УДК 004.02

ПОРЯДОК ОРГАНИЗАЦИИ ЗАЩИТЫ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ НА ПРЕДПРИЯТИИ

Кузьмин Н.А.,
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
Научный руководитель – преподаватель Кривоносова Н.В.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Любая утечка информации на предприятии может нанести серьезный ущерб компании от финансовых убытков до полной ликвидации предприятия. В связи с этим большую роль играет организация устойчивой и оптимальной защиты информации на предприятии. Поэтому многие руководители компаний все чаще задумываются о защите помещений для переговоров от утечки информации по техническим каналам. Данная работа будет посвящена организации защиты выделенного помещения на предприятии.

Итак, на сегодняшний день основными мероприятиями по организации защиты помещения являются:

- определение выделенного помещения для защиты (чаще всего таким помещением является переговорная);
- ограничения доступа в помещение;
- оценка защищенности помещения от утечек информации по техническим каналам связи;
- реализация пассивной защиты помещения путем инженерно-строительных конструкций;
- реализация активной защиты помещения путем установки специализированного оборудования, разрешенного ФСТЭК.

Мероприятия по защите во время проведения совещания:

- перед началом мероприятия необходимо провести осмотр помещения на наличие возможных прослушивающих устройств;
- не допускать посторонних людей в помещение во время проведения совещания;
- различные работы, осуществляемые в помещении вне времени проведения мероприятия, должны проводится в присутствии сотрудника безопасности.

Все применяемые средства должны быть сертифицированы. Реестр сертифицированных средств защиты информации можно найти на сайте ФСТЭК России.

Для обеспечения защиты от различных закладных устройств необходимо периодически проводить «чистку» помещения. Она должна проводится службой безопасности организации путем поиска возможных прослушивающих устройств с помощью специального оборудования.

Для возможности осуществления деятельности по технической защите конфиденциальной информации необходимо получить лицензию ФСТЭК.

Для того чтобы получить лицензию необходимо выполнить аттестацию и разработать документы по защищаемому помещению и системе обработки персональных данных.

Для осуществления данных услуг можно обратиться к лицензиатам ФСТЭК.

В эти услуги входят:

- проведение консультации (организация проводит встречу с клиентом, обсуждает с ним текущие и будущие затраты);
- помощь в аттестации (сотрудники организации проводят аттестацию помещений);
- рекомендации по покупке необходимого оборудования и программного обеспечения;
- обсуждение вопросов по аренде оборудования и помещения;

- консультация по оформлению сотрудников, работающих с конфиденциальной информацией.

Процесс лицензирования представляет собой:

- подачу заявления, составленного согласно требованиям постановления, No 79.;
- при верном оформлении заявления в течение пяти дней лицензирующий орган производит проверку всех документов;
- при нехватке необходимых документов лицензирующий орган отказывает в приеме заявления до устранения нарушения;
- после приема заявления, заявитель в течение 45 дней должен получить ответ от лицензирующего органа.

После успешного получения лицензии специалисты ФСТЭК буду периодически проводить плановые проверки на соблюдение требований.

Организация мер по защите предприятия от угроз информационной безопасности потребует некоторые расходы, такие как приобретение оборудования, затраты на получение лицензии ФСТЭК, подготовка помещения, услуги различных внешних специалистов по информационной безопасности. Также необходимо будет поддерживать систему безопасности на должном уровне. Однако размер затрат не так велик по сравнению с пользой, которую принесет хорошая система защиты информации.