ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ФИЗИКО-МАТЕМАТИЧЕСКИЙ

КАФЕДРА ОРГАНИЗАЦИИ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

САМОСТОЯТЕЛЬНАЯ КОНТРОЛИРУЕМАЯ РАБОТА

по дисциплине: «Инженерно-техническая защита информации»

на тему: «**Разработка сценария инженерно-технической защиты информации в кабинете руководителя организации**»

Выполнил:

Фомин Александр Юрьевич

студент 4 курса ФМФ А группы

специальности

организация и технология защиты информации

очной формы обучения

Руководитель работы:

Сагдеев Константин Мингалеевич

к.т.н., доцент кафедры ОиТЗИ

Ставрополь 2008

Оглавление

Введение

1. Моделирование и ранжирование угроз информации в кабинете руководителя

1.1 Анализ способов и средств наблюдения, моделирование оптического канала утечки информации

1.2 Анализ способов и средств подслушивания акустических сигналов, моделирование акустических каналов утечки информации

1.3 Анализ способов и средств перехвата радиосигналов, моделирование радиоэлектронных каналов утечки информации

1.4 Анализ способов и средств добывания информации о демаскирующих признаках веществ, моделирование материально-вещественных каналов утечки информации

1.5 Ранжирование видов угроз информации в кабинете руководителя

1.6 Вывод

2. Разработка и выбор мер по нейтрализации угроз информации в кабинете руководителя организации

2.1 Анализ методов, способов и средств инженерной защиты объектов и инженерно-технических средств видеоконтроля и обнаружения злоумышленников

2.2 Выработка мер по предотвращению проникновения злоумышленника к источникам информации в кабинете руководителя

2.3 Структура комплекса технических средств охраны административного здания

2.4 Система контроля и управления доступом персонала и транспорта ко всем объектам организации

2.5 Вывод

Заключение

Список литературы

# Введение

Цели работы:

1) Моделирование и ранжирование угроз информации в кабинете руководителя;

2) Разработка и выбор мер по нейтрализации угроз информации в кабинете руководителя организации.

Объект работы: Организация и кабинет руководителя организации.

Предмет работы: Сценарий инженерно-технической защиты информации в кабинете руководителя организации.

Актуальность: Информация является основой для любой деятельности людей. Проведение собственных исследований для получения информации является достаточно дорогостоящим процессом. Поэтому в современном обществе стали широко распространятся незаконные пути добывания информации. В связи с этим возрастает актуальность защиты информации в любой организации и сфере деятельности человека. А разработка сценария инженерно-технической защиты информации в кабинете руководителя организации является одной из мер защиты информации.

# 1. Моделирование и ранжирование угроз информации в кабинете

# руководителя

Для успешной реализации комплекса мер по защите информации в кабинете руководителя организации необходимо смоделировать ряд угроз, которые наиболее вероятно будут воздействовать на конфиденциальную информацию. Затем следует произвести ранжирование приведенных угроз, взяв за основание классификации вероятность конкретной реализации этих опасных воздействий.

## 1.1 Анализ способов и средств наблюдения, моделирование

## оптического канала утечки информации

Наблюдение предполагает получение и анализ изображения объекта наблюдения. При наблюдении добываются, в основном, видовые признаки объектов. Но возможно добывание семантической информации, если объект наблюдения представляет собой документ, схему, чертеж т. д.

Объекты могут наблюдаться непосредственно – глазами или с помощью технических средств. Различают следующие способы наблюдения с использованием технических средств:

- визуально-оптическое;

- с помощью приборов наблюдения в ИК-диапазоне;

- наблюдение с консервацией изображения (фото и киносъемка);

- телевизионное наблюдение, в том числе с записью изображения;

- лазерное наблюдение.

Для визуально-оптического наблюдения применяются оптические приборы, увеличивающие размеры изображения на сетчатке глаза. В результате этого повышается дальность наблюдения, вероятность обнаружения и распознавания мелких объектов. К визуально-оптическим приборам относятся бинокли, монокуляры, подзорные трубы, специальные телескопы. Также могут использоваться приборы для кино и фотосъемки. Существуют всевозможные приборы ночного видения, наблюдения в инфракрасном диапазоне, но применительно к данному зданию такие меры не могут быть осуществлены, большое количество техники не позволит дать злоумышленнику приемлемое изображение.

В данном случае организация находиться в оживленном районе. Здание офиса окружено жилыми домами, магазинами, откуда можно легко вести наблюдение. Однако кабинет руководителя расположен таким образом, что прямой обзор перекрывают цеха.

В общем случае оптический канал утечки информации выглядит следующим образом (рисунок 1):

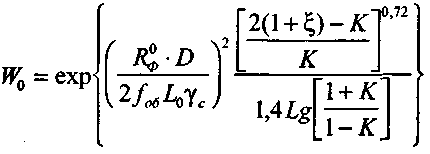


Рисунок 1. – Оптический канал утечки информации

Рассмотрим вероятность обнаружения объекта в оптическом канале утечки информации.

Вероятность обнаружения объекта Wo на заданной дальности рассчитывается по формуле

, (1)

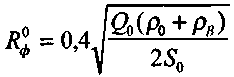


где К – контраст объекта, а Roф – коэффициент формы объекта, которые соответственно рассчитываются по формулам:

, (2)

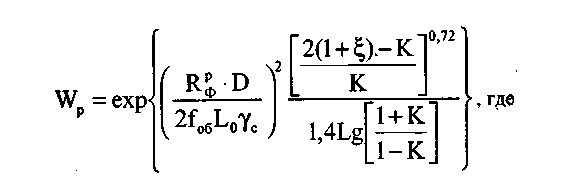


. (3)

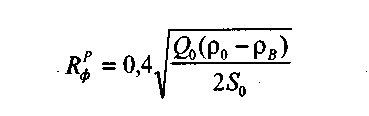


Для расчета вероятности распознавания объекта Wp на заданной дальности аппаратурой фоторазведки используются те же исходные данные и формулы. Отличие заключается в том, что при расчете Wp в формулах необходимо подставить вместо коэффициента формы объекта для обнаружения коэффициент формы объекта для распознавания Rрф

, (4)



(5)



Геометрическая характеристика объекта защиты:

- максимальные линейные размеры объекта (Lo);

- периметр контура объекта (Qo);

- радиус описанной окружности объекта (о);

- радиус вписанной окружности объекта (в);

- площадь объекта(Sо).

Фотометрическая характеристика объекта защиты:

- коэффициент яркости объекта (Во);

- коэффициент яркости фона (Вф).

Характеристика аппаратуры разведки:

- фокусное расстояние объектива (fоб);

- разрешающая способность системы «объектив-фотослой» (с).

Характеристика условий ведения разведки:

- коэффициент задымленности атмосферы ();

- расстояние между объектом и аппаратурой разведки (D).

Для данного кабинета руководителя рассчитаем вероятность обнаружения листа бумаги формата А4, лежащего на столе руководителя злоумышленником с крыши соседнего дома, максимальные линейные размеры которого (Lo) равны 0,3 метра, периметр контура (Qo) равный 1 м., площадь равна 0,06 м., а радиус описанной окружности объекта (о) и радиус вписанной окружности объекта (в) соответственно 0,2 и 0,1 метров. Расстояние до крыши соседнего дома равно 110 метров, от окна до объекта равно 2,5 метра, а коэффициент задымленности атмосферы равен 0,05. Коэффициент яркости листа на стене около 0,6, а коэффициент яркости фона (Вф) около 0,9. Фокусное расстояние объектива (fоб) и разрешающая способность системы «объектив-фотослой» (с) равны соответственно 20 мм и 100 линий/мм. Вероятность обнаружения равна 0,93. Такая вероятность достаточно велика для визуального распознания, написанного на листе бумаги, поэтому в данной организации приняты соответствующие меры по предотвращению угрозы в оптическом канале. А именно – методы энергетического скрытия. Это окна с зеркальным покрытием и шторы, препятствующие проникновению света, что затрудняет вести наблюдение.

## 1.2 Анализ способов и средств подслушивания акустических

## сигналов, моделирование акустических каналов утечки

## информации

Подслушивание, как и наблюдение, бывает непосредственное и с помощью технических средств. Непосредственное подслушивание использует только слуховой аппарат человека. В силу малой мощности речевых сигналов разговаривающих людей и значительного затухания акустической волны в среде распространения непосредственное подслушивание возможно на небольшом расстоянии. Поэтому для подслушивания применяются различные технические средства. Этим способом добывается в основном семантическая (речевая) информации, а также демаскирующие признаки сигналов от работающих механизмов, машин и других источников звуков. Структура этого канала утечки информации приведена на рисунке 2.



Рисунок 2. – Акустический канал утечки информации

Существуют следующие способы получения акустической информации:

- акустооптический;

- виброакустический;

- применение подслушивающих закладок;

- ВЧ-навязывание.

Акустооптический съем информации возможен с тех же позиций, что и наблюдение в оптическом диапазоне.

Виброакустический КУИ реализуется по средствам снятия вибрации со средств коммуникации и вентиляции с последующим преобразованием в акустические колебания. Технические средства, необходимые для реализации ВЧ-навязывания могут быть подключены к линии связи в коммутационной коробке, находящейся на первом этаже.

Для примера рассмотрим расчет словесной разборчивости речи в кабинете руководителя.

Словесная разборчивость речи (W) рассчитывается по формуле

 (6)

где R – интегральный индекс артикуляции речи.

Интегральный индекс артикуляции речи (R) определяется по формуле

****  (7)

где ri – октавный индекс артикуляции. Здесь и далее i – порядковый номер октавной полосы (i=1,2,3,4,5) со среднегеометрическими частотами fсрi=250, 500, 1000, 2000, 4000 Гц.

Октавный индекс артикуляции речи (ri) рассчитывается по формуле

, (8)

где γ – индикаторная функция, показывающая, как энергетические условия разведывательного контакта, влияют на разборчивость звуков в октавных полосах

, (9)

где Qi – октавное отношение «речевой сигнал/помеха» в месте возможного размещения акустических или вибрационных приемных датчиков аппаратуры акустической речевой разведки, дБ;

Ai – формантный параметр спектра речевого сигнала в октавной полосе, дБ;

ki – весовой коэффициент октавной полосы частот.

Числовые значения Ai и ki принимаются из таблицы 1.

Таблица 1. – Числовые значения Ai и ki

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Среднегеометрические частоты октавных полос fcpi, Гц | 250 | 500 | 1000 | 2000 | 4000 |
| Числовое значение формантного параметра спектра речевого сигнала в октавной полосе частот Ai, дБ | 18 | 14 | 9 | 6 | 5 |
| Числовое значение весового коэффициента октавной полосы частот ki | 0,03 | 0,12 | 0,20 | 0,30 | 0,26 |

Числовое значение Qi определяется из энергетического соотношения

, (10)

где Lsi – октавный уровень защищаемого речевого сигнала на выходе источника акустических сигналов, дБ.

Zi – потери (затухание) акустического речевого сигнала (или вибрационного сигнала, сопутствующего защищаемой речи), в среде распространения от источника речи до места размещения приемного акустического (вибрационного) приемника аппаратуры акустической речевой разведки, дБ.

Lшi – уровень акустического (вибрационного) шума в i-ой октавной полосе, дБ, в месте возможного размещения акустического (вибрационного) приемника аппаратуры акустической речевой разведки, дБ.

Все сооружение выполнено кирпичной кладкой в два кирпича со штукатуркой с двух сторон. Разборчивость речи при средней громкости будет равна 12%, что говорит о том, что степень разборчивости через стены будет не приемлема. Это значит, что злоумышленник не сможет уловить даже тему разговора.

## 1.3 Анализ способов и средств перехвата радиосигналов,

## моделирование радиоэлектронных каналов утечки информации

Любой объект защиты информации содержит технические средства передачи, приема, хранения и обработки информации. К таким средствам относятся электронно-вычислительная техника, информационные системы, слаботочное оборудование. Эти средства в свою очередь являются объектами радиоэлектронной разведки злоумышленников, поскольку обладают наиболее информативными каналами утечки информации.

Радиоэлектронный канал относится к наиболее информативным каналам утечки Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала (рисунок 3).



Рисунок 3

В радиоэлектронных каналах утечки информации источники сигналов могут быть четырех видов:

- передатчики функциональных каналов связи;

- источники опасных сигналов;

- объекты, отражающие электромагнитные волны в радиодиапазоне;

- объекты, излучающие собственные (тепловые) радиоволны в радиодиапазоне.

Также возможен перехват сигнала подвижной сотовой связи и излучающих ЗПУ не составляет особого труда, т.к. близко жилые дома, внутри которых можно установить приемники.

Для расчета Wo излучения РЭС аппаратурой РТР необходимы следующие исходные данные (случай прямой видимости).

По объекту:

- мощность передатчика РЭС (Ризл);

- коэффициент направленного действия (КНД) антенны РЭС в направлении аппаратуры разведки (Go);

- длина волны излучения (λ).

По аппаратуре разведки:

- вероятность ложной тревоги (WЛТ);

- предельная чувствительность приемника (Рпр);

- КНД антенны приемника (Gпр).

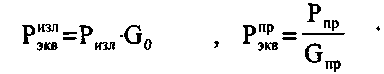
По условиям ведения разведки:

- дальность между объектом и аппаратурой разведки (D).

При наличии перечисленных исходных данных расчет производится в следующем порядке.

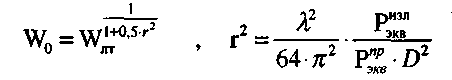
Предварительно определяется эквивалентная мощность передатчика РЭСи эквивалентная чувствительность разведывательного приемника

, (11)



Затем рассчитывается Wo по формулам

, (12)



При ведении пассивной РЭР (РР и РТР) радиосигнал от объекта разведки (излучателя) распространяется к разведывательному приемнику. В этом случае мощность радиосигнала на входе приемника определяется формулой

, (13)

где: РИЗЛ – мощность излучателя;

g0 – коэффициент усиления антенны;

SЭФ – эффективная площадь приемной антенны SЭФ  (0.5÷0.7)\*SГЕОМ;

SГЕОМ – геометрическая площадь приемной антенны;

D – расстояние до разведуемого объекта.

Для средств разведки этот сигнал наблюдается на фоне внутренних шумов приемника. Если спектральная плотность внутренних шумов приемника равна n0, то для максимальной дальности действия средства разведки имеем

, (14)

где: qo – требуемое отношение сигнал/шум на выходе приемника;

αП – потери в отношении сигнал/шум в тракте приемника;

No – спектральная плотность шума; ∆fпр – полоса пропускания приемника.

Реальная дальность действия пассивных средств разведки меньше dМАКС, что обусловлено поглощением энергии излучения при распространении радиоволн в атмосфере. Реальная дальность действия уменьшается по сравнению с dМАКС в  раз, где αпг – коэффициент поглощения сигнала в атмосфере.

При оценке дальности действия активных средств разведки необходимо учитывать двойное распространение радиоволн – до объекта разведки и обратно к приемнику разведсредства.

, (15)

Где  – эффективная поверхность рассеивания объекта.

Реальная дальность действия средства разведки уменьшается по сравнению с в  раз.

Для данной организации рассчитаем возможность перехвата радиоизлучения мобильного телефона, на котором говорят внутри организации. При этом приемник расположен на той же крыше.

Мощность передатчика равна 100 мВт, чувствительность приемника равна  Вт, КНД антенны приемника равен 5, КНД передатчика 1, длина волны излучения 0,3 м., вероятность ложной тревоги 0,001, дальность между объектом и аппаратурой разведки 110 м.

В результате расчетов съем информации активным средством радиоэлектронной разведки возможен на расстоянии до 235 метров. Это расстояние выходит далеко за пределы контролируемой зоны, а следовательно очень опасно.

Для предотвращения возможности утечки информации необходимо использовать генератор шума ГШ-1000.

## 1.4 Анализ способов и средств добывания информации о

## демаскирующих признаках веществ, моделирование материально-

## вещественных каналов утечки информации

информация утечка видеоконтроль защита

Особенность этого канала вызвана спецификой источников и носителей информации по сравнению с другими каналами. Источниками и носителями информации в нем являются субъекты (люди) и материальные объекты, которые имеют четкие пространственные границы.

Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны.

Основными источниками информации материально-вещественного канала утечки информации являются следующие:

* черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации;
* отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;
* содержащие защищаемую информацию дискеты ПЭВМ, нечитаемые из-за их физических дефектов и искажений загрузочных или других секторов;
* бракованная продукция и ее элементы;
* отходы производства с демаскирующими веществами в газообразном, жидком и твердом виде;

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Структурная схема материально-вещественного канала утечки информации приведена на рисунке 4.



Рисунок 4. – Материально-вещественный канал утечки информации

Отходы вывозятся с территории организации специальной компанией по переработке промышленного мусора, с которой предприятие заключило договор. Остальные отходы, выбрасываемые из офиса, помещается в обычные контейнеры за пределами контролируемой зоны. Документы, содержание которых имеет определенную ценность для злоумышленника, уничтожаются в установленном порядке отдельно от других документов.

## 

## 1.5 Ранжирование видов угроз информации в кабинете

## руководителя

В данной организации в кабинете руководителя существуют следующие угрозы:

1) Материально-вещественный канал. Он является наиболее опасным каналом утечки информации в кабинете руководителя для данной организации. Его достоинством является простота доступа к источникам информации. Причем действия, связанные получением сведений таким путем не влекут привлечения к уголовной ответственности. Но для реализации своих целей злоумышленнику придется затратить определенное количество времени для переработки большого объема информации. Также наиболее важные документы уничтожаются в установленном порядке. Но, тем не менее, такая вероятность существует и в кабинете руководителя эта угроза является особенно значимой.

2) Оптический канал утечки информации. Угроза по этому каналу маловероятна, так как в кабинете руководителя предусмотрены меры по предотвращению реализации этой угрозы. Но вероятность существует вследствие того, что на рынке существует обилие разных средств ведения наблюдения, применении которых не исключает утечки информации по этому каналу.

3) Акустический канал утечки информации. Наиболее распространенный способ снятия информации это подслушивание. На рынке существует большое разнообразие технических подслушивающих средств. Но трудность реализации такого способа в кабинете руководителя данной организации заключается в инженерно-строительных особенностях самого здания.

4) Радиоэлектронный канал утечки информации. Реализация угрозы по этому каналу маловероятна, так как существует большое затухания сигнала вследствие поглощения его в железобетонных конструкциях жилых домов и также в кабинете руководителя поставлен генератор шума ГШ-1000.

5) НСД по средствам физического проникновения. Злоумышленник может произвести нарушение целостности, доступности и конфиденциальности информации. Но осуществление этой угрозы практически невозможно, так как организация имеет два КПП и систему видеонаблюдения, как по всему периметру, так и в здании.

## 1.6 Вывод

Таким образом, в результате анализа установлено, что наиболее опасным каналом утечки информации в кабинете руководителя является материально-вещественный канал. Но реализация угроз по остальным каналам тоже возможна, хотя и маловероятна. Поэтому необходимо уделять должное внимание всем каналам утечки информации, так как также возможно их комплексное использование злоумышленником.

# 2. Разработка и выбор мер по нейтрализации угроз информации в

# кабинете руководителя организации

## 2.1 Анализ методов, способов и средств инженерной защиты

## объектов и инженерно-технических средств видеоконтроля и

## обнаружения злоумышленников

Телевизионные средства наблюдения образуют так называемую систему замкнутого телевидения (ССТЧ) или видеоконтроля, в которой передача видеосигналов от телевизионных камер к мониторам производится в пределах контролируемой (охраняемой) зоны.

В общем случае система видеоконтроля включает следующие основные средства:

* передающие телевизионные камеры;
* устройства отображения видеоинформации;
* мониторы;
* устройства обработки видеоинформации (коммутаторы, квадраторы, мультиплексоры);
* устройства регистрации информации (бытовые и специальные видеомагнитофоны);
* кабели, обеспечивающие электрические связи элементов системы видеонаблюдения.

Средства телевизионного наблюдения обеспечивают:

* визуальный контроль за зонами и рубежами зашиты;
* наблюдение за нарушителями рубежей охраны, определение их количества, вооруженности, действий и намерений;
* контроль за действиями лиц охраны и персонала организации;
* запись видеоизображений для последующего обнаружения и опознавания злоумышленников, контроля и анализа действий сотрудников охраны.

В данной организации по всему периметру расставлено 10 видеокамер, одна из которых с поворотным механизмом. Все они выводятся на мониторы службы охраны, находящейся на КПП около въезда на территорию (рисунок 5).



Рисунок 5. – Общий план периметра

Также помимо видеокамер, находящихся на улице, три видеокамеры установлены на первом этаже, где находится кабинет руководителя. Они расположены таким образом, что хорошо просматривается весь коридор (рисунок 6). Изображение с этих видеокамер выходит на мониторы, расположенные на КПП здания на первом этаже.

## 2.2 Выработка мер по предотвращению проникновения

## злоумышленника к источникам информации в кабинете

## руководителя

Одними из мер по предотвращению проникновения злоумышленника к источникам информации в кабинете руководителя является создание рубежей защиты.

В данной организации разработано два рубежа защиты. Первым является бетонный забор и контрольно-пропускной пункт при въезде на территорию.

Рубеж контрольный пропускной пункт находиться в трех состояниях, как и рубеж забор в дневную смену, в пересмену, когда КПП закрыт, как и ночную смену и в ночную смену. В этом случае вероятность попадания злоумышленника во время дневной через КПП будет маловероятной, так как ведется пропускной режим. В другое время попасть на территорию предприятия будет невозможно, потому что охрана во время пересмены и ночной смены уже никого не впускает. Другой вариант попадания на территорию предприятия для злоумышленника, это через забор. Во время пересмены, когда охрана более или менее отвлечена, он может перелезть через забор, но при этом вероятность, что его не обнаружат при помощи камер видеонаблюдения, будет мала. Остальные варианты невозможны, так как на предприятии ведется видеонаблюдение. Причем злоумышленник должен попасть во двор в рабочее время, потому что в нерабочее проезд и проход запрещен и делается периодический обход территории.

Вторым рубежом защиты является пункт охраны перед входом в здание офиса. Дверь в здание может находиться в закрытом состоянии под сигнализацией в нерабочее время и открытая в рабочее время. Контроль осуществляется как на первом, так и на втором рубеже по пропускам, выдаваемые только работникам данной организации. В здание через дверь можно попасть в двух случаях, что злоумышленника не заметит охрана или у злоумышленника будут поддельные документы, работника другой организации. В ночную смену дверь будет под сигнализацией, и территория под наблюдением, при которых проникновение будет невозможно.

Созданные рубежи защиты и вместе с ними система видеонаблюдения практически исключают возможность проникновения злоумышленника на территорию организации. Также как и в любом здании офиса по требованиям пожарной безопасности все здание оборудовано системой пожарной сигнализации.

## 2.3 Структура комплекса технических средств охраны

## административного здания

В данной организации по всему периметру расставлено 10 видеокамер, одна из которых с поворотным механизмом. Все они выводятся на мониторы службы охраны, находящейся на КПП около въезда на территорию (рисунок 5).



Рисунок 6. – План этажа

Восемь камер предназначены для контроля периметра, а две других – для контроля внутренней территории.

## 2.4 Система контроля и управления доступом персонала и

## транспорта ко всем объектам организации

Для пропуска люду и автомобилей на территорию данной организации создан контрольно-пропускной пункт: проходная для людей и ворота для транспорта. В общем случае КПП включает:

1. зал со средствами управления доступом для прохода людей;
2. бюро пропусков;
3. камера хранения вещей персонала и посетителей, не разрешенных для проноса в организацию;
4. помещения для начальника охраны, дежурного контролера, размещения охранной сигнализации и связи и др.;
5. средства управления доступом транспорта.

КПП обеспечивает необходимую пропускную способность людей и транспорта. Он содержит механизмы и устройства идентификации людей.

В данной организации на КПП применяется вращающий турникет в полный рост. Дверной просвет турникета исключает возможность прохода вдвоем. Для транспорта используются автоматические ворота. В организации используется два КПП, непосредственно перед входом на территорию организации и в здании офиса на первом этаже.

Способы идентификации людей разделяются на атрибутивные и биометрические. В качестве таких идентификаторов могут быть:

1) пропуска, жетоны и другие документы на право допуска;

2) идентификационные карточки.

В данной организации используются только атрибутивные способы. Это пропуска для работников организации.

**2.5 Вывод**

Таким образом, в результате анализа были определены меры по противодействию от проникновения злоумышленника. Созданные рубежи защиты и вместе с ними система видеонаблюдения практически исключают возможность проникновения злоумышленника на территорию организации. Также как и в любом здании офиса по требованиям пожарной безопасности все здание оборудовано системой пожарной сигнализации, что исключает нарушение целостности информации.

Также была рассмотрена структура комплекса технических средств охраны административного здания и удаленно расположенного складского помещения, с помощью которой можно увидеть места расположения средств охраны от проникновения злоумышленника на территорию организации и структуру КПП, который является первым рубежом защиты от злоумышленника.

# Заключение

В процессе изучения инженерно-технической защиты информации в кабинете руководителя организации было произведено моделирование и ранжирование угроз информации в кабинете руководителя и разработка и выбор мер по нейтрализации угроз информации в кабинете руководителя организации.

Таким образом, в результате анализа установлено, что наиболее опасным каналом утечки информации в кабинете руководителя является материально-вещественный канал. Но реализация угроз по остальным каналам тоже возможна. Поэтому необходимо уделять должное внимание всем каналам утечки информации, так как также возможно их комплексное использование злоумышленником.

Также были определены меры по противодействию от проникновения злоумышленника. Созданные рубежи защиты и вместе с ними система видеонаблюдения, контрольно-пропускные пункты практически исключают возможность проникновения злоумышленника на территорию организации.

# Список литературы

1. Курс лабораторных работ по дисциплине «Инженерно-техническая защита информации».

2. Курс лекций по дисциплине «Инженерно-техническая защита информации».

3. Торокин А.А. Инженерно-техническая защита информации. – М.: Ось-89, 2005.

4. Ярочкин В.И. Информационная безопасность: Учебное пособие для студентов непрофильных вузов. – М.: Академический Проект, 2005.