своим поставщиком оборудования. Также работникам можно предоставить корпоративные скидки, если с данным поставщиком у организации имеются партнерские связи. Некоторые работники могут захотеть или будут вынуждены подключить к своему устройству периферийное оборудование, например мониторы или клавиатуры, для работы в офисе. В этом случае следует указать, кто будет приобретать и кто будет владеть каждой единицей оборудования.

Доступность служб

Концепция BYOD не обязана носить исключительный характер. Следует продумать, какие именно службы вы хотите предоставлять на личных устройствах и будет ли их набор различен для различных групп работников, типов пользователей, устройств и сети.

Для людей, которым нравится устанавливать приложения непосредственно на своей компьютер для личного использования, организации могут организовать скидки на профессиональные версии пакета Office для Mac и ПК по программе Microsoft Software Assurance. В таком случае, лицензирование полностью переходит под личную ответственность работника, а компания сможет избежать рисков или ответственности за нарушение прав собственности.

Внедрение

После разработки концепции BYOD для ее успешной реализации чрезвычайно важен этап информирования. Сотрудникам должны быть предоставлены информационные руководства, которые помогут принять решение о целесообразности участия в программе и о том, как выбрать необходимое устройство для своих нужд. Они также должны осознавать степень ответственности, которую они принимают на себя при использовании собственного устройства, в том числе при доступе к данным, их использовании и хранении. Рабочие и бизнес-данные должны храниться на личных устройствах строго изолированно для соответствия требованиям электронного поиска и политикам хранения данных. Таким же образом служебная электронная почта никогда не должна отправляться с личных ящиков. Политика пользования должна распространяться на личные устройствах в той же мере, что и на служебные.

Распределение затрат

Одним из главных преимуществ внедрения концепции BYOD является возможность снижения затрат путем частичной или полной оплаты сотрудниками стоимости различных устройств, которые они используют для работы, и освобождение ИТ-отдела от обязанностей по закупке и поддержке растущего парка аппаратных средств в масштабах предприятия. Это в наибольшей степени справедливо для ситуаций с прекращением предоставления служебных ноутбуков и других устройств. Недавнее исследование показывает, что подавляющее большинство организаций, внедривших или планирующих внедрить BYOD, частично либо полностью компенсируют сотрудникам затраты на собственные устройства для рабочих нужд. Предоставление компенсации также может позволить организациям в некоторой степени управлять ориентированностью на потребителя — 61 процент респондентов указывают это как основную цель выплаты компенсации или финансового возмещения.[2]

«Программа "Использование собственных устройств сотрудников" компании Citrix, которая позволяет заменить свои служебные устройства на личные, создавалась в расчете на экономию 18-20 %, — заявил г-н Мартин. — Эта величина, достигаемая за счет уменьшения общей стоимости стандартного служебного устройства, которое могло быть предоставлено, включая стоимость операционной системы, трехлетнего обслуживания и гарантии, а также налоговый вычет, используется для расчета предоставляемой денежной компенсации». Участники программы должны быть осведомлены, что выплачиваемое пособие считается доходом, подлежащим налогообложению. В регионах с повышенными ставками индивидуального налога на прибыль можно увеличить размер компенсации так, чтобы чистый объем субсидии был равным для всех участников программы. Любая BYOD-политика, с распределением затрат или без нее, должна четко обозначать, кто будет платить за доступ к ресурсам вне сетевой инфраструктуры компании, например по беспроводным 3G-сетям, через общественные Wi-Fi-сети или проводной широкополосный доступ из дома.

Если будет выплачиваться субсидия, то она должна соответствовать всему сроку участия работника. Субсидии должны предоставляться на регулярной основе, например, через каждый стандартный трехлетний цикл обновления аппаратных средств, для того, чтобы личные устройства устаревали по сравнению со служебными. Если участник увольняется из компании в течение цикла реализации BYOD, можно затребовать возвращения части выделенной субсидии. В компании Citrix работники, которые увольнялись из компании или прекращали участие в программе в течение года после регистрации, обязаны были возвратить пропорциональную долю полученной субсидии.

Распределение затрат влияет на характер внедрения BYOD в организации. Одновременное внедрение может повысить расходы по мере вступления сотрудников в программу и, как следствие, взыскания субсидии, в каждый момент начала цикла обновления конечных устройств. Предложение вступать в программу работникам накануне окончания срока использования их устройств позволит распределить нагрузку, обычно на три года. Организации, которые не предоставляют субсидий, могут открыть регистрацию всех желающих сотрудников в первый день работы программы.

Безопасность и соответствие стандартам

Многие ИТ-директора выражают озабоченность тем, что предстоящая ориентированность на потребителя ИТ-структуры приведет к значительному увеличению бизнес-рисков. Это обоснованное сомнение, которое часто возникает у клиентов Citrix, обращающихся за рекомендациями по внедрению BYOD. В то время, как установка приложений непосредственно на некорпоративные устройства может повысить риски, программа BYOD основана на технологиях управления мобильностью предприятия, виртуализации приложений и десктопов Windows, защищенного общего доступа к файлам, что позволяет управлять рисками и снижать их. Вся бизнес-информация остается защищенной в центрах обработки данных, ее хранение на конечных устройствах осуществляется только в случаях крайней необходимости. В случаях когда требуется хранение данных на конечном устройстве, они могут быть защищены путем их изоляции, шифрования и методами дистанционного удаления. Для предотвращения утечки ИТ-отдел может использовать политики, запрещающие вывод на печать или доступ к устройствам хранения на стороне клиента, таким как локальные диски и USB-накопители. Участники программы также должны обеспечить надлежащую установку и обновление антивирусного и антишпионского ПО на конечном устройстве. Компания Citrix бесплатно предоставляет антивирусную защиту работникам, участвующим в программе BYOD.

На мобильных устройствах контроль, защита и управление доступом к приложениям и данным могут осуществляться с помощью политик, учитывающих владельца устройства, состояние или местоположение. ИТ-отделы могут регистрировать любое устройство и управлять им, обнаруживать устройства под управлением суперпользователя, а также полностью или выборочно удалять данные с несоответствующих требованиям, утерянных, украденных или принадлежащих уволенным сотрудникам и подрядчикам устройств. Средства обеспечения безопасности приложений включают: безопасный доступ к приложениям через туннельные соединения, черный список, белый список и динамичные контекстно-зависимые политики.

Для защиты сети предприятия некоторые организации используют технологию управления сетевым доступом (network access control, NAC) для аутентификации пользователей, подключающихся к сети, и проверки наличия на их устройствах антивирусного ПО и последних обновлений безопасности. Компания Citrix использует иной подход, позволяя участникам программы BYOD использовать сеть Citrix для доступа по запросу к своим данным, приложениям и десктопам через Citrix NetScaler Access Gateway после двухфакторной аутентификации, но не позволяя подключать само личное устройство к сети. «Такой подход позволяет устанавливать минимальное количество ограничений на личных устройствах пользователей, но обеспечивает безопасность нашей сети и соответствует принципам открытой вычислительной культуры, принятой в компании Citrix», — отметил г-н Геновэй. NetScaler Access Gateway можно также использовать для предоставления детального доступа, основанного на политиках, к приложениям и данным через веб-браузер. Единый вход в систему и устойчивые ко взлому пароли обеспечивают удобство и защиту.

Вне брандмауэра виртуализация и шифрование обычно могут нивелировать уязвимости в системе безопасности Wi-Fi, WEP-шифрования, открытых беспроводных сетей, 3G/4G и других методов доступа потребительского уровня. Средства сетевой безопасности обеспечивают обнаружение и защиту от внутренних и внешних мобильных угроз; блокировку неконтролируемых устройств, неавторизованных пользователей и не отвечающих требованиям приложений; а также интеграцию с системами управления относящейся к безопасности информацией и событиями (SIEM).

В случае ухода участника программы BYOD из организации, нарушения политики BYOD, утери или кражи личного устройства ИТ-структура должна иметь способ немедленного прекращения доступа к данным и приложениям, включая автоматическую отмену контроля использования связанных с работой учетных записей SaaS и выборочное удаление данных на утерянных устройствах.

Вместо разрешения реализации открытых подходов BYOD, при которых работники могут использовать любые устройства для доступа к приложениям и данным предприятия, некоторые организации выбирают управляемый подход. В этом случае ИТ-отдел управляет личными устройствами напрямую, включая регистрацию, проверку, авторизацию и доступ к ресурсам устройства.

Поддержка и обслуживание устройств

Программа BYOD часто снижает общий объем обслуживания, необходимый для каждого устройства, потому что пользователь также является и владельцем устройства. «Это подтвердит любой, кто брал машину напрокат. Люди заботятся о своем имуществе лучше, чем кто-либо посторонний. У личного устройства гораздо меньше шансов возврата в ИТ-отдел со следами кофе, пролитого на клавиатуру», — говорит г-н Геновэй.

Тем не менее, политика BYOD должна четко определять организацию и финансирование технического обслуживания и поддержки. Когда личное устройство заменяет служебное конечное устройство, у пользователей могут возникать завышенные ожидания от ИТ-поддержки — этот момент должен быть четко определен, чтобы не допустить существенного увеличения объема сложности работы ИТ-отдела.

Стремясь не допустить усложнения структуры, для чего собственно и внедряются политики BYOD, компания Citrix предпочла режим «без участия», предоставляя поддержку только по вопросам беспроводной сети, антивирусного и антивредоносного ПО и в отношении клиентов Receiver на личных устройствах. Работники Citrix, использующие личные компьютеры, имеют возможность запроса на получение прокатного устройства Citrix сроком на 10 дней в случае необходимости в ремонте собственного устройства. Вся остальная поддержка осуществляется через форум сообщества участников BYOD, в котором предусмотрен раздел получения самостоятельной поддержки.

В то время, как некоторые ИТ-организации создают целые команды для поддержки BYOD, в компании Citrix программе посвящается только 10 процентов рабочего времени работника, включая ведение блога BYOD, ответы на вопросы и выплату компенсаций участникам программы. Подобно тому, как для многих потребительских устройств в комплект поставки включено краткое руководство по началу работы объемом всего один лист, компания Citrix сосредоточена на том, чтобы облегчить пользователям загрузку Receiver на любое устройство и быстро ввести его в работу.

Стратегия технологической безопасности BYOD

Компания обеспечивает поддержку BYOD в организациях, предлагая единый магазин приложений и защищенный доступ к бизнес-информации. Решения Citrix BYOD включают в себя управление мобильностью предприятия, виртуализацию приложений и десктопов Windows, защищенный общий доступ к файлам, совместную работу и дистанционную поддержку. В рамках этого подхода ИТ-отделы могут обеспечить доступность корпоративных приложений, защищенного общего доступа к файлам и синхронизацию для любых устройств, которые сотрудники принесут на работу, сохраняя при этом требуемый уровень безопасности и контроля.

В решениях Citrix BYOD используются все необходимые функции, чтобы концепция BYOD стала простой, безопасной и эффективной в любой организации.

Магазин приложений *на основе Citrix Receiver*
Доступ к необходимым приложениям с устройств по своему выбору, в том числе с десктопа или ноутбука под управлением Windows или Mac, мобильного устройства под управлением iOS, Android или Windows, Google Chromebook или мобильного устройства BlackBerry. Все эти устройства будут работать с непрерывным роумингом и в высоком разрешении из любого места и через любые сети. Единый магазин приложений обеспечивает доступ в одно касание к мобильным, веб-, пользовательским и Windows-приложениям, включая встроенный общий доступ к файлам и приложения для повышения производительности.

Защищенный доступ *на основе Citrix NetScaler Access Gateway*
Унифицированная структура управления позволяет ИТ-отделам защищать, управлять и оптимизировать доступ к приложениям, десктопам и службам с любого устройства. Управление доступом, аудит и создание отчетов с поддержкой соответствия стандартам и защитой данных.

Управление мобильностью предприятия *на основе Citrix XenMobile*
ИТ-отделы получают возможность контроля использования и управления приложениями, данными и устройствами по уникальным идентификаторам, автоматической отмены контроля использования учетных записей уволенных сотрудников и выборочное удаление данных на утерянных устройствах. Бизнес-приложения и данные, разработанные как ИТ-отделом, так и сторонними лицами, находятся в хранилище, отделенном от личных приложений и данных на устройстве.

Обеспечение безопасности компанией Citrix при разработке решений BYOD

- Управление мобильностью предприятия, виртуализация приложений и десктопов Windows и общий доступ к файлам обеспечивают безопасность, защиту данных и управление ИТ-ресурсами для личных устройств с такой же степенью эффективности, как и для корпоративных устройств.
- Все данные предприятия хранятся и подвергаются резервному копированию в центре обработки данных.
- Конфиденциальная бизнес-информация доставляется на конечные устройства только в изолированной зашифрованной форме для предотвращения потери и кражи.
- В случаях когда необходимо хранение данных на личных устройствах, ИТ-отдел получает возможность изолировать, шифровать и, при необходимости, удалять эти данные дистанционно.
- Централизация данных и выполнение вычислений по запросу на любом устройстве способствуют непрерывному функционированию предприятия и быстрому восстановлению после отказов.
- Политики управления записями, информацией и хранения данных для документов и электронной почты применяются и контролируются централизованно.
- Комплексный мониторинг, протоколирование действий и составление отчетов обеспечивают конфиденциальность данных и соответствие стандартам.

Виртуализация десктопов и приложений Windows *на основе Citrix XenDesktop и Citrix XenApp*
ИТ-отделы могут преобразовать приложения и целые десктопы Windows в услуги по запросу для любого устройства. Поскольку управление приложениями и данными производится внутри центров обработки данных, ИТ-отделы могут централизованно обеспечивать защиту данных, соответствие стандартам, управление доступом и администрирование пользователей на личных устройствах так же легко, как на корпоративных конечных устройствах, и в той же самой унифицированной среде.

Совместное использование файлов *на основе Citrix ShareFile*
Безопасное использование данных совместно с любым пользователем и синхронизация файлов на всех своих устройствах. Гибкие возможности хранения, управление на основе политик, составление отчетов, шифрование данных и их дистанционное удаление позволяют сохранять высокую степень защищенности бизнес-данных.

Сотрудничество *на основе Citrix GoToMeeting и Citrix Podio*
Сотрудники могут за несколько секунд организовывать встречи и присоединяться к ним из любого места, с любого устройства, с поддержкой передачи видеоизображения высокой четкости для непосредственного личного общения. Citrix GoToWebinar и Citrix GoToTraining также позволяют сотрудникам проводить большие семинары или учебные сессии по сети. Ленты активности в соцсетях, пользовательские приложения и совместные рабочие пространства помогают сотрудникам работать вместе более эффективно.

Дистанционная поддержка *на основе Citrix GoToAssist*
Централизованная поддержка пользователей и технологий со стороны ИТ-отделов вне зависимости от их местонахождения с целью сокращения простоев в работе ПК, компьютеров Mac, мобильных устройств, серверов и сетей в пределах организации.

Заключение

Являясь стратегией, которая лежит в основе таких ИТ-тенденций, как ориентированность на потребителя, гибкость рабочего пространства, мобильность и облачные вычисления, BYOD будет продолжать менять способ организации работы сотрудников и организаций. Правильная стратегия, реализованная посредством доставки по запросу данных, приложений и десктопов на любое устройство, обеспечит следующие возможности.

- **Расширение возможностей сотрудников** в выборе собственных устройств для улучшения производительности, совместной работы и мобильности.
- **Защита закрытой информации** от потери и хищения, соблюдение нормативных требований к конфиденциальности, соответствие стандартам и управление рисками.
- **Снижение затрат и упрощение управления** путем введения самообслуживания, автоматизированного управления и мониторинга.
- **Упрощение ИТ-инфраструктуры** благодаря наличию единого комплексного решения для защиты данных, приложений и устройств.

Являясь лидером в поставке гибких решений для мобильного стиля работы и одной из первых компаний, внедривших BYOD в своей организации, опираясь на свой практический опыт и использование зарекомендовавших себя методов, компания Citrix предоставляет комплексные технологии для успешной реализации программ BYOD. Решения BYOD от Citrix уже помогли многим организациям различных масштабов получить все преимущества от реализации программы BYOD.

Для получения дополнительных сведений посетите веб-сайт www.citrix.ru/byod или ознакомьтесь с другими нашими информационными документами по этой теме.

Дополнительные ресурсы

- Безопасная доставка корпоративной информации на устройства под управлением Android и Apple iOS
- Управление мобильностью предприятия: работа с концепцией BYOD (использование собственных устройств сотрудников) с безопасной доставкой приложений и данных
- Комплект Starter Kit для организации использования собственных устройств сотрудников

1,2 Citrix, Workplace of the Future: a global market research report, September 2012.

Представительство Citrix Systems
в России и странах СНГ
Комплекс Москва Сити, Северная башня
Адрес: 123317, г. Москва,
ул.Тестовская д.10,
Тел. +7 495 662 1726
www.citrix.com

О Citrix
Citrix (NASDAQ:CTXS) — компания, предлагающая облачные технологии для мобильного стиля работы, поощряя людей работать и сотрудничать из любого места, осуществляя безопасный доступ к приложениям и данным с любых современных устройств так же легко, как из собственного офиса. Решения Citrix по облачным вычислениям помогают ИТ-отделам и поставщикам услуг создавать частные и публичные облачные системы, используя виртуализацию и сетевые технологии для обеспечения высокой производительности, гибкости и экономической эффективности услуг для мобильного образа жизни. С помощью лидирующих на рынке решений для мобильных устройств, виртуализации десктопов, облачных сетевых технологий, облачных платформ, организации сотрудничества и совместного использования данных компания Citrix помогает организациям любого размера обрести скорость и гибкость, необходимые для достижения успеха в современном мире, который становится все мобильнее и динамичнее. Более 260 000 организаций и более чем 100 млн пользователей по всему миру используют продукты Citrix. Годовой доход в 2012 году составил 2,59 млрд долларов США. Узнать больше на сайте www.citrix.ru.