ТОП-5: что должен знать заказчик при построении комплексной защиты корпоративной среды

В журнале "Информационная безопасность/Information Security" уже не раз поднималась тема построения комплексной защиты корпоративной среды, но сейчас она актуальна как никогда прежде. Редакция опросила четырех экспертов из разных компаний, на что же должен обратить внимание заказчик, которого волнует безопасность его предприятия.

Александр Веселов,
руководитель отдела технического консалтинга, "С-Терра СиЭсПи"

1. Комплексный подход. Фундамент любой системы – модель угроз и нарушителя. На их основе происходит выбор защитных мер с учетом экономической эффективности.

2. Проверенные контрагенты. Важно, чтобы поставщик и интегратор обладали хорошей репутацией, а их решения были проверены рынком. Они должны обладать необходимыми лицензиями, экспертизой, иметь в штате квалифицированных специалистов.

3. Стандартизация и интеграция. Использование стандартных протоколов и технологий позволяет добиться интеграции различных средств защиты друг с другом.

4. Соответствие требованиям регуляторов. Если в информационной системе обрабатывается информация, подлежащая обязательной защите в соответствии с законодательством, то необходимо использовать средства защиты, прошедшие сертификацию в ФСБ России и ФСТЭК России.

5. Непрерывный жизненный цикл. После внедрения системы защиты не стоит останавливаться на достигнутом, требуется постоянный мониторинг и аудит, тесты на проникновение, переоценка рисков, а при необходимости – доработка системы защиты. ●