IBM Security
Описания – Передовые идеи

Десять правил использования собственных устройств (BYOD)

Узнайте, как защитить данные предприятия, если сотрудники используют для работы персональные устройства

IBM

Следует ли разрешить использование собственных устройств?

Быстрый рост количества мобильных устройств на рабочих местах для многих ИТ-руководителей представляется необъяснимым. Мобильные устройств и приложения для этих устройств изменили образ нашей жизни – общение, путешествия, покупки, работу и др. Это преобразование мобильной инфраструктуры было настолько радикальным, настолько революционным, что уже сложно представить себе жизнь без мобильных устройств. Возникла концепция использования собственных устройств сотрудников, которая была принята сотрудниками с энтузиазмом.

Бессмысленно притворятся, что ничего не происходит, или заявлять: «Мы запрещаем это для своих сотрудников». Правда заключается в том, что сотрудники уже используют мобильные устройств и, скорее всего, продолжат подключаться к сети предприятия с использованием недопустимых устройств независимо от того, есть на это разрешение или нет. В 2016 г. большей части сотрудников предприятий будет запрещено использовать в рабочих целях собственные смартфоны или планшеты.

При этом неизбежно возникает вопрос: как поддержать желание сотрудников использовать персональные приложения и устройства и повысить их производительность в безопасной среде с защитой данных предприятия? *Десять правил использования собственных устройств (BYOD)* показывают, как создать спокойную, защищенную и эффективную мобильную среду.

Десять правил использования собственных устройств (BYOD)

1. Сначала разработайте политику, а затем приобретайте технологию
2. Выявите устройства с доступом к ресурсам предприятия
3. Используйте простую регистрацию
4. Настраивайте устройства по беспроводной связи
5. Помогите своим пользователям помочь самим себе
6. Соблюдайте конфиденциальность персональной информации
7. Храните персональные данные отдельно от данных предприятия
8. Управляйте использованием данных
9. Постоянно контролируйте устройство на предмет несоответствия принятым требованиям
10. Используйте прибыль на инвестированный в собственные устройства пользователей капитал

1. Сначала разработайте политику, а затем приобретайте технологию

Как и для других ИТ-проектов политика должна предшествовать технологии – даже в облачной среде. Для эффективного использования технологии управления мобильными устройствами (MDM) в отношении сотрудников с собственными устройствами по-прежнему необходимо принять решение о политиках. Такие политики влияют не только на ИТ, они воздействуют на отдел управления персоналом, юридический отдел и отдел обеспечению безопасности – на любую структуру в организации, где мобильные устройства используются для повышения производительности.

Политика в отношении собственных устройств влияет на все бизнес-подразделения, поэтому ее невозможно разработать исключительно силами ИТ-отдела. С учетом различных потребностей пользователей ИТ-специалисты должны понимать, что все эти пользователи причастны к разработке политики.

Одной правильной политики в отношении собственных устройств не существует, но имеется ряд вопросов, на которые следует найти ответы:

- **Устройства.** Какие мобильные устройства будут поддерживаться? Только определенные устройства или любые устройства по желанию пользователей?
- **Тарифные планы.** Будет ли организация оплачивать счета за мобильные устройства? Будет ли это регулярная денежная выплата и будут ли сотрудники представлять отчеты о расходах?
- **Соответствие нормативным требованиям.** Какие правила в организации регулируют использование данных, требующих защиты? Например, закона о преемственности страхования и отчетности в области здравоохранения (HIPAA) требует наличие встроенного шифрования на любом устройстве, где хранятся данные, на которые распространяется действие закона.
- **Безопасность.** Какие требуются меры безопасности (защита паролем, устройства с несанкционированным изменением микропрограммы или правами суперпользователя, антивредоносные приложения, шифрование, ограничения для устройств, резервирование iCloud)?
- **Приложения.** Какие приложения запрещены? Сканирование IP-адресов, совместное использование данных, Dropbox?
- **Соглашения.** Распространяется ли на устройства сотрудников с данными предприятия соглашение о допустимом использовании (AUA)?
- **Услуги:** К ресурсам какого типа предоставляется доступ к сотрудникам – к электронной почте? Используются ли беспроводные сети или VPN? Системы управления взаимоотношениями с клиентами (CRM)?

- **Конфиденциальность.** Сбор каких данных выполняется с устройств сотрудников? Какие персональные данные никогда не собираются?

Когда речь идет об устройствах пользователей, для вопросов нет никаких ограничений. Это должен быть открытый и честный диалог о том, как будут использоваться устройства и как в действительности ИТ-отдел может удовлетворить такие потребности.

2. Выявите устройства с доступом к ресурсам предприятия

Представьте следующее. Вы начинает использовать решение MDM, предполагая, что компания поддерживает примерно 100 устройств. Имеется подробный список типов устройств и пользователей – все как обычно. Но, при первом просмотре отчетов оказывается, что используется более 200 устройств. Это реальный сценарий, никакого обмана. Такое происходит гораздо чаще, чем можно было бы подумать.

Не надо себя обманывать. Неизвестное может нанести вред. Перед окончательным принятием стратегии изучите текущую среду мобильных устройств. Для этого необходимо средство, которое поддерживает постоянную связь со средой электронной почты и определяет устройства, подключенные к сети предприятия. Помните, что после включения для почтового ящика ActiveSync для синхронизации можно использовать несколько устройств без уведомления ИТ-отдела.

В программу для мобильной среды необходимо включить все мобильные устройства. Владельцев этих устройств необходимо уведомить о вступлении в силу новых политик безопасности.

3. Используйте простую регистрацию

Сложность ведет к несоблюдению правил. После определения устройств для регистрации в программе для устройств пользователей следует использовать технологию, которая обеспечивает простой подход для регистрации пользователей. Это должен быть несложны и защищенный процесс с одновременной конфигурацией устройства.

В идеальном случае сотрудник должен перейти по ссылке в электронном сообщении или уведомлении на профиль MDM, созданный для устройства этого сотрудника, включая принятие условий соглашения о допустимом использовании (AUA).

Рассматривайте устройства пользователей как брак с соглашением AUA и как добрачный контракт, поддерживающий гармоничные взаимоотношения.

Чтобы помочь существующим пользователям зарегистрироваться в программе собственных устройств, используйте соответствующие инструкции. Рекомендуется удалить учетные записи ActiveSync существующих пользователей, чтобы на их устройствах можно было отделить данные предприятия и обеспечить управления этими данными. Для новых устройств следует создавать новые профили.

С точки зрения ИТ требуется возможность массовой регистрации существующих устройств или возможность для пользователей самостоятельно зарегистрировать свои устройства. Также необходима аутентификация сотрудников с использованием базового процесса, например, одноразовый пароль или с использованием существующих корпоративных директорий, например, Active Directory/LDAP. Любые новые устройства, с которых выполняется попытку доступа к ресурсам предприятия, должны помещаться в карантин с уведомлением ИТ-отдела. Такой подход позволяет ИТ-специалистам гибко блокировать устройства или запускать процесс их регистрации, если такой процесс утвержден, и обеспечивать соответствие действующим политикам предприятия.

4. Настраивайте устройства по беспроводной связи

Если имеется что-то, чего не может выполнить политика в отношении собственных устройств и решение MDM, число обращений в службу поддержки значительно увеличится. Для оптимизации эффективность ИТ-отдела и бизнес-пользователей настройку устройств следует выполнять по беспроводной связи.

После подтверждения пользователем условий AUA платформа должна предоставить сотруднику все необходимые профили, учетные данные и настройки для доступа к следующим службам:

- Электронная почта, контакты и календарь
- VPN и Wi-Fi
- Документы и информационные ресурсы предприятия
- Внутренние и общедоступные приложения

На данном этапе также разработайте политики по ограничению доступа к некоторыми приложениям и создайте предупреждения о превышении пользователем полномочий по использованию данных или о превышении лимита за месяц.

5. Помогите своим пользователям помочь самим себе

И вы сами себя поблагодарите. Пользователя нужны работающие устройства, а ИТ-специалистам требуется оптимизировать работу службы поддержки. Надежная платформа самообслуживания позволяет пользователям непосредственно выполнять следующие действия:

- Сброс забытого PIN-кода и пароля
- Определение местоположение потерянного устройства на веб-портале с использованием интегрированных картографических сервисов
- Полное удаление информации на устройстве, удаление важных данных предприятия Безопасность, защита данных

предприятия и обеспечение соответствия нормативным требованиям – общая ответственность. Возможно, для сотрудников это станет тягостной необходимость, но других возможностей для снижения риска без их сотрудничества не существует. Портал самообслуживания может помочь сотрудникам лучше понять, почему они не обеспечивается соответствие нормативным требования.

6. Соблюдайте конфиденциальность персональной информации

Разумеется, политика в отношении собственных устройств сотрудников – это не только защита данных предприятия, тщательно разработанная программа в отношении собственных устройств обеспечивает недоступность данных сотрудников для посторонних, включая ИТ-специалистов. Информация личного порядка (PII) может использоваться для идентификации, контактов или для определения местоположения сотрудника. Некоторые законы о неприкосновенности частной жизни запрещают организациям даже просмотр таких данных. Сообщите сотрудникам о политике защиты конфиденциальной информации и объясните, сбор каких данных с устройств сотрудников невозможен. Например, решение MDM должно поддерживать анализ информации, к которой разрешен или запрещен доступ, например:

- Персональная электронная почта, контакты и календарь
- Данные приложений и текстовые сообщения
- История звонков и голосовая почта

С другой стороны, сообщите пользователям, какая информация собирается, как она используется и почему это выгодно пользователям.

Улучшенное решение MDM позволяет использовать политику защиты конфиденциальной информации для настройки конфиденциальности, включая скрытие местоположения и информации о программном обеспечении, установленном на устройстве. Это помогает компаниям обеспечить соответствие нормативам PII и позволяет сотрудникам спокойно себя чувствовать, запрещая просмотр личной информации на смартфонах и шаблонах. Пример.

- Отключение отчетности по инвентаризации приложений скрывает от администраторов персональные приложения.
- Отключение служб определения местоположения для предотвращения доступа к указателям местоположения, например, физический адрес, географические координаты, IP-адрес и Wi-Fi SSID.
- Важными ключевыми словами являются прозрачность и понятность Если каждый знает правила, снижается общий уровень неприятия политики в отношении собственных устройств сотрудников.

7. Храните персональные данные отдельно от данных предприятия

Согласно соглашению по собственным устройствам сотрудников для ИТ-отделов и пользователей такие персональные данные, как фотографии с вечеринок или «История американского романа» отделяются от производственных приложений.

Проще говоря, ИТ-специалисты должны защитить корпоративные приложения, документы и другие материалы на случай ухода сотрудника из организации, а персональные сообщения электронной почты, приложения и фотографии остаются недоступными для ИТ-отдела предприятия.

Свободу такого подхода оценят не только пользователи, но также и ИТ-специалисты, жить которым станет значительно легче. Благодаря такому подходу ИТ-отделы могут выборочно удалять корпоративные данные с устройства уволившегося сотрудника. В зависимости от обстоятельств в случае потери сотрудником устройства можно выполнить его полную очистку. Эффективное решение MDM предоставляет такой выбор.

По оценкам около для 86% устройств выполняется выборочная очистка – удаляются только данные предприятия.

8. Управляйте использованием данных

Политика в отношении собственных устройств сотрудников в значительной степени освобождает ИТ-отделы от деятельности в сфере связи, но во многих компаниях по-прежнему требуется помогать сотрудникам управлять данными, чтобы избежать чрезмерных расходов.

Если организация платит за использование устройства, то ей необходимо контролировать это устройство. Если организации не платит за использование устройства, она может помочь пользователям следить за использованием данных. Необходимо отслеживать использование данных на устройствах в сетях и в роуминге и генерировать предупреждения при превышении лимита порога для объема используемых данных.

Пределы для объема данных в роуминге и в сетях можно задать в мегабитах, также можно указать дату выставления счета для рассылки уведомлений на основе использованного процента от допустимого объема данных. Рекомендуется рассказывать пользователям о преимуществах использования Wi-Fi (при наличии). Автоматическая конфигурация Wi-Fi обеспечивает автоматическое подключение устройств к Wi-Fi предприятия, если пользователь находится в сфере действия сети.

Если тарифный план включает 50 долларов США или 200 МБ данных в месяц, сотрудники положительно отнесутся к предупреждение о том, что дополнительный объем данных они будут оплачивать самостоятельно.

9. Постоянно контролируйте устройство на предмет несоответствия принятым требованиям

После регистрации устройства значение имеет только контекст. Рекомендуется постоянно контролировать определенные сценарии использования устройств и автоматическое применения политик. Пользователь пытается отключить средства управления? Устройство соответствует политике безопасности? Требуется ли корректировки на основе просматриваемых данных? Теперь можно приступить к рассмотрению дополнительных политик или правил. Вот несколько типичных вопросов:

- **Устройства с правами суперпользователя или с несанкционированным изменением микропрограммы:** Чтобы не платить за приложения, сотрудники иногда выполняют несанкционированное изменение микропрограммы или получают права суперпользователя телефона, открывая дверь для вредоносного ПО, способного похищать информацию. Если для устройства выполнено несанкционированное изменение микропрограммы, решение MDM должно выполнить определенные действия, например, выборочно удалить данные предприятия с устройства.
- **Не спешите с очисткой, отправьте SMS-сообщение:** Если программы, связанные с пустой тратой времени, например, Angry Birds, нарушают политики предприятия, хотя и не представляют никакой опасности, рекомендуется использовать автоматическую очистку. Решение MDM может применять политики на основе нарушений. MDM может отправить пользователю сообщение с указанием срока для удаления приложения, иначе будет выполнена очистка устройства.
- **Доступность новых операционных систем.** Чтобы поддерживать эффективность собственных устройств сотрудников, требуется простой способ уведомлений о готовности к установке новой ОС. В правильном решении MDM обновления ОС представляют собой функцию самообслуживания. Ограничение на использование предыдущих версий ОС помогает обеспечить соответствие нормативным требованиям и оптимизировать работу устройства.

10. Используйте прибыль на инвестированный в собственные устройства пользователей капитал

Хотя использование собственных устройств сотрудников перекладывает ответственность на приобретение устройств сотрудниками, стоит рассмотреть этот вопрос комплексно с учетом долгосрочных затрат организации.

При разработке политики рассмотрите вопрос влияния политики на повышение рентабельности. Используйте сравнение, как это показано далее:

Модель с устройствами, принадлежащими компании

- Во сколько обойдется каждое устройство
- Стоимость полностью оплачиваемого тарифа
- Стоимость утилизации устройств через каждые несколько лет
- Планы гарантийного обслуживания
- Время и объем работы ИТ-специалистов по управлению программой

Собственные устройства сотрудников

- Стоимость частично оплачиваемого тарифа
- Исключение стоимости приобретения устройства
- Стоимость платформы управления мобильной средой

Универсального решения не существует, но тщательно разработанная политика в отношении собственных устройств пользователей может указать направление, обеспечивающее эффективное управление мобильными устройствами.

Разумеется, увеличение производительности отмечается довольно часто, если сотрудники мобильны и постоянно подключены к ресурсам компании. Собственные устройства сотрудников – это отличный способ повысить производительность новых пользователей, для которых ранее было невозможно использовать устройства компании.

Собственные устройства сотрудников: безопасность свободы

Собственные средства сотрудников – это новые практические рекомендации по предоставлению сотрудникам возможности работать на собственных устройствах, что позволяет существенно снизить финансовую и административную нагрузку на ИТ-отделы. Но собственные устройства сотрудников не могут обеспечить упрощенное управление и экономию расходов без тщательно разработанной политики и надежной платформы управления.

Для тех, кто находится на ранних этапах реализации мобильной стратегии, решение IBM® MaaS360® предлагает массу образовательных ресурсов.

Если принято решение об использовании собственных устройств сотрудников, щелкните здесь, чтобы воспользоваться бесплатной пробной версией MaaS360 в течение 30 дней. Решение MaaS360 создано на основе облачной среды, поэтому среда тестирования автоматически превращается в рабочую среду без потерь данных.

О решении IBM MaaS360

IBM MaaS360 – это платформа управления мобильной средой предприятия, предоставляющая средства повышения производительности и защиты данных. Тысячи организаций рассматривают MaaS360 в качестве основы для своих мобильных инициатив. MaaS360 предоставляет инструменты комплексного управления с действенными средствами защиты пользователей, устройств, приложений и данных, обеспечивая поддержку развертывания любых мобильных сред. Чтобы получить дополнительную информацию и начать пользоваться пробной версией, посетите веб-сайт www.ibm.com/maas360

О подразделении IBM Security

Платформа обеспечения безопасности IBM предоставляет средства интеллектуального анализа безопасности и помогает организациям сформировать целостную защиту сотрудников, данных, приложений и инфраструктуры. Компания IBM предоставляет решения для управления идентификацией и доступом, управления информацией и событиями безопасности, защиты баз данных, разработки приложений, управления риском, управления конечными точками, защиты от вторжений и так далее. Компания IBM поддерживает работу одной из крупнейших в мире организаций, занимающихся исследованиями, разработкой и предоставлением решений по безопасности. За дополнительной информацией обращайтесь на веб-сайт по адресу www.ibm.com/security

IBM Восточная Европа/Азия
123317, Москва
Пресненская наб., 10
Тел.: +7 (495) 775-8800
Факс: + 7 (495) 258-6468, 258-6404
ibm.com/ru

Подготовлено в США.
Март 2016 г.

WGW03112-RURU-01