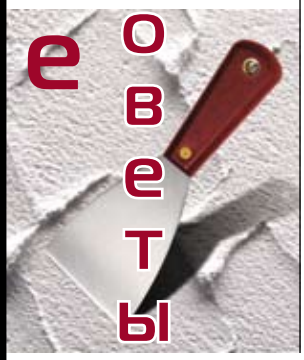
Полезные советы



Задача заказчика – отделить зерна от плевел

Доступ к служебной информации должен быть управляем и контролируем по различным критериям, а значит, мобилизация сводится к вопросам информационной безопасности, считает Руслан НИГМАТУЛИН, директор департамента по работе с корпоративными клиентами, «С-Терра СиЭсПи».

Руслан НИГМАТУЛИН

Что должно быть первым: выбор моделей корпоративных устройств, а потом разработка системы управления доступом (т.е. по сути, политики безопасности) или наоборот? На этот вопрос разные люди дадут разные ответы. Вполне очевидно, что ответит начальник отдела информационной безопасности. А что скажет директор по маркетингу? Или руководитель компании? Или высокопоставленный госчиновник?

Так какой же должна быть оптимальная стратегия мобилизации? Стихийной и беспощадной или планируемой и осторожной? Если мы говорим о крупном корпоративном секторе или о госорганах, то тщательное планирование – важнейшая составляющая. Ошибка может обойтись дорого.

Попробуем перечислить необходимые этапы планирования (без привязки к обязательному порядку, так как часто планирование происходит во взаимодействии разных отделов).

Итак, функциональность. Раз мы говорим о доступе к корпоративным ресурсам, то кроме Интернета понадобятся еще почта (в том числе с веб-интерфейсом), система электронного документооборота, специализированные программы и т. д.

Далее, информационная безопасность. Как контролировать потоки данных? Кому разрешить только почту, кому доступ к документации, кому доступ к системам управления? Разрешать ли хранить информацию на устройствах или обеспечить только доступ к ней? Как поступать в случае утери или кражи устройств? Нужны ли сертифицированные устройства и какого класса? Пожалуй, стоит отметить, что тема информационной безопасности как никакая другая требует классического подхода. Не занимайтесь самодеятельностью – начните с составления политики безопасности, модели угроз.

Цена и эксплуатационные характеристики. Это вещи взаимосвязанные. Кто будет поддерживать парк устройств, сам владелец или сторонний оператор? Во что обойдется вдруг потребовавшееся усовершенствование? Короче, речь о TCO (совокупная стоимость владения). При мысли о сокращении TCO идея BYOD становится довольно привлекательной. Но вспомним об информационной безопасности. В общем, надо думать.

В глобальном процессе мобилизации есть две стороны. Одна – заказчик, который в хорошем случае знает, что хочет, а в сложном случае – не очень. Другая, гораздо более активная – производители и интеграторы. Естественно, что они хотят заработать на своих разработках и услугах. При этом производители собственно мобильных устройств, разработчики мобильных приложений, операторы связи, интеграторы различного уровня компетенции могут предлагать комплексные решения в различных комбинациях. Заказчику предстоит решить классическую задачу – отделить зерна от плевел. И отказаться от ее решения нельзя. Ибо в эпоху жестокой конкуренции нельзя уступать сопернику в оружии ни на шаг. А мобильный, по сути тотальный, доступ к информации – оружие великой силы. ИКС