**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

**ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНЕВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ**

Дата сдачи: 09.02.02г.

кафедра «Системы и технологии защиты информации»

**КУРСОВАЯ РАБОТА**

по дисциплине: **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

на тему: Разработка комплексной системы защиты информации объекта защиты.

**Вариант №15**

Проверил: Выполнил:

преподаватель студентка: Крюкова А.Н.

Решков К.А. шифр: 2000-ИТ-1250

Омск

2004

**Введение**

Становление информационного общества связано с широким распространением персональных компьютеров, построением глобальной информационной Сети и подключения к ней большого числа пользователей. Эти достижения должны коренным образом изменить жизнь общества, выдвинув на передний план деятельность, связанную с производством, потреблением, трансляцией и хранением информации.

Одной из наиболее серьезных проблем, затрудняющих применение информационных технологий, является обеспечение информационной безопасности.

**Информационная безопасность** – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – её функционирование не создаёт информационных угроз для элементов самой системы и внешней среды.

**Угроза безопасности информации** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными и непреднамеренными воздействиями на нее.

Компьютерная революция помогла информации стать центром внимания основополагающих воззрений. Признание информации основой жизни вряд ли сводимо к внутренним мотивациям. Социальные, экономические и политические науки в попытках осознания происходящих перемен обращают пристальное внимание на компьютерную информацию, как на новый фактор глобального влияния.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Согласно ГОСТу 350922-96, защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

**Целью курсовой работы является:**

Разработать комплексную систему защиты информации, обеспечивающую выполнение требований соответствующей нормативной базы и блокирование определенных технических каналов утечки информации.

# Описание объекта защиты

##

## 1.1 Описание вида деятельности и формы собственности объекта защиты

Объектом защиты в данной курсовой работе согласно Гост Р51275-99. об Объекте информатизации, то есть - это совокупность информационных средств и систем обработки информации, используемые в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещение или объектов, в которых они установлены или помещения и объекты, предназначенные ведения конфиденциальных переговоров. Будет являться **Помещение** состоящего из 1 компьютера и проектора для презентаций. Используется для проведения заседаний совета директоров. На компьютере содержатся данные относящиеся к коммерческой тайне.

Помещение находится в здании отделения дороги Златоустовского региона в региональном отделе автоматизированной системы управления, для проведения информационных заседаний и решения различных вопросов по отделу. Объект защищается на уровне Регионального отдела автоматизированной системы управления занимающийся деятельностью информационных ресурсов, поставке и настройке программного обеспечения ПК для пользователей различных предприятий Златоустовского региона. Данное помещение используется отделом для заседаний и советов по решению различных информационных вопросов в количестве 7 ответственных лиц заседания.

**Вариант задания для курсовой работы**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Граница контролируемой зоны | Категория информации ограниченного доступа | Технический канал утечки информации(угроза) |
| помещение | КТ | ВА | ОК |

Принятые сокращения:

ПД – персональные данные;

КТ – коммерческая тайна;

СТ – служебная тайна;

ПЭМИ – паразитные электромагнитные излучения;

ВА – виброакустический;

ОЭ – оптико-электронный.

## 1.2 План объекта защиты, взаимное расположение других помещений


# 2. Категорирование информации на объекте защиты

##

## 2.1 Определение перечня общедоступной информации

Перечень общедоступной информации:

1. Информация об уставе организации, правилах внутреннего трудового распорядка дня и правил техники безопасности при работе с персональной техникой;

2. Информация о занимаемых должностях сотрудников, ФИО и их рабочих телефонах;

3. Информация о графике работы организации;

4. Клиентские база данных;

5. Информация о списках предприятий по региону и их курирующих лиц;

##

## 2.2 Определение перечня информации ограниченного доступа

 Перечень информации ограниченного доступа:

1.Личная информация о сотрудниках и их должностных инструкциях;

2.Информация о поставках техники для распределяемых предприятий;

3.Информация о финансовой деятельности организации (бухгалтерский учет и заработной платы сотрудников);

4.Информация о сетевых настройках компьютеров и серверов;

5.Информация о документах организации;

#

# 3. Угрозы информации с ограниченным доступом

**Угроза безопасности информации** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными и непреднамеренными воздействиями на нее.

## 3.1 Определение перечня внутренних угроз

В реальности существует два вида угроз информационной безопасности:

**1. Внутренняя:**

- несанкционированный доступ в помещение;

- несанкционированный доступ к данным внутри корпоративной сети и данных ПК без ведома сотрудника;

- возможность записи информации на переносные устройства (флэш-накопители, CD- и DVD-диски и т.п.);

- пересылка фотоснимков бумажных носителей и экранов мониторов с помощью мобильных телефонов и другими способами, через удаленный доступ к ПК;

- программные вирусы и «троянские» программы;

- незаконное скачивание и распространение за пределами предприятия лицензионных программ организации;

- не контролируемая электронная почта;

- вынос техники организации, без соответствующего документа;

- внос посторонней техники на территорию организации;

##

## 3.2 определение перечня внешних угроз

**2. Внешняя:**

- несанкционированный доступ из сети Интернет;

- снятие информации с кабельных систем (ЛВС и электропитания) при помощи технических средств;

- запись разговоров на расстоянии сквозь стены (окна, двери) и т. д.;

-несанкционированная установка, микрофонов в помещениях;

# 4. Реализация комплексной системы защиты информации

##

## 4.1 Разработка системы разграничения доступа

4.1.1 Матрица доступа будет определять порядок доступа с соответствующими правами на запись (**W**), чтение
(**R** ), и модификацию данных (**U**) к общедоступной и закрытой информации различным ролям в сети.

**Матрица доступа к общедоступным информационным ресурсам**

|  |  |
| --- | --- |
| Сотрудники | Роли |
| G1 | G2 | G3 | G4 | G5 |
| S1 | R | R | R | RW | RW |
| S2 | R | R | RW | RW | RW |
| S3 | R | R | R | RW | RW |
| S4 | R | R | R | RW | RW |
| S5 | R | R | RW | RW | RW |
| S6 | R | R | R | RW | RW |
| S7 | RWU | RWU | RWU | RWU | RWU |

**Информация G доступ к которой не ограничен (общедоступная информация).**

**Роли G**

G1. Информация об уставе организации, правилах внутреннего трудового распорядка дня и правил техники безопасности при работе с персональной техникой;

G2. Информация о занимаемых должностях сотрудников, ФИО и их рабочих телефонах;

G3. Информация о графике работы организации;

G4. Клиентские база данных;

G5. Информация о списках предприятий по региону и их курирующих лиц;

 **Сотрудники S**

**S**1 Программист;

**S**2 Программист 1 категории;

**S**3 Программист 2 категории;

**S**4 Технолог;

**S**5 Технолог 1 категории;

**S**6 Техник 1 категории;

**S**7 Ведущий программист;

**Информация G доступ к которой ограничен.**

**Роли G**

G1.Личная информация о сотрудниках и их должностных инструкциях;

G2.Информация о поставках техники для распределяемых предприятий;

G3.Информация о финансовой деятельности организации (бухгалтерский учет и заработной платы сотрудников);

G4.Информация о сетевых настройках компьютеров и серверов;

G5.Информация о документах организации;

**Сотрудники S**

**S**1 Программист;

**S**2 Программист 1 категории;

**S**3 Программист 2 категории;

**S**4 Технолог;

**S**5 Технолог 1 категории;

**S**6 Техник 1 категории;

**S**7 Ведущий программист;

**Матрица доступа к ограниченным информационным ресурсам**

|  |  |
| --- | --- |
| Сотрудники | Роли |
| G1 | G2 | G3 | G4 | G5 |
| S1 | R | R | R | RW | R |
| S2 | R | R | R | RW | R |
| S3 | R | R | R | RW | R |
| S4 | R | R | R | RW | R |
| S5 | RW | RW | R | RW | R |
| S6 | R | R | R | R | R |
| S7 | RWU | RWU | RWU | RWU | RWU |

##

## 4.1.2 Меры по разграничению доступа

- определение перечня информации, составляющей коммерческую тайну;

- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

##

## 4.1.2.1 Средства и системы защиты

**Средство защиты информации** – техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации.

**Средства защиты информации делятся на:**

**1. Физические** – различные инженерные средства и сооружения, затрудняющие или исключающие физическое проникновение (или доступ) правонарушителей на объекты защиты и к материальным носителям конфиденциальной информации:

**2. Аппаратные** – механические, электрические, электронные и другие устройства, предназначенные для защиты информации от утечки, разглашения, модификации, уничтожения, а также противодействия средствам технической разведки:

**3. Программные** – специальные программы для ЭВМ, реализующие функции защиты информации от несанкционированного доступа, ознакомления, копирования, модификации, уничтожения и блокирования.

**4. Криптографические** – технические и программные средства шифрования данных, основанные на использовании разнообразных математических и алгоритмических методов.

**5. Комбинированные** – совокупная реализация аппаратных и программных средств и криптографических методов защиты информации.

 В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами. По вибрационному каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

# 4.2 Разработка организационно распорядительной документации.

При разработке организационно- распорядительной документации необходимо учитывать ограничение на распространение информации с ограниченным доступом.

##

## 4.2.1 Трудовой договор

Трудовой договор - соглашение между работодателем и работником, в соответствии с которым работодатель обязуется предоставить работнику работу по обусловленной трудовой функции, обеспечить условия труда, предусмотренные трудовым законодательством и другими нормативными актами, своевременно и в полном размере выплачивать работнику заработную плату, а работник обязуется лично выполнять определенную этим соглашением трудовую функцию, соблюдать правила внутреннего трудового распорядка, действующие у данного работодателя.

Существенными условиями трудового договора являются (ст.57 ТК РФ):

* место работы - наименование и местонахождение организации, куда принимается работник;
* трудовая функция - род работы в соответствии с квалификацией по определенной профессии (должности), которую должен выполнять работник. Род работы остается неизменным на все время действия трудового договора. Работодатель не вправе требовать от работника выполнения работы, не обусловленной трудовым договором;
* дата начала работы;
* условия оплаты труда (в том числе размер тарифной ставки или должностного оклада работника, доплаты, надбавки и поощрительные выплаты).

Трудовой договор может содержать и дополнительные условия, например (ст.57 ТК РФ):

* об установлении испытательного срока;
* о неразглашении охраняемой законом тайны;
* о совмещении профессий (должностей);
* о видах и об условиях дополнительного страхования работника;
* об улучшении социально-бытовых условий работника и членов его семьи;
* об обязанности работника отработать после обучения не менее установленного трудовым договором срока, если обучение проводилось за счет средств работодателя;
* о продолжительности дополнительного отпуска, а также иные условия, не ухудшающие положение работника по сравнению с ТК РФ, законами и иными нормативными правовыми актам (ст.57 ТК РФ).

Заключение трудового договора происходит в письменной форме, договор составляется в двух экземплярах, каждый из которых подписывается сторонами. Один экземпляр трудового договора передается работнику, другой хранится у работодателя.

Прием на работу оформляется приказом о приеме на работу (распоряжением) предприятия работодателя и фиксируется записью в трудовой книжке. Основанием приказа о приеме на работу служит заявление о приеме на работу, написанное работником.

Приложение к договору - это правовой документ, являющийся неотъемлемой частью договора и содержащий дополнительные данные о сделке.

В трудовых договорах используются следующие приложения:

* Должностная инструкция;
* График работы;
* Соглашение о неразглашении конфиденциальной информации;
* Перечень расценок работ.

## 4.2.2 Должностные инструкции

Должностная инструкция - документ, в котором закрепляются обязанности сотрудника, предъявляемые к нему квалификационные требования, порядок замещения и взаимоотношений.

Соглашение применяется на основании и в соответствии с договором, к которому прилагается; форма соглашения определяется индивидуально в каждом конкретном случае.

В должностной инструкции обязательно должен быть прописан пункт о неразглашении конфиденциальной информации (персональных данных).

Ниже приведен пример одной должностной инструкции техника 1- категории, на одного сотрудника данной работы, остальные должностные инструкции аналогичны с некоторой разницей.

**ГЛАВНЫЙ ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР**

ФИЛИАЛ ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА

«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»

(«ОАО «РЖД»)

**ЧЕЛЯБИНСКИЙ**

ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

 **Утверждаю**

Начальник Челябинского ИВЦ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.А. Алексеев

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2007 года

**ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ**

1. **Ф.И.О.:** Фролова Александра Николаевна
2. **Отдел:** РОАСУ-1
3. **Должность:** Техник 1 категории
4. **Замещает:**
5. **Кем замещается:** Программистом 2 категории
6. **Порядок подчинения:** Начальнику отдела, программисту 1 категории
7. **ОБЯЗАННОСТИ:**
	1. Сопровождение инвентаризации «Реестр-регистр», «Реестр-Сбор».
	2. Сопровождение АС «Удар».
	3. Сопровождение комплекса ЕК АСУТР ШР, КУ на предприятиях: ШЧ-10, ПЧ-2, ДТШ Златоуст.
	4. Сопровождение АСУТР по функциональности «Профобучение» и «Охрана труда» на всех предприятиях региона.
	5. Установка программного обеспечения, настройка задач на конкретное рабочее место.
	6. Решение проблем, возникающих при эксплуатации АРМов.
	7. Обучение причастных работников предприятий работать на ПЭВМ, с последующей аттестацией.
	8. Инструктирование причастных сотрудников на рабочих местах о действиях в сложившихся ситуациях по телефону, с помощью программ удаленного доступа, либо выходит на предприятия.
	9. Изучение технологических и методологических материалов.
	10. Участие в составлении планов и отчетов о работе отдела.
	11. Соблюдение правил ТБ и ППБ, устава о дисциплине работников ж.д., правил внутреннего распорядка ИВЦ, требований и правил трудовой дисциплины.
	12. Выполнение отдельных поручений руководства ИВЦ, начальника отдела и его заместителя.
8. **ДОЛЖЕН ЗНАТЬ:**
	1. Технологию бухгалтерского и кадрового учета в системах ЕКАСУФР и ЕК АСУТР.
	2. Технологию установки клиентских мест в системах ЕКАСУФР и ЕК АСУТР.
	3. Правила личной и противопожарной безопасности.
9. **НЕСЕТ ОТВЕТСТВЕННОСТЬ:**
	1. За внедрение задач в пределах своих обязанностей.
	2. За соблюдение сроков выполнения работ.
	3. За соблюдение ТБ, ПТЭ и ППБ.
10. **ИМЕЕТ ПРАВО:**
	1. Обращаться к работникам служб и отделов управления дороги и других подразделений по вопросам, связанным с решением задач для дан­ной службы, отдела или подразделения.
	2. Докладывать о нарушениях, допущенных при эксплуатации оборудования руководителям ИВЦ и службы НКИ.
	3. Обращаться к руководителям отдела и ИВЦ по вопросам организации работы и условий труда.

Начальник РОАСУ-1 \_\_\_\_\_\_\_\_\_\_\_\_ С.В. Быкова “ \_\_\_ “ апреля 2007 г.

ОЗНАКОМИЛСЯ \_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Фролова “ \_\_\_ “ апреля 2007

## угроза доступ собственность защита

## 4.2.3 Инструкции пользователя

Так как каждое место работника оборудовано компьютерной техникой, то существует и инструкция пользователя этой компьютерной техникой. В инструкции пользователя должна быть указана информация о наличии паролей, а так же об ограничении на распространение конфиденциальной информации по корпоративной сети организации через электронную почту.

Приступая к работе, необходимо надлежащим образом подготовить свое рабочее место.

**При обслуживании электронных вычислительных машин.**

Наиболее опасным при обслуживании ПЭВМ является возможное поражение электрическим током.

Сила тока в 0,1А может явиться смертельной. Сопротивление человеческого организма электрическому току колеблется и зависит от ряда причин, в том числе от состояния кожного покрова, от общего состояния нервной системы человека.

Запрещается:

а) присоединять и отсоединять разъемы питания при включенной машине;

б) производить пайку электропаяльником напряжением в сети выше 42 В.

При проведении ремонтных работ на ПЭВМ необходимо создать нормальное освещение рабочего места.

В рабочем режиме все устройства ПЭВМ должны быть закрыты внешней облицовкой.

Заменять бумагу, красящую ленту, только после полной остановки оборудования.

Не загромождать проходы.

**Требования для работающих на ПЭВМ.**

На рабочем месте, где установлена ПЭВМ, должны находиться только обрабатываемые документы, не допускается присутствие посторонних предметов. Стул должен быть удобным, регулируемым по высоте. Экран дисплея должен быть расположен на расстоянии не менее 50 см от глаз работника. Для защиты от прямых солнечных лучей, большой яркости на экранах дисплеев необходимо пользоваться затемняющими шторами.

Операторы, работающие постоянно с терминалами, должны делать перерывы в работе через каждые 2 часа работы на 10 – 15 минут. Во время перерывов делать точечный массаж глаз, чтобы снять усталость.

Не реже 1 раза в смену удалять пыль с экранов при выключенном мониторе. Для исключения влияния статического электричества на работающих не рекомендуется при включенных дисплеях дотрагиваться до экрана руками.

# 4.3 Блокирование технических каналов утечки информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (TCP), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью TCP разведывательной информации об объекте.

##

## 4.3.1 Выбор ТКУИ, подлежащих блокированию. Вибрационные технические каналы утечки информации

В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами. По вибрационному каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

Для установки на внешних оконных стеклах могут использоваться сверхминиатюрные радиостетоскопы, покрытые липкой резиновой массой и по внешнему виду напоминающие шарик или комочек грязи. Такой шарик путем ручного броска приклеивается с наружной стороны окна и передает информацию в течение 1 - 2 дней, по их истечении резиновая масса высыхает, закладка отлипает от поверхности, на которой была прикреплена, и падает. Для установки радиостетоскопов в местах, физический доступ к которым невозможен, используются специальные бесшумные пистолеты или арбалеты, стреляющие “стрелами - радиозакладками”. Стрела с миниатюрной радиозакладкой, в удароустойчивом исполнении, надежно прикрепляется к поверхностям из любого материала: металла, дерева, пластмассы, стекла, камня, бетона и т.п. при выстреле с расстояния до 25 м.

В период строительства в стены здания могут быть встроены радиостетоскопы длительного времени действия, оснащенные системой дистанционного управления. Время работы таких устройств может составлять в режиме дежурного приема более 10 лет, а в режиме передачи – более 6 месяцев.

Для исключения несанкционированного доступа к информации по виброакустическим каналам утечки информации, необходимо определить элементы помещения, через которые может возникнуть утечка. Можно выделить следующие типовые конструкции, по которым передаются речевые сигналы:

В акустическом сигнале это - несущие стены зданий, перегородки, перекрытия зданий, окна, двери, вентиляционные воздуховоды;

В вибрационном канале это - стены и перегородки, перекрытия, оконные рамы, дверные коробки, трубопроводы, короба вентиляции. Это окна, двери, батареи, телефонный и электрический кабель.

 Краткое описание содержимого комнаты.

Заявляемая категория объекта:

Этаж: .....2

Площадь (кв. м), высота потолков (м): каб. - 48 м2, (6\*8 м), h - 3,30 м

- подвесной (воздушный зазор) потолок гипсолитовый, зазор h - 0,3 м

Перекрытия (потолок, пол), толщина (мм): железобетонные перекрытия

Стеновые перегородки: бетон толщина 50 мм

Стены наружные:кирпичные

- толщина (73см)

- кирпич керамический пустотелый

- экранирование и штукатурка: присутствует

- другие материалы: с внутренней стороны стены отделаны под «евростандарт»

**Окна:**

- размер проема: .....200\*80 см

- количество проемов: .....3

- наличие пленок (назначение, тип, марка) .....отсутствуют

- тип окна (с двойным утолщенным стеклом): толщина стекла 6 мм (ОРС 18-15 В)

**Двери** :

- размер проема: одностворчатые 220\*90 см

- двери: 220\*90 см одностворчатые

- тип: легкая одинарная деревянная без уплотнений, замок электронный

**Описание смежных помещений:**

-назначение, характер проводимых работ: сверху: бухгалтерия, отдел кадров, север - коридор, юг – дорога к зданию, запад - приемная, восток – внешняя стена.

-наличие в них технических средств ..... передачи и обработки данных: ПЭВМ, телефоны.

**Система электропитания (освещение):**

- сеть: 220 В / 50 Гц

- тип светильников и их количество: галогеновые потолочные светильники (6 шт.)

**Система заземления:** имеется

Системы сигнализации (тип): имеется: пожарная (фотооптические детекторы) - 2 шт., охранная (акустические детекторы) - 6 шт.

Система вентиляции (тип): приточно-вытяжная, с мех. побуждением, проем 250\*160 мм

**Система отопления:**

-центральное водяное: водяное, три стояка, проходящие транзитом снизу вверх

- наличие экранов на батареях: декоративное укрытие

 **Телефонные линии:**

- количество и тип ТА: .....2 шт., (Voice Coder-2400- 1 шт), Panasonic - беспроводной 900 МГц )

- городская сеть 1 шт., два параллельных аппарата (обычный и беспроводной)

- тип розеток: евророзетка.

- тип проводки: двухпроводные линии, «хлорка»

**Оргтехника:** ПЭВМ в полной конфигурации - 1 шт., проектор 1шт.

* **Описание обстановки вокруг объекта:**
* Объект расположен в ЖД районе города, окружен с трех сторон постройками различного назначения и ведомственной принадлежности, с 4-той стороны дорогой со светофором и трамвайной линией. Слева от объекта расположено одноэтажное здание, в котором размещен линейный отдел милиции. Расстояние между зданиями составляет около 10-20 м. Справа от объекта на расстоянии 30-35 м расположен пятиэтажный жилой дом. С входной стороны здания на расстоянии 50 м с проходящей дорогой между зданием, расположено семейное 4-х этажное здание семейного общежития

Схематический план объекта защиты:

10

11

5

9

7

61

8

41

31

2

1

1.Телефонные аппараты (обычный и беспроводной).

2.ПК.

3.Стол под рабочую технику

4.Кресло, место руководителя.

5.Сканер.

6.Факс.

7.Стол для совещаний.

8. Плакат для проектора.

9.Окно.

10.Проектор

11.Вх.дверь.

##

## 4.3.2 Определение нормы блокирования

Контролируемая зона – это территория объекта, на которой исключено неконтролируемое пребывания лиц не имеющие постоянного или разового доступа.

Контролируемая зона может ограничиваться периметром охраняемой территорией частично, охраняемой территорией охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнаты, кабинеты, в которых проводятся закрытые мероприятия. Контролируемая зона может устанавливаться больше чем охраняемая территория, при этом обеспечивающая постоянный контроль за не охраняемой частью территории. Постоянная контролируемая зона – это зона границы, которой устанавливается на длительный срок. Временная зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера.

Первой категории универсального объекта, требуется 50 метров контролируемой зоны. Второй категории объекта, требуется 30 метров, а третей категории объектов требуется 15 метров контролируемой зоны.

Также требуется определенный размер контролируемой зоны для разных типов специализированных объектов **таблица №1.**

При выборе мест для размещения объектов необходимо строго

соблюдать требования по обеспечению размера КЗ.

Требования размеров КЗ по защите перехвата побочных электромагнитных излучений.

**Таблица№1**

|  |  |
| --- | --- |
| Тип СО | КЗ (м) |
| Телефон.ап | 250 |
| ПК | 100 |
| окно | 50 |
| Стол | 45 |
| Вх.дверь | 40 |
| Факс | 35 |
| Тел.розетка | 30 |
| Место.рук | 20 |
| проектор | 15 |

Возможности по перехвату информации будут во многом определяться затуханием информационного сигнала в ограждающих конструкциях и уровнем внешних шумов в месте установки контактного микрофона (табл. 2).

**Таблица№2**

|  |  |
| --- | --- |
| **Наименование конструкции** | **Затухание сигнала, дБ** |
| Стена в 0,5 кирпича | 40 – 48 |
| Стена в 1 кирпич | 44 – 53 |
| Стена в 2 кирпича | 46 – 60 |
| Стена из железобетонных блоков (100 мм) | 40 – 50 |
| Стена из железобетонных блоков (200 мм) | 44 – 60 |
| Окно одинарное (4 мм) | 22 – 28 |
| Окно двойное (4 мм) | 32 – 48 |
| Дверь типовая | 23 – 34 |
| Дверь металлическая, облицованная | 32 – 48 |

Качество добываемой средствами акустической разведки речевой информации по прямому акустическому и виброакустическому каналам вполне достаточно для составления подробной справки о содержании перехваченного разговора (табл. 3)

**Таблица№3**

|  |  |  |
| --- | --- | --- |
| **Место установки датчика аппаратуры акустической разведки** | **Вид принимаемого сигнала** | **Словесная разборчивость, %** |
| За окном на расстоянии 1,0 - 1,5 м от оконной рамы при закрытой форточке | Прямой акустический | 67 – 80 |
| За окном на расстоянии 1,0 - 1,5 м от оконной рамы при открытой форточке | Прямой акустический | 97 – 98 |
| На оконной раме или внешнем оконном стекле при закрытой форточке | Виброакустический | 71 – 80 |
| За дверью (без тамбура) | Прямой акустический | 91 – 97 |
| За перегородкой из материалов типа гипсолит, асбестоцемент | Прямой акустический | 71 – 87 |
| На перегородке из материалов типа гипсолит, асбестоцемент | Виброакустический | 84 – 95 |
| На железобетонной стене | Виброакустический | 80 – 98 |
| В воздуховоде (6 - 8 м от ввода) | Прямой акустический | 87 – 95 |
| На трубопроводе (через этаж) | Виброакустический | 95 – 97 |

По конструкции помещения, можно сделать вывод, что через монолитные бетонные стены информацию считать невозможно. Но стеновые перегородки, межкомнатные двери, системы отопления, пожаротушения и система вентиляции подлежат блокированию. Так же информацию можно считать через канал радиовещания, телефонную линию, электрическую розетку. Через окна можно снять информацию электронным стетоскопом.

## 4.3.3 Меры по блокированию ТКУИ

Сущность защитных мероприятий сводится к перекрытию возможных каналов утечки защищаемой информации, которые появляются в силу объективно складывающихся условий ее распространения и возникающей у конкурентов заинтересованности в ее получении. Каналы утечки информации достаточно многочисленны. Они могут быть как естественными, так и искусственными, т.е. созданными с помощью технических средств.

##

## 4.3.3.1 Средства и системы защиты

**Возможные каналы утечки информации**

##### Рассмотрим возможные каналы утечки информации и несанкционированного доступа к ресурсам, которые могут быть использованы противником в данном помещении, а также возможную защиту от них. Анализ представленных материалов показывает, что в настоящее время номенклатура технических средств коммерческой разведки весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной.

##### Решение подобной задачи возможно только с использованием профессиональных технических средств и с привлечением квалифицированных специалистов. (табл.4)

**Таблица№3** Основные методы и средства несанкционированного получения информации и возможная защита от них.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N п/п**  | **Действие человека (типовая ситуация)**  | **Каналы утечки информации**  | **Методы и средства получения информации**  | **Методы и средства защиты информации**  |
| 1  | Разговор в помещении  | * Акустика
* Виброакустика
* Гидроакустика
* Акустоэлектроника
 | * Подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система
* Стетоскоп, вибродатчик
* Гидроакустический датчик
* Радиотехнические спецприемники
 | Шумовые генераторы, поиск закладок, защитные фильтры, ограничение доступа  |
| 2  | Разговор по проводному телефону  | * Акустика
* Электросигнал в линии
* Наводки
 | * Аналогично п.1

Параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка | * Аналогично п.1
* Маскирование, скремблирование, шифрование
* Спецтехника
 |
| 3  | Разговор по радиотелефону  | * Акустика
* Электромагнитные волны
 | * Аналогично п.1
* Радиоприемные устройства
 | * Аналогично п.1
* Аналогично п.2
 |
| 4  | Документ на бумажном носителе  | Наличие  | Кража, визуально, копирование, фотографирование  | Ограничение доступа, спецтехника  |
| 5  | Изготовление документа на бумажном носителе  | * Наличие
* Паразитные сигналы, наводки
 | * Аналогично п.4
* Специальные радиотехнические устройства
 | * Аналогично п.1
* Экранирование
 |
| 6  | Почтовое отправление  | Наличие  | Кража, прочтение  | Специальные методы защиты  |
| 7  | Документ на небумажном носителе  | Носитель  | Хищение, копирование, считывание  | Контроль доступа, физическая защита, криптозащита  |
| 8  | Изготовление документа на небумажном носителе  | * Изображение на дисплее
* Паразитные сигналы, наводки
 | * Визуально, копирование, фотографирование
* Специальные радиотехнические устройства
 | Контроль доступа, криптозащита  |
| 9  | Передача документа по каналу связи  | Электрические и оптические сигналы  | Несанкционированное подключение, имитация зарегистрированного пользователя  | Криптозащита  |
| 10  | Производственный процесс  | Отходы, излучения и т.п.  | Спецаппаратура различноного назначения, оперативные мероприятия  | Оргтехмероприятия, физическая защита  |

Таким образом, основным направлением противодействия утечке информации является обеспечение физической(технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

#

# 4.4 Комплексная система защиты информации объекта защиты

Комплексная система защиты информации объекта защиты состоит:

1) Блокирование технических каналов утечки информации;

2) Исключение внешних и внутренних угроз;

3) Дополнительные меры.

Основными причинами утечки информации являются:

• несоблюдение персоналом норм, требований, правил эксплуатации АС;

• ошибки в проектировании АС и систем защиты АС;

• ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае лицом, совершающим несанкционированные дейст­вия, двигают личные побудительные мотивы. Причины утечки информа­ции достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922-96 рассматриваются три вида утечки информации:

• разглашение;

• несанкционированный доступ к информации;

• получение защищаемой информации разведками (как отечественны­ми, так и иностранными).

##

## 4.1.1 Политика безопасности объекта защиты

Политика безопасности – это, в первую очередь, обеспечение информационной безопасности, которая включает в себя защиту от воздействия внешних и внутренних угроз.

Для защиты персональных данных по виброакустическому каналу утечки информации используем следующие действительные меры.

**Вибрационные**

Перехват акустических сигналов

\* электронными стетоскопами

\* стетоскопам и, комплексированными с устройствами передачи информации по радиоканалу

\* стетоскопами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн

\* стетоскопами 2 комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям и т.п.

##

## 4.1.1.1 Решение по технической защите информации

Утечка информации по вибро-акустическим каналам может произойти при проведении совещаний и переговоров в помещении для селекторного слушания. Чтобы этого избежать, примем следующие меры:

1. Перед началом совещания нужно проверить помещение портативным многофункциональным прибором СРМ-700 или спектральным кореллятором OSCOR OSC-5000.

### 2. Использовать приборы виброакустической защиты SI-3001 для исключения утечки через окна, две стеновые перегородки, а так же через двери и другие опасные зоны.

 3. Перед началом совещания нужно снять со стен зеркала, картины, планшеты и т.п.

 4. В батареи желательно вставить резиновые прокладки между комнатами.

 5. Перед началом совещания в помещении для переговоров также необходимо потребовать оставить в своих рабочих кабинетах все сотовые и радиотелефоны.

##

## 4.1.2 Вывод об адекватности принятых мер

Как правило, у потребителя, столкнувшегося с задачей реализации виброакустической защиты информации, возникает проблема выбора системы для ее обеспечения. При этом большинство покупателей руководствуется следующими критериями: низкая цена, минимальные габариты и количество вибропреобразователей, подключаемых к генератору. К сожалению, при подобном подходе не всегда удается построить высококачественную систему защиты. Эффективность любой системы виброакустического зашумления обычно зависит от следующих основных параметров:

* коэффициент полезного действия (КПД) вибропреобразователей;
* возможность регулировки спектра помехового сигнала в октавных полосах;
* наличие системы контроля эффективности работы.

Таким образом, итоговый уровень паразитных акустических помех во многом зависит от правильности настройки (регулировки) системы наряду с ее правильно выбранной конфигурацией. Контроль эффективности работы позволяет осуществлять наблюдение за выполнением норм по защите помещения при работе приборов виброакустического зашумления. Это обеспечивается установкой разветвленной системы измерения уровня сигнала на ограждающих конструкциях. Использование данных систем гарантирует решение следующих задач:

* контроль работоспособности преобразователей и системы в целом;
* контроль выполнения требований по защите помещений.

Если первая задача не предполагает серьезных требований к системе контроля и на рынке уже представлены приборы, в которых она нашла реализацию, то для решения второй задачи необходимо применение точных измерительных устройств (шумомеров) 0-1 класса точности, что значительно повышает стоимость системы. Рассмотрев основные особенности систем виброакустического зашумления, следует отметить и их дополнительных функций, к которым относятся:

* активация системы по голосу (по наличию сигнала);
* модульная реализация системы.

# 5. Результаты курсовой работы

Результатом курсовой работы является законченное решение по защите информации обрабатываемой на объекте защиты включающее в себя:

* План объекта защиты включая взаимное расположение соседних помещений и (или) зданий (чертеж);
* Перечень информации ограниченного доступа;
* Перечень угроз информации ограниченного доступа;
* Должностные инструкции работников по обработке информации с ограниченным доступом;
* Матрица доступа;
* План объекта защиты с определенными разведопасными направлениями (чертеж);
* Перечень средств и систем используемых для защиты информации;
* Политика безопасности.

#

# Заключение

В данной курсовой работе рассмотрена комплексная система защиты информационных ресурсов объекта – помещения для презентаций и совещаний ответственных лиц регионального отдела. Изложены основные сведения, которые требуются для организации такой защиты. Среди них и теоретическая база, и практические решения информационной безопасности такие как: выявление каналов утечки информации и их защита, способов несанкционированного доступа и их предотвращение, модели угроз и приемы их реализации.

Способы защиты информационных ресурсов должны представлять собой целостный комплекс защитных мероприятий, которые должны быть тщательно спланированы. Главной целью злоумышленника является получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т.д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации.

 Главной целью данной курсовой работы была разработка комплексной системы защиты информации через виброакуститеские каналы утечки информации, эта работа выполнена.

# Список литературы

1. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие (под общей редакцией Реймана Л.Д.) М.: НТЦ «ФИОРД-ИНФО», 2002г.-272с.
2. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебное пособие-М.: Радио и связь, 2001г.-368с.
3. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных /П.Ю.Белкин, О.О.Михальский, А.С. Першаков и др.- М.: Радио и связь, 1999.
4. Хисамов Ф.Г. Макаров Ю.П. Оптимизация аппаратных средств криптографической защиты информации //Системы безопасности. -2004. – февраль-март №1 (55). –стр.108.
5. WEB-сайт www.razvedka.ru
6. www.confident.ru