БЕЗОПАСНОСТЬ ПРИМЕНЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Е.А. ДОЦЕНКО

Самые современные технологии межсетевого экранирования, криптографическое программное обеспечение, современные методы разграничения доступа зачастую бессильны перед хищением данных сотрудниками компании, использующими мобильные устройства. В свою очередь, благонадежность сотрудников не решает другой проблемы — угроза утери информации вместе с ее носителем.

Наиболее вероятным инструментом хищения информации являются мобильные устройства, начиная от ноутбука и смартфона и заканчивая различными USB-накопителями. Напрашивается решение — обеспечить подключение только разрешенных мобильных устройств, не позволять вынос этих устройств за пределы периметра. Однако достаточность и оправданность данных мер можно поставить под вопрос. Опыт многих мировых компаний говорит о том, что тотальный контроль над сотрудниками наоборот подвергает активы предприятия повышенному риску осуществления угроз со стороны работников.

С утерей мобильных устройств в какой-то мере немного проще. С одной стороны достаточно применения только шифрования, с другой, данных мер недостаточно. Следует применять комплексный подход, начиная от криптографической защиты и заканчивая удаленным уничтожением данных.

Руководство организации должно четко понимать обозначенные проблемы. Разработка и поддержание грамотной политики безопасности поможет снизить риски до минимального значения. Регулярные тренинги персонала, проведение семинаров, различного рода стимулирование и наказание должны в совокупности обозначить позицию руководства по обеспечению информационной безопасности и не давать предпосылок для таких видов мотивации злонамеренных действий как корыстный интерес, месть из-за обиды и т.п.