**Практическая работа №2**

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Москва 2024.

**Цель работы:** получить практические навыки по созданию сценария инженерно-технической защиты информации в кабинете руководителя организации.

**1. Теоретическая часть**

**Сценарий инженерно-технической защиты информации в кабинете руководителя организации**

Сценарий предназначен для формирования на практических занятиях навыков по обеспечению защиты информации в кабинете руководителя организации. Рассматриваются все основные этапы и процедуры защиты информации:

* описание кабинета руководителя как наиболее сложного объекта защиты;
* описание угроз информации в кабинете руководителя организации;
* выбор рациональных мер по защите информации в кабинете руководителя организации.

 **I. Описание кабинета руководителя организации как наиболее сложного объекта защиты**

1. Выбор кабинета как объекта защиты обусловлен следующими факторами:

* в кабинете руководителя циркулирует наиболее ценная информация организации;
* кабинет посещают сотрудники организации всех должностных категорий по служебным и личным вопросам, а также посетители организации;
* в кабинете, как правило, размещаются различные радио- и электрические приборы, которые могут быть источниками побочных электромагнитных излучений и наводок;
* в кабинете во время докладов и совещаний проводится демонстрация продукции, документов, плакатов, аудио- и видеоматериалов;
* в кабинете много элементов интерьера и мебели, в которой легко спрятать закладные устройства.

Кабинет руководителя, как правило, граничит с приемной и другими служебными помещениями. В приемной возможно длительное присутствие посторонних лиц (сотрудников и посетителей), ожидающих приема. В результате недостаточной защиты информации в кабинете (например из-за слабой звукоизоляции стены), относительно частого открывания двери в кабинет, продолжения в приемной разговора на служебные темы выходящих из кабинета людей, работа секретаря с документами в присутствии находящихся в приемной людей могут создать реальные предпосылки для утечки информации из приемной.

Во время совещания с участием представителей других организаций или беседы руководителя с посетителями последние могут попытаться записать конфиденциальный разговор с помощью скрытой записи на диктофон или закладного устройства с целью последующего использования этой информации во вред руководителю организации или организации в целом.

Здание, в котором находится кабинет, как правило, окружено другими административными и жилыми домами, через окна или с крыши которых возможно наблюдение за источниками информации в кабинете, а также возможен перехват из кабинета радиосигналов закладных устройств и побочных электромагнитных излучений и наводок.

Следовательно, кабинет представляет собой объект защиты, в котором, с одной стороны, циркулирует наиболее ценная информация, а с другой стороны, возможен доступ в него всех категорий сотрудников и посетителей, в том числе тех, которые могут заниматься добыванием информации.

2. Характеристика информации, защищаемой в кабинете руководителя

## Виды информации в кабинете руководителя

В кабинете руководителя на различных носителях могут находиться почти все виды защищаемой в организации информации, в том числе:

* семантическая информация в документах, с которыми работает руководитель или которые приносят его заместители, другие сотрудники, представители других организаций, а также на чертежах и плакатах, развешиваемых на стенах или проецируемых во время докладов или совещаний;
* семантическая информация во время конфиденциального разговора руководителя с посетителями и выступлений участников совещания;
* информация о видовых признаках VIP-персон, посещающих руководителя и по характеру деятельности которых можно определить тематику обсуждаемых вопросов;
* видовые демаскирующие признаки продукции, макетов и опытных образцов, которые демонстрируются руководителю на разных этапах их производства, а также их изображения на плакатах, экранах видеопроектора или телевизора;
* демаскирующие признаки веществ, приносимых руководителю для демонстрации соответствующей продукции, а также образцы исходных материалов.

Таким образом, основными видами информации в кабинете руководителя являются: речевая информация, семантическая, информация на плакатах, экране видеопроектора, информация о видовых демаскирующих признаках продукции.

## Источники информации в кабинете руководителя

Основными источниками информации в кабинете руководителя являются:

* руководитель организации;
* должностные лица организации, посещающие кабинет;
* представители других организаций, с которыми руководитель обменивается секретной (конфиденциальной) информацией в ходе встреч или совещаний;
* посетители во время приема по личным вопросам, разговор с которыми может содержать сведения, содержащие коммерческую или иную тайну;
* документы на столах, плакаты на стенах, аудио- и видеодокументы;
* приносимая в кабинет продукция, сведения о которой и ее демаскирующие признаки содержат государственную, коммерческую или иную тайну;
* приносимые в кабинет материалы и продукция в виде веществ, информация о составе и технологии изготовления которых защищается.

Характеристика информации и ее источников дана в табл. 2.

Продукция, сигналы которой содержат защищаемые сигнальные признаки, во время ее демонстрации в кабинете не включается во избежание утечки информации. Поэтому информация о сигнальных демаскирующих признаках разрабатываемой продукции в сценарии не рассматривается.

При определении цены защищаемой в кабинете руководителя информации используется шкала с 5 градациями: очень высокая, высокая, средняя, низкая, очень низкая. Для понимания значений шкалы уточним граничные значения:

* очень высокая – цена информации, утечка которой может нанести государству очень большой ущерб или привести к банкротству фирмы;
* очень низкая – цена информации, потеря которой не имеет последствий.

С учетом этого остальные значения цены информации обозначают следующее:

* высокая – цена информации, утечка которой может нанести государству большой ущерб или заметно ухудшить финансовое состояние фирмы;
* средняя – цена информации, потеря которой может привести к существенным для государства и фирмы финансово-экономическим потерям, но может компенсироваться внутренними резервами фирмы;
* низкая – цена информации, утечка которой приводит к малым потерям.

Виды информации в кабинете и соответствующие им значения цены указаны в табл. 2.

Таблица 2 Характеристика информации и ее источников

|  |  |  |  |
| --- | --- | --- | --- |
| Вид информации в кабинете  | Источник информации  | Максимальная цена информации  | Место нахождения информации в кабинете  |
| Семантическая документальная  | Документы  | Очень высокая  | В сейфе, на столах, стене, плакатах, доске, экране монитора или видеопроектора  |
| Семантическая речевая акустическая  | Люди  | Очень высокая  | В кабинете  |
| Семантическая речевая, читаемая по губам  | Люди  | Средняя  |  |
| Видовые признаки  | Продукция  | Средняя  | На столе, стене, плакатах, доске, экране монитора или видеопроектора  |
| То же  | Люди  |  | В кабинете  |
| »  | Вещества и материалы  | Очень низкая  | На столах  |
| Вещественные признаки  | Продукция химического производства  |  | На столах  |
| Продукция других производств  |  Низкая  | На столах  |
| То же  | Материалы  | Очень низкая  | На столах  |

Для государственных структур признаком цены информации может служить ее гриф секретности: «чрезвычайной важности» – чрезвычайно высокая, «совершенно секретно» – очень высокая, «секретно» – высокая, для «служебного пользования» – низкая.

Наибольшую цену имеет семантическая документальная информация. Цена информации о видовых или вещественных признаках зависит от их информативности. На предприятиях химической и смежных сфер промышленности цена информации о вещественных признаках продукции может быть высокой, т. к. состав веществ и технология их изготовления для этих предприятий является основной государственной или коммерческой тайной. Для машиностроительных предприятий цена такой информации низкая. Но могут быть исключения, например, если существенное улучшение параметров продукции достигнуто за счет применения новых материалов.

При формировании табл. 2 очень важно указать все места нахождения источников информации в кабинете, т. к. они могут существенно влиять на величину угрозы канала утечки. Например, если документ находится на столе, то возможности его наблюдения через окно весьма ограничены; если он в виде плаката повешен на стену напротив окна, то риск наблюдения резко возрастает.

**II. Описание угроз информации в кабинете руководителя организации**

Информация в кабинете подвергается угрозам воздействия и утечки. Эти потенциальные угрозы существуют всегда, но возможность их резко возрастает, когда злоумышленник пытается проникнуть в организацию или вербует сотрудника, возникает очаг пожара или проявляются достаточно информативные признаки технических каналов утечки информации.

1. Описание угроз воздействия на источники информации

При описании угроз воздействия прогнозируются маршруты движения злоумышленника из нулевого состояния вне территории организации к источникам информации в кабинете руководителя, оцениваются параметры (вероятность и время реализации) участков маршрутов (дуг семантической сети). По ним оценивается ущерб и ранг угроз.

Способы проникновения злоумышленника в кабинет руководителя зависят от «квалификации» злоумышленника, модели объектов защиты и времени проникновения.

В данном сценарии рассматривается вариант проникновения «квалифицированного» злоумышленника, который имеет в организации сообщника без специальной подготовки.

Время проникновения целесообразно разделить на рабочее и нерабочее время организации. Рабочее время характеризуется следующими условиями: пропуск людей и автотранспорта производится через контрольно-пропускной пункт (КПП) по пропускам, извещатели технических средств охраны на территории и в здании выключаются, входная дверь в административное здание, в котором размещается кабинет руководителя, открывается для свободного прохода.

В рабочее время несанкционированное проникновение в организацию возможно через КПП по фальшивым документам и через забор. Хотя второй способ проникновения в рабочее время маловероятен, полностью исключить его нельзя. В рабочее время проникнуть в кабинет может как «чужой» злоумышленник, так и сотрудник организации. Очевидно, что сотруднику сделать это проще. Проникновение возможно при открытых и закрытых дверях кабинета и приемной, но наиболее легкий вариант для злоумышленника – обе двери открыты. Такой вариант в принципе возможен, когда руководитель уходит или выходит из кабинета, а секретарь выходит из приемной, не закрыв оба кабинета. Более частый вариант – дверь кабинета закрыта, а в приемную – открыта.

Во внерабочее время проникновение злоумышленника в организацию возможно через забор, а также через окно и дверь здания, примыкающего к тротуару.

Если злоумышленник имеет предварительную информацию о расположении и типах средств охраны и видеоконтроля, он может попытаться проникнуть в кабинет во внерабочее время путем скрытого преодоления в ночное время рубежей и зон безопасности или спрятавшись в конце рабочего дня в одном из незакрываемых помещений организации. Возможные варианты проникновения злоумышленника в кабинет представлены в виде семантической цепи на рис. 2.



Рис. 2. Семантическая цепь представления вариантов проникновения злоумышленника в кабинет руководителя с градацией вероятностей перехода:

ом – очень малая; м – малая; с – средняя; в – высокая; ов – очень высокая

2. Описание технических каналов утечки информации

Описание выявленных технических каналов утечки информации предполагает определение показателей их угроз.

## Описание оптических каналов утечки информации

Возможны следующие оптические каналы утечки информации из кабинета руководителя:

* объект наблюдения в кабинете – окно кабинета – окно

противоположного дома – оптический прибор злоумышленника;

* объект наблюдения в кабинете – приоткрытая дверь – злоумышленник;
* объект наблюдения в кабинете – телевизионное закладное устройство – проводной или радиоканал – телевизионный приемник злоумышленника.

Вероятность обнаружения объектов наблюдения в кабинете и их распознавания зависит от количества и информативности видовых демаскирующих признаков. Эти признаки получают из изображения объекта наблюдения на сетчатке глаза, фотоснимке, фоточувствительной поверхности оптического приемника. Количество признаков зависит от:

* разрешающей способности оптического приемника; - масштаба изображения относительно реального объекта.

Минимальные размеры элемента изображения объекта наблюдения в виде точки на светочувствительном элементе, определяются как , где *D* – дальность от светоприемника до объекта наблюдения; *f* – фокусное расстояние объектива оптического приемника.

В качестве технического средства наблюдения за объектами в кабинете через его окна рассматривается фотоаппарат ФС-122 («Фотоснайпер») с объективом Таир-30, фокусное расстояние которого равно 300 мм, а разрешающая способность объектива 50 лин/мм. Такой фотоаппарат размещается в удобном для скрытого переноса портфеле типа «кейс». При использовании фотопленки с разрешающей способностью = 100 лин/мм 

разрешение фотоаппарата (объектив – пленка) *R* = 33 лин/мм. Для *D*=50 м размеры элемента объекта, отображаемого на светочувствительном элементе в виде точки-пикселя, соответствуют 10 мм. Минимальные линейные

размеры объекта, который можно распознать с вероятностью 0,9, составляют 5–6 см. Такие минимальные размеры могут иметь буквы и цифры на плакатах, иллюстрирующих выступления докладчиков на ответственных совещаниях.

При полученных значениях разрешения могут быть также распознаны лица людей и внешний вид достаточно крупной продукции. Однако прочитать документ формата А4, рассмотреть изображение на экране компьютера и телевизора, прочитать произносимые слова по губам нельзя. Следовательно, риск рассмотренного оптического канала утечки информации, содержащейся в изображении плакатов, людей и крупногабаритной продукции, велик, а утечки информации, содержащейся в изображениях документов формата А4, очень мал.

Другой оптический канал утечки информации может возникнуть при приоткрытой двери кабинета или заглядывании в кабинет посторонних лиц. В этом случае могут быть прочитаны тексты не только на плакатах, но и на столах и экранах светопроектора и телевизора. Но при наличии бдительного секретаря в приемной возможностью такого наблюдения очень мала.

Наконец, возможность реализации угрозы наблюдения с помощью видео закладного устройства также мала, т. к. установка телевизионной камеры в кабинете – серьезная разведывательная операция. Однако пренебрегать такой возможностью нельзя.

На основании перечисленных данных риск утечки информации при наблюдении можно оценить следующим образом:

* очень высокий – семантической документальной информации, отображаемой на плакатах;
* очень малый – остальной документальной информации;
* средний – о видовых признаках людей;
* малый – о видовых признаках продукции;
* очень малый – о видовых признаках веществ и материалов.

## Описание акустических каналов утечки информации

Утечка речевой информации возможна по следующим акустическим техническим каналам:

* источник речевого сигнала – стена в соседнее помещение – акустический приемник злоумышленника;
* источник речевого сигнала – приоткрытая дверь в приемную – акустический приемник;
* источник речевого сигнала – закладное устройство – радиоканал – радиоприемник злоумышленника;
* источник речевого сигнала – стекло окна – модулированный лазерный луч – фотоприемник лазерной системы подслушивания;
* источник речевого сигнала – воздухопровод – акустический приемник;
* источник речевого сигнала – случайный акустоэлектрический преобразователь в техническом средстве – побочное излучение технического средства – радиоприемник;
* источник речевого сигнала – случайный акустоэлектрический преобразователь в техническом средстве – проводные кабели, выходящие за пределы контролируемой зоны;
* источник речевого сигнала – воздушная среда помещения – диктофон у злоумышленника.

Для оценки угроз речевой информации необходимо оценить уровень акустического сигнала в возможных местах размещения акустического приемника злоумышленника. Такими местами являются: - приемная;

* коридор;
* смежные с кабинетом помещения;
* помещения с трубами отопления, проходящими через кабинет;
* помещения, акустически связанные с кабинетом через воздуховоды вентиляции.

Кроме того, речевая информация в кабинете может ретранслироваться по радиоканалу или проводам телефонной линии и электропитания закладными устройствами и побочными электромагнитными излучениями основных и вспомогательных технических средств и систем, а также средствами лазерного подслушивания. Так как носителями информации при ретрансляции являются электромагнитная волна в радиодиапазоне и электрический ток, то угрозы и меры по предотвращению перехвата рассматриваются в радиоэлектронном канале утечки информации. Также акустическая информация может быть получена с помощью лазерного средства подслушивания, установленного в помещении противоположного дома. Характеристика акустических каналов утечки информации дана в табл. 3.

Таблица 3 Характеристика акустических каналов утечки информации

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Характеристика речи  | Гром-кость, дБ  | Основной элемент среды распространения, дБ  | Величина звукоизоляции, дБ  | Место нахождения акустического приемника  | Уровень шума, дБ  |
| Спокойный разговор  | 50–60  | Стена и дверь в приемную  | 27  | Приемная  | ≈30  |
| Громкая речь  | 60–70  | Стена в коридор  | 51  | 35–40  |
| Шумное совещание  | 70–80  | Стена в смежную комнату  | 40  | помещение  |
| То же  | 70–80  | Межэтажное перекрытие  | 50  |  |
| »  | 70–80  | Вентиляционный короб  | 0,2 дБ/м 3–7 дБ на изгиб  |  | 30  |
| »  | 70–80  | Трубы отопления  | 25–35  | На трубе отопления  | 30  |

В качестве критерия защищенности речевой информации используется отношение сигнал/шум, при котором качество подслушиваемой речевой информации ниже допустимого уровня. В соответствии с существующими нормами понимание речи невозможно, если отношение помеха/сигнал равно 6–8, а акустический сигнал не воспринимается человеком как речевой, если отношение помеха/сигнал превышает 8–10. Следовательно, для гарантированной защищенности речевой информации отношение сигнал/шум 10 дБ. Оценка угрозы утечки информации по при подслушивании человеком производится по . При применении технического акустического величины повышается на 6 дБ.

Уровни громкости речевой информации в возможных местах размещения акустического приемника злоумышленника при громкости источника 70 дБ.

Таблица 4 Уровни громкости речевой информации

|  |  |  |
| --- | --- | --- |
| Место размещения акустического приемника злоумышленника  | Уровень громкости, дБ  | Оценка риска подслушивания  |
| Приемная  | 5–10  | Очень высокий  |
| Коридор  | –15– (–20)  | Отсутствует  |
| Соседнее помещение  | ≈(–5)  | Низкий  |
| Верхнее (нижнее) помещение  | –15– (–10)  | Отсутствует  |
| Вентиляционный короб  | 0–5  | Средний  |
| Трубы отопления  | 0–5  | Средний  |

Как следует из данных табл. 4, наибольшую угрозу создает канал утечки, приемник которого расположен в приемной и в коробе вентиляции. Каналом утечки, приемник которого расположен в коридоре, можно пренебречь.

## Моделирование радиоэлектронных каналов утечки информации

Радиоэлектронные каналы утечки информации из кабинета руководителя представляют собой простые каналы и части составных акусто- радиоэлектронных каналов утечки информации. Простые каналы образованы побочными электромагнитными излучениями и наводками радиосредств и электрических приборов, размещенных в кабинете, в том числе:

* компьютера при обработке на нем закрытой информации;
* видеодвойки (в случае просмотра видеокассет с закрытой информацией).

Кроме того, опасные сигналы случайных акустоэлектрических преобразователей в радиосредствах и электрических приборах могут добавить к простым оптическим и акустическим каналам радиоэлектронные каналы утечки информации и создать акустоэлектронные каналы утечки. Источниками радиоэлектронных каналов утечки в составе акустоэлектронных составных являются:

* коммутационное оборудование и кабели внутренней АТС;
* электрические приборы в кабинете (вторичные часы единого времени, вентилятор, громкоговоритель оперативного оповещения);
* передатчики акустических и телевизионных закладных устройств.

Если в кабинете установлено телевизионное закладное устройство, например, в типовых папках (скоросшивателях) с отверстием в торце, то составной оптико-электронный канал утечки информации содержит радиоэлектронный канал утечки информации с элементами: телевизионная камера – телевизионный приемник – видеомагнитофон или злоумышленникнаблюдатель.

Побочные НЧ- и ВЧ-излучения основных технических средств и систем (ОТСС) имеют очень широкий диапазон частот: доли герцев – тысячи мегагерцев (длины волн: сотни метров – десятки сантиметров). Помещение кабинета с учетом его размеров, представляет собой ближнюю, переходную и дальнюю зоны побочного излучения ОТСС. На частотах до 30 МГц помещение образует ближнюю зону. В зависимости от вида излучателя в ближайшей зоне может преобладать электрическое или магнитное поле.

Информация в помещении находится в безопасности, если уровни ее носителей в виде электрических сигналов и напряженности поля не превышают нормативы. Следовательно, для предотвращения подслушивания путем перехвата опасных сигналов необходимо определить эти уровни на границе контролируемой зоны (периметра кабинета) и в случае недопустимо больших значений определить рациональные меры по их уменьшению.

Уменьшение затухания электромагнитной волны в железобетонных стенах с повышением ее частоты вызвано снижением экранирующего эффекта металлической арматуры железобетона. На частоте 1 ГГц длина волны равна 30 см, что соизмеримо с размерами ячеек арматуры.

При ослаблении электромагнитной волны стенами здания на 20 дБ дальность ее распространения уменьшается на 1 порядок. Учитывая, что окна кабинета выходят на улицу, риск перехвата радиоизлучений ПЭВМ из кабинета руководителя организации можно оценить значением «средний», а электрических сигналов акустоэлектрических преобразований – «низкий».

Таким образом, наибольший ущерб информации, содержащейся в кабинете руководителя, могут нанести следующие угрозы:

* наблюдение из окна противоположного дома текста и изображений на плакатах экрана, укрепленных на стенах кабинета;
* подслушивание разговора в кабинете через приоткрытую дверь в приемную руководителя;
* подслушивание громкого разговора через стену, разделяющую кабинет и коридор;
* наблюдение через окно противоположного дома за участниками совещания;
* наблюдение через открытую дверь за участниками совещания;
* перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора;
* перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, трансляции, часов единого времени, электропитания и заземления;
* подслушивание с помощью стетоскопа речевой информации

акустических сигналов, распространяющихся по трубам отопления;

* подслушивание речевой информации акустических сигналов, распространяющихся по воздухопроводам;
* подслушивание с помощью акустических закладных устройств, установленных в кабинете;
* скрытое наблюдение с помощью предварительно установленных телевизионных камер;
* скрытное проникновение к источникам информации, хранящимся в ящиках стола, компьютере, сейфе.

**III. Нейтрализация угроз информации в кабинете руководителя организации**

## Меры по предотвращению доступа 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. Эти извещатели обеспечивают замыкание или размыкание контактов геркона при приближении магнита на расстояние не более 10 мм и удалении не более 45 мм. Аналогичный извещатель устанавливается на дверях кабинета.

Для обнаружения злоумышленника в кабинете необходимо установить объемный извещатель (пассивный оптико-электронный, ультразвуковой, радиоволновой, комбинированный). Выбор производится исходя из помехоустойчивости, объема 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 обеспечения 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 следующие извещатели: оптико-электронный «Фотон-5», создающий «занавес» с максимальной дальностью 12 м; ультразвуковой «Эхо-2» для площади 30 м2; радиоволновой объемный «Волна-5» с регулируемой дальностью 2–16 м и комбинированный «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. Наиболее доступным извещателем с требуемыми 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 емкостный извещатель «Пик» с регулируемой чувствительностью на приближение человека на расстояние до

0,2 м.

Для защиты информации, содержащейся в компьютере, от действий злоумышленника (хищения информации путем копирования или изъятия винчестера) можно использовать емкостный 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 может использоваться съемный винчестер, помещаемый в сейф.

## 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 средства:

* шторы на окнах;
* жалюзи;
* тонированные пленки на стеклах.

Шторы – традиционное средство для предотвращения скрытого наблюдения через окно 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 не рекомендуется использовать. Для обеспечения скрытости 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 предпринимаются 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 кинематический видеомагнитофон имеет большие, чем телевизионная камера размеры и энергопотребление, поэтому 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 излучение. Поэтому для обнаружения и локализации телевизионной камеры применяются средства поиска радиоизлучающих зарядных устройств: индикаторы поля, специальные радиоприемники, автоматизированные комплексы для радиомониторинга и др. Перед совещанием во время «чистки» кабинета применяются также нелинейные локаторы и металлодетекторы.

## Меры по защите речевой информации от подслушивания

Для защиты от подслушивания речевой информации в приемной необходимо существенно повысить звукоизоляцию дверей и стен 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. Звукоизоляция стен между кабинетом и приемной, кабинетом и коридором, кабинетом и смежным помещением повышается путем утолщения стен и крепления к ним дополнительных перегородок. Наиболее удобным строительным материалом для этого является кирпич, который укладывают на ширину половины или длины целого кирпича вплотную к стенке. Утолщенная стена из качественного кирпича обеспечивает повышение звукоизоляции с 48 до 53 дБ. Кладка утолщенной стены с зазором между стенками 40 мм увеличивает звукоизоляцию еще примерно на 4–5 дБ. Утолщение стены целесообразно проводить со стороны приемной, так как это позволит уменьшить выступ двойной двери с тамбуром в приемную.

Возможно также укрепление на стене строительных материалов (многослойной фанеры различной толщины, стеклопластика, пемзобетонных плит и др.). 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 перед ним укрепляют экран и (или) размещают глушитель звука.

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 половину длины кирпича;
* установка на батареи отопления резонаторных экранов или излучателей генератора виброакустического зашумления;
* закрытие окон 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 скрыто работающего диктофона PDRT-18 под столешницу стола руководителя возле стула для посетителя и стола заседаний;
* применение устройств для подавления сигналов скрыто работающего диктофона.

*Примечание*. Установка двойной двери повышает звукоизоляцию с 18 до

48 дБ, утолщение стены увеличивает звукоизоляцию примерно на 20 дБ.

## Предотвращение перехвата электрических и радиосигналов

Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается:

* выключением во время разговора всех радиосредств и электрических приборов, в которых нет необходимости;
* 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 фильтрам 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, включаемого во время проведения совещания по тематике, содержащей тайну;
* установкой в свободный слот системной платы компьютера плат генератора помех.

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

* использования защитных ПЭВМ;
* размещения системного блока в специальном сейфе;
* установки винчестера в съемный кожух и хранения его в сейфе;
* программной защиты доступа к компьютеру и отдельным папкам;
* криптографического шифрования информации, хранящейся на машинных носителях.

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

-

Рис. 3. Примерный план расположения организации

Кабинет руководителя имеет два окна, выходящие на улицу, и дверь в приемную. Площадь кабинета составляет около 30 м2, приемной – 20 м2. Схематический чертеж варианта кабинета приведен на рис. 4.



Рис.

 4.

Примерный план кабинета руководителя

Для описания фактов, влияющих на защищенность информации в

кабинете, проводится его обследование. Описание

помещения содержит 5

групп факторов:

-

общая характеристика помещения;

-

ограждения;

-

предметы мебели и интерьера;

-

радиоэлектронные средства и электрические приборы;

-

средства коммуникаций.

Результаты обследования помещены в табл.

 5.

Таблица 5

Результат обследования защищаемого помещения

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п  | Факторы влияния  | Параметры  | Примечание  |
| 1  | 2  | 3  | 4  |
|  | **1. Общая характеристика**  |
| 1.1  | Этаж  | 3-й  |   |
| 1.2  | Площадь, м2  | 30 м2  |   |
| 1.3  | Смежные помещения  | Справа – приемная; слева – кабинет заместителя; сверху – служебное помещение организации  |   |
|  |  **2. Ограждения**  |
| 2.1   | Стены   | *Наружная* – железобетонная толщиной 400 мм, на стене укреплены 2 чугунные батареи отопления, соединенные металлическими трубами с трубами в боковых стенах; *смежная с коридором* – железобетонная толщиной 140 мм; 2 вентиляционных отверстия;*смежная с приемной* – кирпичная толщиной в 1 кирпич (270 мм); *смежная с кабинетом заместителя* – железобетонная толщиной 140 мм  |   |
| 2.2  | Потолок  | Железобетонная плита толщиной 400 мм, окрашенная водо-эмульсионной краской  |   |
| 2.3  | Пол  |  Железобетонная плита толщиной 400 мм, покрытая паркетом и ковролином |   |
| 2.4  | Окна  | Количество – 2, двухрамные, обращены на улицу, толщина стекла –3 мм  |   |
| 2.5  | Дверь  | Типовая щитовая, без доводчика, выход в  |   |
|  |  **3. Предметы мебели и интерьера**  |
| 3.1  | Картина  | Размеры рамы 700×500 мм, расположена под углом к стене, смежной с коридором  |   |
| 3.2  | Шкаф книжный  | Дверцы стеклянные, на 4 полках книги и папки с документами  |   |
| 3.3  | Сейф напольный  | Замок механический кодовый  |   |
| 3.4  | Стол приставной  | Имеет под столешницей полку  |   |
| 3.5  | Столик под телевизионную аппаратуру  | 1 шт.  |   |

Окончание табл. 5

|  |  |  |  |
| --- | --- | --- | --- |
| 1  | 2  | 3  | 4  |
| 3.6  | Доска-экран  | Размер 2000×1200 мм, из белого пластика  |   |
| 3.7  | Кресло кожаное вращающееся  | 1 шт.  |   |
| 3.8  | Кожаные кресла для отдыха  | 2 шт.  |   |
| 3.9  | Журнальный столик  | 1 шт.  |   |
| 3.10  | Стол для заседаний  | Рассчитан на 10 человек  |   |
| 3.11  | Стулья  | Деревянные полужесткие, 10 шт.  |   |
|  | **4. Радиоэлектронные средства и электрические приборы**  |
| 4.1  | Компьютер  | Состав: системный блок, монитор, мышь, клавиатура, 2 динамика, на письменном столе  |  |
| 4.2  | Телефон закрытой связи (ЗАС)  | На приставном столике  |   |
| 4.3  | Видеодвойка (телевизор+видеомагнито фон)  | В случае просмотра видеокассет с закрытой информацией  |   |
| 4.4  | Телефон городской АТС  | На приставном столике  |   |
| 4.5  | Телефон внутренней АТС  | На приставном столике  |   |
| 4.6  | Концентратор  | Под приставного столика  |   |
| 4.7  | Видеодвойка  | Просмотр видеокассет с открытой информацией  |   |
| 4.8  | Вентилятор  | На письменном столе  |   |
| 4.9  | Вторичные часы единого времени  | На стене, смежной с приемной  |   |
| 4.10  | Громкоговоритель оповещения  | На стене, смежной с коридором  |   |
| 4.11  | Настольная лампа  | 1 шт.  |   |
| 4.12  | Люстра из 5 рожков  | 1 шт. на потолке  |   |
| 4.13  | Извещатели пожарные  | 2 шт. на потолке  |   |
|  | **5. Средства коммуникаций**  |
| 5.1  | Розетки электропитания  | Одна – возле письменного стола, другая – возле видеодвойки  |   |
| 5.2  | Телефонные розетки  | 2 шт. возле письменного стола  |   |
| 5.3  | Электропроводка  | Скрытая в стенах  |   |
| 5.4  | Кабели телефонных линий  | Наружные, на стене возле письменного стола  |   |
| 5.5  | Кабель локальной сети  | Витая пара, укрепленная на стене  |   |
| 5.6  | Шлейф пожарной сигнализакции  | Наружный, на потолке и стене возле письменного стола  |   |

*Примечание.* Характеристики ограждений, указанные в этой таблице, занижены по сравнению с типовыми реальными значениями с целью выявления большего количества угроз подслушивания.

**В вашем отчете по практической работе должны быть:**

1. Примерный план кабинета (нарисованная схема как в примере)
2. Результат обследования защищаемого помещения (полная таблица)

Кабинет 418