ГБПОУ СПТ им. Б.Г.Музрукова

МДК.03.01. Технические методы и средства , технологии защиты информации
Раздел 5. Методическое обеспечение инженерно-технической защиты информации

Лекция 47

Нейтрализация угроз информации в кабинете руководителя организации

Разработчик: Столяров И.В.,
преподаватель ГБПОУ СПТ им. Б.Г.Музрукова

г. Саров
2017

3. Нейтрализация угроз информации в кабинете руководителя организации

3.1. Меры по предотвращению проникновения злоумышленника к источникам информации

Так как проникновение злоумышленника возможно через дверь в приемную, то в ночное время необходимо создать дополнительный рубеж и контролируемую зону в приемной Для этого на двери из коридора в приемную устанавливается магнитоконтактный извещатель типа СМК-3 или более современные ИО-104-2, 4. Датчик ИО-104-4 имеет меньшие габариты. Эти извещатели обеспечивают замыкание и размыкание контактов геркона при приближении магнита к герконе на расстояние не более 10 мм контакты и удалении более 45 мм.

Аналогичный извещатель устанавливается на дверях кабинета. Для обнаружения злоумышленника в кабинете необходимо установить объемный извещатель. В кабинете в принципе можно установить пассивный оптикоэлектронный, ультразвуковой, радиоволновый и комбинированный извещатели. Выбор производится по помехоустойчивости, объему кабинета и затрат на приобретение и эксплуатацию. В отличие от приемной, средства охраны которой в рабочее время отключаются, средства охраны кабинета при отсутствии на рабочем месте руководителя организации целесообразно сохранять во включенном состоянии. Для обеспечении такого режима необходимо использовать отдельный шлейф.

Учитывая небольшую площадь кабинета, целесообразно применять или пассивные оптико-электронные извещатели или активные волновые с регулируемой мощностью излучения. В качестве таких средств могут использоваться оптико-электронный извещатель «Фотон-5», создающий «занавес» с максимальной дальностью 12 м, ультразвуковой «Эхо-2» для площади 30 м^2, радиоволновой объемный «Волна-5» с регулируемой дальностью 2–16 м и комбинированный извещатель «Сокол-2», совмещающий пассивный инфракрасный и радиоволновой принципы обнаружения. Последний обеспечивает дальность действия: минимальную — 3–5 м, максимальную — 12 м. Он может крепиться к стене или на потолке, имеет высокую помехоустойчивость. Из сравнительного анализа указанных извещателей можно сделать вывод о том, что наиболее дешевым извещателем с приблизительно равными функциональными возможностями является оптико-электронный извещатель «Фотон-5». По критерию эффективность/стоимость лучшие показатели имеет комбинированный извещатель «Сокол-2».

Кроме рассмотренных средств целесообразно установить локальные извещатели для охраны сейфа и компьютера. Для охраны сейфа можно использовать охранный поверхностный емкостной извещатель «Пик» с регулируемой чувствительностью на приближение человека в интервале до 0,2 м.

Для защиты информации в компьютере от физического контакта его с злоумышленником и хищения информации путем копирования или изъятия винчестера качестве извещателя можно использовать также емкостной извещатель «Пик», антенна которого соединена с корпусом сейфа. Для механической защиты системный блок с винчестером может быть размещен в специальном сейфе под приставным столиком или использоваться съемный винчестер, помещаемый в сейф.

3.2. Защита информации в кабинете руководителя от наблюдения

Для защиты информации от наблюдения применяют методы энергетического скрытия путем увеличения затухания среды распространения. Для прекращения функционирования оптического канала утечки информации «окно кабинета — окно противоположного жилого дома» можно применить следующие меры:

- шторы на окна;
- жалюзи;
- тонированные пленки на стеклах.

Шторы — традиционные средства для предотвращения скрытного наблюдения через окна кабинета, но они существенно ухудшают естественную освещенность кабинета и накапливают пыль.

Тонированные пленки на стеклах исключают возможность наблюдения за объектами защиты в кабинете, незначительно уменьшают освещенность кабинета, но позволяют легко выявить окна помещений с повышенными требованиями к безопасности информации, что из-за соображений скрытности защиты делать не следует. Для обеспечения скрытности защиты применять пленку надо на всех окнах, по крайней мере, этажа, а лучше здания.

Наиболее приемлемый вариант защиты — применение жалюзи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению — защите от солнечных лучей.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

Меры по обнаружению и локализации скрытно установленной в кабинете телевизионной камеры проводятся периодически и перед проведением совещания. Исключить установку камеры между проверками нельзя. Телевизионное изображение может передаваться в реальном масштабе времени или записываться на пленочный или цифровой видеомагнитофон с последующей ускоренной передачей. Однако, учитывая, что кинематический видеомагнитофон имеет большие, чем телевизионная камера, размеры и энергопотребление, его практическое применение в настоящее время ограничено. В будущем следует ожидать появление бескинематических цифровых видеомагнитофонов для скрытой записи. Основным демаскирующим признаком телевизионной камеры и видеомагнитофона является радиоизлучение. Поэтому для обнаружения и локализации телевизионной камеры применяются средства поиска радиоизлучающих закладных устройств: индикаторы поля, специальные радиоприемники, автоматизированные комплексы для радиомониторинга и др. Перед совещанием во время «чистки» кабинета применяются также нелинейные локаторы и металлодетекторы.

3.3. Меры по защите речевой информации от подслушивания

1. Для защиты от подслушивания речевой информации в приемной необходимо существенно повысить звукоизоляцию дверей как наиболее слабого звена в акустической защите и стены до, по крайней мере, до 55 дБ на частоте 1000 Гц. Такая звукоизоляция обеспечивается двойной дверью с тамбуром шириной не менее 20 см с уплотнителями по периметру дверных полотен. Для предотвращения утечки информации через ограждения кабинета возможны 3 варианта:

- повышение поверхностной плотности ограждения;
- установление дополнительной перегородки;
- зашумление ограждения.

Так как звукоизоляция пропорциональна поверхностной плотности среды распространения акустической волны, то при недостаточной звукоизоляции утолщают стены. Наиболее удобным строительным материалом для этого является кирпич, который укладывают на ширину половины или длины целого кирпича вплотную к стенке.

Возможно также укрепление на стене строительных материалов (многослойной фанеры различной толщины, стеклопластика, пемзобетонных плит и др.).

Утолщенная стена из красного кирпича обеспечивает повышение звукоизоляции с 48 дБ до 53 дБ. Кладка утолщенной стены с зазором между стенками 40 мм увеличивает звукоизоляцию еще приблизительно на 4–5 дБ. Утолщение стены целесообразно проводить со стороны приемной, так как это позволит уменьшить выступ двойной двери с тамбуром в приемную.

Звукоизоляция стен между кабинетом и приемной, кабинетом и коридором, кабинетом и смежным помещением повышается путем утолщения стен и крепления к ним дополнительных перегородок. Утолщение стен производится путем кирпичной кладки у стены кабинета. В качестве дополнительных перегородок используются асбестоцементные, гипсокартонные, древесностружечные, древесноволокнистые плиты толщиной 10–20 мм. Они крепятся к стене с помощью деревянных реек и брусков толщиной 40–50 мм по периметру и поверхности стены. По периметру между перегородкой и другими ограждениями устанавливаются упругие (из губчатой резины) прокладки. Между перегородкой и стеной может быть размещен звукопоглощающий пористый материал.

В качестве меры, повышающей энергетическое скрытие речевой информации в кабинете, на стенах могут быть укреплены виброакустические излучатели акустических генераторов помех.

Для исключения утечки информации через батареи и трубы отопления перед батареями устанавливают резонаторные экраны в виде деревянных перегородок с отверстиями.

Для предотвращения утечки информации через вентиляционное отверстие пред ним укрепляют экран и (или) размещают в нем глушитель звука.

С учетом рассмотренного в качестве мер предотвращения подслушивания рекомендуется:

- установка двойной двери с уплотнительными прокладками и тамбуром глубиной 30 см;
- увеличение толщины стены между кабинетом и приемной, а также соседними помещениями на 0,5 кирпича;
- установка на батареи отопления резонаторных экранов или излучателей генератора виброакустического защумления;

- закрытие окна плотными шторами, установка на стекла окон излучателей генератора виброакустического зашумления (для предотвращения лазерного подслушивания при закрытых окнах);
- установка перед воздухозаборниками воздухопроводов акустических экранов;
- установка датчиков комплекса обнаружения скрытно работающего диктофона PDTR-18 под столешницу стола руководителя возле стула для посетителя и стола заседания;
- применение устройств для подавления сигналов скрытно работающего диктофона.

Установка двойной двери повышает звукоизоляцию с 18 дБ до 48 дБ, утолщение стены увеличивает звукоизоляцию примерно на 20 дБ.

3.4. Предотвращеиие перехвата радио- и электрических сигналов

Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается:

- выключением во время разговора всех радиосредств и электрических приборов, без которых можно обойтись;
- установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания;
- установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд» и «Гранит-VIII» — ограничителей малых амплитуд с фильтрами от ВЧ-навязывания;

- установкой НЧ-фильтров в цепь вторичных часов единого времени (устройство МП-4);
- установкой буфера в цепь громкоговорителя системы оповещения (устройство МП-5);
- использованием в кабинете генератора пространственного электромагнитного зашумления кабинета, включаемого во время проведения совещения с по тематике, содержащей тайну;
- установкой в свободный слот системной платы компьютера платы генератора помех.

Кроме того, информация на компьютере в кабинете руководителя организации может защищаться путем:

- использования защищенных ПЭВМ;
- размещения системного блока в специальном сейфе;
- установкой винчестера в съемный кожух и хранение его в сейфе;
- программной защиты доступа к компьютеру и отдельным папкам;
- криптографическим шифрованием информации, хранящейся на машинных носителях.

Кроме того, после проведения капитального ремонта и перед проведением совещания производится чистка помещения с целью обнаружения закладных устройств.