УДК 004.02

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЙ

Раузер Д.К.
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»

В настоящее время в экономике активно развивается направление конкурентной разведки - деятельности по хищению коммерческой тайны. Даже для небольшой компании малого бизнеса необходима защита информационных активов, представляющих сведения о деятельности компании. Данная работа будет посвящена обзору мероприятий, посвященных защите выделенного помещения в компании.

Защита информации в любой компании начинается с определения уязвимостей и угроз. Классификация и уровень угроз безопасности информации зависят от расположения и архитектурно-строительных характеристик помещения, от вида представленной информации и от типов радио- и электроустройств в комнате. Поэтому, для определения угроз необходимы структурные и пространственные модели помещения.

Структурная модель описывает состав различных элементов комнаты: двери, окна, толщина стен и перекрытий, радио- и электронные устройства, телефонные и другие линии связи, кабели электропитания.

Пространственная же модель характеризует расположение помещения в коридоре, на этаже и ориентацию окон относительно внешних возможных мест расположения технических средств злоумышленника.

Для примера, прослушивание переговоров через дверь возможно с условием, если вход в комнату для конференций выполнен с нарушением определенных требований по звукоизоляции. Не следует также вести переговоры при открытых окнах, ибо в этом случае открыт непосредственный открытый доступ к акустической информации. Если стены, перегородочные конструкции, потолки и пол помещений для ведения конференций не проверяются на предмет звукоизоляции или не отвечают требованиям защиты, то они не считаются гарантированной защитой от прослушивания, а также, весьма опасными с позиции доступа к содержанию переговоров являются вентиляционные каналы. Они позволяют прослушивать акустическую информацию в комнате на значительном расстоянии. Поэтому к оборудованию вентиляционных каналов предъявляются особые требования.

В настоящее время для прослушивания разговоров широко распространено использование направленных микрофонов. При этом дистанция прослушивания в зависимости от реальной помехозащитной обстановки может достигать сотен метров. Для прослушивания злоумышленники применяют и проводные микрофоны. Чаще всего используются микрофоны со специально проложенными проводами для передачи информации, а также микрофоны с передачей информации по линии сети в 220 В. Не исключено использование для передачи прослушиваемой информации и других видов коммуникаций (например, проводов сигнализации).

К пассивным методам защиты акустической информации относится звукоизоляция и экранирование. Во время совещания неуместно понижение громкости человеческой речи, поэтому для защиты информации следует применять звукопоглощающие, звукоизоляционные и глушащие звук материалы и техники.

Единственное главное требование к данному методу - исключить добывание информации злоумышленниками за пределами помещения. Необходима звукоизоляция

оконных и дверных проемов, как и использование звукоизолирующих покрытий пола, стен и потолка.

Наиболее слабыми элементами помещений являются оконные и дверные проёмы. Они обладают существенно меньшими по сравнению с другими ограждающими конструкциями поверхностными плотностями материалов и трудно уплотняемыми зазорами и щелями. Стандартные двери и окна не удовлетворяют предъявленным требованиям по защите акустической информации в комнатах от прослушивания, поэтому их следует устанавливать с повышенной звукоизоляцией, путем применения дополнительных уплотняющих прокладок по периметру притвора дверей или окон. Применение уплотняющих прокладок повышает звукоизоляцию дверей на 5-10 дБ, что является ощутимым приростом.

К техническим методам относят различные устройства, такие как генераторы звуковой речеподобной помехи, генератор радиошума, устройства по выявлению диктофонов и закладных устройств.

Для предотвращения подслушивания с помощью закладных устройств необходимо проведение углубленной «очистки» помещения. Она должна проводится службой безопасности компании. После проведения процедуры помещение должно опечатываться и допуск в него должен быть ограничен, либо разрешен лишь в сопровождении сотрудника службы безопасности организации.

Таким образом, защита речевой информации от утечки по техническим каналам – одно из важных направлений в сфере информационной безопасности. Однако, это направление достаточно хорошо изучено, разработаны механизмы активной и пассивной защиты, созданы структуры, оказывающие услуги по организации защиты. В связи с изученностью становится больше и злоумышленников, поэтому на сегодняшний день практически всем компаниям нужно организовать защиту помещения для переговоров от утечки по техническим каналам.