



мобильные устройства правят миром: пришло время MDM как услуги

С появлением все большего количества разнообразных мобильных устройств пришло время пересмотреть **стратегию управления мобильными устройствами** (Mobile Device Management, **MDM**). Это вовсе не новая вещь для ИТ, но мобильный ландшафт стремительно меняется, а политики безопасности остаются прежними.

В общем смысле, MDM — это набор политик и инструментов, которые контролируют мобильные устройства сотрудников и защищают корпоративные данные. Сегодня, когда **у каждого есть мобильные устройства**, появился спрос на новую стратегию MDM — такую, которая не только контролировала бы их, но и не ограничивала бы функционала.

Так что же заставляет компании пересматривать MDM? Сам факт того, что мобильных устройств стало больше. Понятие «мобильное устройство» сегодня включает в себя смартфоны, [планшеты](#), [фэблеты](#), [ультрабуки](#), носимые устройства и многое другое. Более двух третей респондентов [пользуются своими личными мобильными устройствами](#) на работе. Современная система MDM должна справляться и с этим.

больше устройств, больше данных, больше риска

Чем шире ваши сотрудники используют мобильные устройства, тем выше вероятность, что важная корпоративная информация случайно — или намеренно — попадет в чужие руки. Поэтому в обязательном порядке тщательно продумайте стратегию MDM. Крупные компании стремятся **разрабатывать и применять глобальную политику безопасности**, чтобы защитить свои данные от любых угроз. Но как это сделать, если количество гаджетов стремительно растет?

Совсем недавно главную опасность представляли черви, троянские кони и вирусы. Но вместе с мобильными устройствами появились новые проблемы. Угрозы ясны, но не вполне понятно, как с ними справляться. Сегодня в центре внимания специалистов по безопасности — кража телефонов и взлом каналов связи. Это чревато большими потерями, особенно если не соблюдаются должные меры предосторожности. Ведь можно защититься только от известных угроз — а за мобильными устройствами сложнее уследить, чем за атаками изнутри.

Самая главная проблема очевидна: сотрудники **работают с корпоративными данными на своих личных устройствах**, а потом — намеренно или нечаянно — выносят их за пределы локальной сети. Закрытых систем сегодня почти не осталось. Девять из десяти руководителей компаний [признались, что работают с корпоративными данными со своих телефонов](#). Что же можно с этим сделать?



все под контролем

Для начала осознайτε одну простую вещь: все мобильные устройства должны находиться под вашим контролем. ИТ-отдел должен помнить про все смартфоны, фаблеты, планшеты и ультрабуки сотрудников. Нельзя забывать даже про умные часы и очки Google Glass, хотя они еще не набрали популярность. Стратегия MDM должна быть **надежной, всеобъемлющей** и, главное, **современной**. И еще — она должна справляться с любым изменением и ростом мобильного ландшафта.

Развитие Интернета вещей (IoT) и усложнение коммуникаций M2M («устройство-устройство») тоже играют важную роль. С распространением Интернета вещей мобильных устройств станет еще больше — а вы помните, что их все нужно контролировать. Например, уже появились подключенные к интернету автомобили — а ведь это **новая разновидность рабочего места**, где также хранятся данные. И это далеко не единственный вестник перемен. Поэтому ваша система MDM должна уметь быстро реагировать на ситуацию. Иначе и быть не может. Ведь вы не хотите тратить на нее слишком много средств и при этом не готовы жертвовать безопасностью?

локальные или облачные решения?

Обычно стратегию MDM разрабатывают и реализуют локально, чтобы ИТ-отдел мог более полно ее контролировать. Но хорошая стратегия должна учитывать множество разных факторов. И сегодня, когда мобильных устройств вокруг становится все больше и больше, даже у лучших ИТ-отделов может просто не хватить сил. Что же все-таки можно сделать? В первую очередь, **зашифруйте** данные на всех устройствах — тогда, даже если они потеряются или будут украдены, **посторонним будет сложнее извлечь информацию**. Многие компании все чаще создают корпоративные магазины приложений, чтобы сотрудники не устанавливали ненадежные программы. Но чем больше появляется разных устройств с разными операционными системами, тем сложнее это реализовать.

Если ресурсов вашего ИТ-отдела не хватает, подумайте об облаках. Их преимущества для компаний хорошо известны. В сфере MDM облачные решения дешевле локальных как в установке, так и в использовании. Облачные системы MDM — или, как их все чаще называют, **MDM как услуга** — дают возможность использовать именно те функции, которые вам нужны. Мобильные устройства развиваются, и пользователи продолжают охотно покупать новинки, поэтому гибкая облачная система MDM кажется очень перспективным вариантом.

Гордон Макриллос (Gordon Makryllos)