МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ЭКОНОМИКИ И ПРЕДПРИНИМАТЕЛЬСТВА

Курсовая работа

по теории информационной безопасности и методам защиты информации

На тему

**"Каналы утечки и методы несанкционированного доступа к конфиденциальной информации на предприятии"**

Работу выполнил студент гр. ЭиП-252 Зуев А.И.

Работу проверил Доцент кафедры

Информационная безопасность.

Верхорубов В.В.

Челябинск 2004

Содержание

Аннотация

Введение

1. Защищаемая информация

2. Описание каналов утечки информации

3. Краткая характеристика предприятия ОАО "Челябгипромез"

Заключение

Список использованной литературы

# Аннотация

Данную работу можно разделить на две части:

В первой части работы рассматриваются каналы утечки информации, методы и способы съема информации через каждый рассмотренный канал утечки информации, а также рассматриваются методы и способы защиты информации применительно к конкретному каналу утечки информации.

Во второй части работы приводится краткая характеристика предприятия ОАО "Челябгипромез", рассматриваются возможные каналы утечки информации на данном предприятии, а также рассматриваются методы и способы защиты информации.

В конце работы подводится итог уровня общей защищенности предприятия ОАО "Челябгипромез".

# Введение

Владение информацией во все времена давало преимущества той стороне, которая располагала более точной и обширной информацией, тем более, если это касалось информации о своих соперниках.

"Знать наперед намерения противника - это, по сути, действовать как Бог!" - в свое время изрек стратег китайской мудрости Сунь-цзы. Противниками могут выступать и конкурент, и опытный профессионал, и мощная организованная структура. Взаимоотношения при этом могут быть вполне цивилизованными и джентльменскими, а могут оказаться до крайности безжалостными и неэтичными. Мощь интеллекта не аналог морали, так же как не стыкуется с моралью истинный профессионализм.

Рассекречивание закрытой информации какой-либо организации, может привести как к небольшим финансовым потерям, так и к полному развалу организации. Следовательно, возникает острая необходимость защиты закрытой информации.

# 1. Защищаемая информация

Отметим, что законом защищается только документированная информация. Федеральный Закон "Об информации, информатизации и защите информации" определяет это понятие следующим образом:

"Документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать".

Документирование информации проводится по строго определенным правилам. Основные из них изложены в ГОСТ 6.38-90 "Система организационно-распорядительной документации. Требования к оформлению документов.", ГОСТ 6.10.4-84 "Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники".

Закон выделяет три категории такой информации:

* информация, составляющая государственную тайну;
* персональные данные;
* информация, составляющая коммерческую тайну.

Информацией первой категории владеет само государство и, естественно, именно оно выдвигает требования по ее защите и контролирует их выполнение. Соответствующие положения закреплены в Законе Российской Федерации "О государственной тайне", принятом в 1993 году. Следует знать, что нарушение этих требований влечет за собой применение санкций, предусмотренных Уголовным кодексом.

Собственниками второй категории информации являемся мы с Вами, так как эта информация затрагивает нашу с Вами личную жизнь. Однако, понимая степень значимости этой информации и ее роль в обеспечении безопасности каждой отдельно взятой личности, государство взяло ее под свой патронаж и рассматривает ее защиту, как одну из своих важных задач.

Информацией третьей категории владеют сами учреждения, и поэтому они вправе ей распоряжаться, а, следовательно, и выбирать степень ее защиты. Правда, применить какие-либо санкции в случае нарушения конфиденциальности возможно, только если предварительно были выполнены особые формальности, оговоренные Гражданским кодексом Российской Федерации.

Суть этих формальностей, изложенных в статье 139 Гражданского кодекса Российской Федерации, заключается в том, что, во-первых, информация должна иметь действительную или потенциальную коммерческую ценность, во-вторых, учреждению необходимо принять определенные меры по охране конфиденциальности и, в-третьих, все сотрудники, знакомые с этими сведениями, должны быть официально предупреждены об их конфиденциальности. При отнесении информации к категории "коммерческая тайна" следует руководствоваться положениями Гражданского кодекса Российской Федерации (статья 139), Федерального Закона "Об информации, информатизации и защите информации" (часть 3, статья 10) и Постановления Правительства Российской Федерации от 5 декабря 1991 года за номером 35 "О перечне сведений, которые не могут составлять коммерческую тайну".

Сведения, относимые к категории "коммерческая тайна", можно разделить на две группы:

* Научно-техническая и технологическая информация, связанная непосредственно с деятельностью учреждения, то есть конструкторская и технологическая документация, сведения об используемых материалах, описание методов и способов производства разрабатываемых изделий, специфический или уникальный программный продукт, перспективные планы развития или модернизации производства;
* Деловая информация о деятельности учреждения, то есть финансовая документация, перспективные планы развития, аналитические материалы об исследованиях конкурентов и эффективности работы на рынке товаров и услуг и т.п.

Чтобы отнесение к категории коммерческой тайны приобрело законную силу, оно должно быть оформлено в виде специального перечня, утвержденного руководителем учреждения. Только в этом случае можно говорить о придании конфиденциальной информации определенных вещных прав.

Более подробно все эти вопросы освещены в законопроекте "О коммерческой тайне", который уже более двух лет рассматривается Правительством и Федеральным собранием.

Нельзя не сказать и о том, что Гражданским кодексом Российской Федерации информация наделена правами товара. Она может представлять определенную ценность (даже не относясь к вышеперечисленным категориям), обмениваться, продаваться, дариться и т.п., поэтому, оценивая информацию с точки зрения важности ее защиты, следует учитывать и этот аспект.

# 2. Описание каналов утечки информации

Под каналами утечки информации понимаются методы и способы получения закрытой информации.

Каналы утечки информации подразделяются на следующие категории:

* Технические;
* Материально-вещественные;
* Легальные;
* Агентурные.

Рассмотрим каждый из каналов утечки информации более подробно.

**Технические каналы утечки информации**

Под техническим каналом утечки информации понимают способ получения информации с помощью технических средств.

Технические каналы утечки информации по физическим принципам можно классифицировать на следующие группы:

* **Акустические**

1. **Воздушные;**
2. **Вибрационные;**
3. **Электроакустические;**
4. **Оптико-электронные;**
5. **Параметрические;**

* **визуально-оптические;**
* **электромагнитные;**
* **компьютерные.**

***Акустические***

В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов, технические каналы утечки акустической информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

***Воздушные***

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными микропередатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т.п.

*Методы съема информации:*

* Установка радио-закладок в стенах и мебели;
* Съем информации по системе вентиляции;
* Съем информации с использованием диктофонов;
* Съем информации направленным микрофоном.

*Способы съема информации:*

* Подслушивание;
* Диктофон;
* Микрофон;
* Направленный микрофон.

*Методы и средства защиты информации:*

* Шумовые генераторы;
* Поиск закладок;
* Ограничение доступа.

***Вибрационные***

В вибрационных каналах (структурных каналах) утечки информации средой распространения акустических сигналов является конструкция зданий (стены, потолки, полы), трубы водо - и теплоснабжения, канализации и другие твердые тела.

*Методы съема информации:*

* За счет структурного звука в стенах и перекрытиях;
* Утечка по сети отопления, газо - и водоснабжения.

*Способы съема информации:*

* Вибродатчики.

*Методы и средства защиты информации:*

* Защитные фильтры.

***Электроакустические***

Электроакустические каналы утечки информации обычно образуются за счет преобразования акустических сигналов в электрические по двум основным направлениям: путем "высокочастотного навязывания" и путем перехвата через вспомогательные технические средства и системы.

Технический канал утечки информации путем "высокочастотного навязывания" образуется при несанкционированном контактном введении токов высокой частоты от ВЧ-генератора в линии, имеющие функциональные связи с элементами вспомогательных технических средств и систем, на которых происходит модуляция ВЧ-сигнала. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. С другой стороны, вспомогательные технические средства и системы могут сами содержать электроакустические преобразователи. К таким вспомогательным техническим средствам и системам относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Используемый в них эффект обычно называют "микрофонным эффектом".

*Методы съема информации:*

* Съем информации за счет наводок и "навязывания";
* Съем информации за счет использования "телефонного уха";
* Утечка по охранно-пожарной сигнализации.

*Способы съема информации:*

* Подключение к вспомогательным техническим средствам и системам (телефон, датчики пожарной сигнализации, громкоговорители ретрансляционной сети).

*Методы и средства защиты информации:*

* Использование специальных устройств;
* Отключение телефонных аппаратов от линии при ведении в помещении конфиденциальных разговоров;
* установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке;
* Использование метода "выжигания" закладных устройств или их блоков питания путем подачи в линию высоковольтных импульсов.

***Оптико-электронные***

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т.п., создается оптико-электронный (лазерный) канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие, как правило, в ближнем инфракрасном диапазоне и известные как "лазерные микрофоны". Дальность перехвата составляет несколько сотен метров.

*Методы съема информации:*

* Лазерный съем акустической информации с окон.

*Способы съема информации:*

* С помощью "лазерных микрофонов".

*Методы и средства защиты информации:*

* Звукоизоляция окон;
* Установка на стекла окон "виброгенераторов".

***Параметрические***

Параметрический канал утечки акустической информации образуется в результате воздействия акустического поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем, проводов, дросселей и т.п., что приводит к изменениям параметров сигнала, например, модуляции его информационным сигналом. Промодулированные высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами. Параметрический канал утечки акустической информации может быть создан и путем высокочастотного облучения помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых (добротность, частота и т.п.) изменяются по закону изменения акустического (речевого) сигнала.

*Методы съема информации:*

* Высокочастотный канал утечки в бытовой технике.

*Способы съема информации:*

* С помощью спец. оборудования.

*Методы и средства защиты информации:*

* Шумовые генераторы;
* Не устанавливать элементы высокочастотных генераторов (например: телевизор);
* Поиск закладок.

***Визуально-оптические***

Каналы утечки графической информации, реализуются техническими средствами. И предоставляют информацию в виде изображений объектов или копий документов, получаемых путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т.п. Для документирования результатов наблюдения проводится съемка объектов, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки, либо осуществляют видеосъемку из зданий расположенных по близости.

*Методы съема информации:*

* Наблюдение, фотографирование, видеосъемка объекта.

*Способы съема информации:*

* Съем информации с использованием видео-закладок;
* Использование закамуфлированной техники (фотоаппарата, видеокамеры);
* Наблюдение за объектом вне его зоны (из соседних зданий).

*Методы и средства защиты информации:*

* Поиск закладок;
* Экранировка помещения;
* Использование жалюзи или штор.

***Электромагнитные***

Для электромагнитных каналов утечки характерными являются побочные излучения:

Электромагнитные излучения элементов технические средства обработки информации.

Носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала.

Электромагнитные излучения на частотах работы высокочастотных генераторов технические средства обработки информации и вспомогательные технические средства и системы.

В результате воздействия информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты технических средств передачи информации.

Самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом.

Возможными причинами возникновения электрических каналов утечки могут быть:

Наводки электромагнитных излучений технические средства обработки информации.

Возникают при излучении элементами технические средства обработки информации информационных сигналов, а также при наличии гальванической связи соединительных линий технические средства обработки информации и посторонних проводников или линий вспомогательные технические средства и системы.

Просачивание информационных сигналов в цепи электропитания.

Возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в цепи заземления.

Образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания.

*Методы съема информации:*

* Утечка за счет побочного излучения терминала;
* Съем информации с дисплея;
* Утечка по цепям заземления;
* Утечка по трансляционной цепи и громко говорящей связи;
* Утечка по охранно-пожарной сигнализации;
* Утечка по сети электропитания.

*Способы съема информации:*

* электромагнитный датчик;

*Методы и средства защиты информации:*

* Экранирование.

***Компьютерные***

Этот уникальный электронной механизм для хранения и обработки информации имеется в каждой деловой организации. Более того, они зачастую связаны с внешним миром с помощью модемов и телефонных линий, выделенных сетей. Связь компьютера с внешним миром является каналом обмена, отправки и получения информации, благодаря которому организация может более оперативно работать, но данная связь также является каналом заполучения информации, которой обладает организация.

*Методы съема информации:*

* Программно-аппаратные закладки;
* Компьютерные вирусы, логические бомбы, троянские кони и т.п.;
* Подключение к удаленному компьютеру.

*Методы и средства защиты информации:*

* Использование сертифицированного ПО;
* Установка FireWall’ов;
* Использование антивирусов.

***Материально-вещественные каналы утечки информации***

К материально-вещественному каналу утечки информации относится

относится снятие информации непосредственно с носителя информации.

*Методы съема информации:*

* несанкционированное размножение, копирования или хищения носителей информации;
* Визуальный съем информации с дисплея или документов;
* Использование производственных и технологических отходов.

*Способы съема информации:*

* Наблюдение;
* Обработка мусора;
* Копирование документов;
* Хищение носителей информации.

*Методы и средства защиты информации:*

* Ограничение доступа;
* Использование "уничтожителей документов";
* Физическая защита.

***Легальные***

Под легальными каналами утечки информации понимается переработка открытой информации для выявления из нее закрытых сведений.

*Методы съема информации:*

* Литература;
* Периодические издание;
* Выведывание под благовидным предлогом информации у лиц, располагающих интересующей информацией;
* СМИ;
* Интернет.

*Методы и средства защиты информации:*

* Работа с персоналом;
* Постановления о неразглашении конфиденциальной информации;
* Фильтрация данных предоставляемых для опубликования.

***Агентурные***

Агентурные каналы утечки информации это использование противником тайных агентов для получения закрытой информации.

В данном канале утечки информации используются следующие методы:

* Внедрение своих агентов в организацию;
* Проведение беседы (анкетирования) с агентами находящимися (работающими) в организации;
* Вербовка агентов уже находящихся (работающих) в организации.

К вербовке агента необходимо подходить с психологической точки зрения. Необходимо понять характер агента, выявить его слабости и мотивы из-за которых он может выдать необходимую информацию. И в конечном счете с играть на его мотивах.

Личные мотивы выдачи информации

Так как всякий индивид в демонстрируемом поведении направляется определенными побуждениями, понимание таковых дает возможность подобрать к нему ключи и в итоге получить необходимые данные.

О мотивах некоего человека узнают путем его изучения, причем следует учитывать и степень выраженности (очень сильно, довольно сильно, слабо) этих побуждений.

Характерные мотивы выдачи индивидом информации и возможные пути их утилизации таковы:

1. Алчность. (Обещание или же предоставление денег и иных материальных ценностей);

2. Страх за себя. (Шантажирование, а порою и угроза либо факт грубого физического или утонченного психологического воздействия);

3. Страх за своих близких. (Явная угроза либо факт разнотипного насилия - в духе похищения, избиения, изнасилования, кастрации, "сажания на иглу", полного физического устранения);

4. Фактор боли. (Качественная пытка или угроза интенсивного болевого воздействия);

5. Сексуальная эмоциональность. (Ловкое подсовывание полового партнера и различной порнографии с перспективой "расслабления", шантажа или обмена);

6. Безразличие. (Четкая реализация депрессии, возникающей в результате инспирированных или спонтанных жизненных обстоятельств, а иной раз и в результате психофизической обработки объекта);

7. Внутренний авантюризм. (Предоставление шансов индивиду для ведения им своей игры);

8. Счеты с "системой" или организацией. (Умное использование идеологических разногласий и существующей неудовлетворенности объекта своим нынешним положением либо завтрашней перспективой);

9. Счеты с конкретными лицами. (Разжигание таких негативных чувств как месть, зависть и неприязнь с непреодолимым желанием нанести "врагу" определенный ущерб);

10. Национализм. (Игра на глубинном ощущении некоей национальной общности, ненависти, гордости, исключительности);

11. Религиозные чувства. (Пробуждение неприязни к "иноверцам" или же привязывание определенной ситуации к избранным доктринам исповедуемой религии);

12. Гражданский долг. (Игра на законопослушности);

13. Общечеловеческая мораль. (Игра на порядочности);

14. Подсознательная потребность в самоуважении. (Спекуляция на идеальных представлениях человека о самом себе);

15. Корпоративная (клановая) солидарность. (Игра на конкретной элитарности);

16. Явная симпатия к получателю или его делу. ("Резонирующая подстройка к объекту");

17. Тщеславие. (Провоцирование желания объекта произвести определенное впечатление, показать свою значимость и осведомленность);

18. Легкомыслие. (Приведение человека в беззаботнейшее состояние неосмотрительности и болтливости. К этому же можно отнести задействование "хронотопа" - явно повышенной доверчивости человека в некое время и в определенном месте ("случайный попутчик");

19. Угодливость. (Четкая реализация подсознательной (волевой) и осознанной (деловой и физической) зависимости объекта от получателя);

20. "Помешательство" на чем-либо. (Близкая возможность для коллекционера приобрести (или потерять) страстно желаемую вещь; игра на фобиях);

21. Нескрываемый расчет получить определенную информацию взамен. (Техники "баш на баш" или "вождение за нос");

22. Страстное стремление убедить в чем-либо, изменить отношение к чему-либо (или кому-либо), побудить к определенным действиям. (Методы "заглатывание наживки" и "обратной вербовки").

*Методы и средства защиты информации:*

* Работа с персоналом.

# 3. Краткая характеристика предприятия ОАО "Челябгипромез"

***Организационно-правовая форма деятельности и количество собственников.***

Открытое Акционерное Общество "Челябгипромез".

***Основные подразделения института:***

Главные инженеры проектов.

Бюро авторского надзора.

Творческая архитектурная мастерская.

Технический отдел.

Металлургический отдел.

Прокатный отдел.

Механико-технологический отдел.

Теплосиловой отдел.

Отдел газовый и защиты атмосферы.

Сантехнический отдел.

Отдел водного хозяйства.

Электротехнические отделы.

Отдел пожарной автоматики и связи.

Строительный отдел.

Отдел машиностроения.

Отдел генсмет и проектов организации строительства.

Бюро нормо-контроля и экспертизы.

Отдел изысканий.

Отдел выпуска проектов.

Отдел комплектации оборудования.

Отдел генпланов и транспорта.

Отдел САПР.

Бюро экономического анализа.

***Адрес***

Адрес юридический: 454090, РФ, г. Челябинск, пр. Ленина, 35

Адрес физический: 454090, РФ, г. Челябинск, пр. Ленина, 35

Адрес почтовый: 454090, РФ, г. Челябинск, пр. Ленина, 35

***Количество работающих, кадровый и национальный состав.***

920 чел. (92 г.);

800 чел. (94 г.);

490 чел. (96 г.).

Национальный состав разнообразен, но большинство рабочих русских.

***Характер продукции и*** *услуг.*

079900M: комплексное проектирование объектов черной металлургии и объектов других отраслей, гражданского строительства и объектов соцкультбыта (07.98)

030900M, 102500M: проведение инженерно-изыскательских работ в строительстве (07.98)

030900M, 102500M: разработка проектно-сметной документации промышленного и гражданского строительства, объектов соцкультбыта (07.98)

065200M, 102500M: разработка мероприятий по охране окружающей среды и территорий промышленной и социально-культурной сфер (07.98)

030900M: разработка технической документации по использованию вторичных минеральных и энергетических ресурсов (07.98)

030900M, 102500M: разработка документации и проведение комплектации оборудованием и материалами строящихся и реконструируемых объектов (07.98)

102500M: научно-техническая продукция и методические пособия для строительства (07.98)

102500M: ведение авторского надзора в строительстве (07.98)

102500M: обследование существующих объектов и сооружений и разработка рекомендаций (07.98)

011800M: внешнеэкономическая деятельность (07.98)

040200M: предпринимательская и посредническая деятельность (07.98)

***Наличие внешнеторговых связей.***

ОАО "ЧЕЛЯБГИПРОМЕЗ" разрабатывает некоторые проекты совместно с европейскими компаниями, которые работают на Российском рынке. Внешнеторговые связи отсутствуют.

***Наличие на предприятии сведений, составляющих государственную тайну.***

На предприятии “ЧЕЛЯБГИПРОМЕЗ” не содержатся сведения составляющих государственную тайну.

***Оснащенность управления и производства средствами СВТ, наличие специализированных подразделений, наличие локальной сети и её соединение с внешним миром.***

В институте “ЧЕЛЯБГИПРОМЕЗ” проведена локально-вычислительная сеть. ЛВС связана с внешним миром через глобальную сеть Internet. В институте стоит сервер, который выполняет также роль файл сервера. К нему подключена вся компьютерная сеть, и выход в Интернет осуществляется через данный сервер.

***Наличие самостоятельной АТС и корпоративных пользователей услугами мобильной связи.***

В институте имеется собственная мини-АТС (внутренние телефоны имеют 3-х значный номер).

***Характеристика строений***

административное здание повышенной этажности (пр. Ленина, 35) с общей рабочей площадью 13320 м2 (07.98). В связи с тем, что административное здание - повышенной этажности, верхние этажи данного строения могут представлять интерес для спецслужб.

отдельно стоящий двухэтажный блок с размерами в плане 30 х 18 м, на первом этаже располагается автогараж на 4 бокса, на втором спортзал (05.97)

У "Челябгипромеза", также имеется база отдыха с участком 2,8 га (05.97)

***Способ охраны, оснащенность охранных подразделений и оборудование инженерно-техническими средствами охраны зданий объекта.***

В институте действует контрольно пропускной режим. В здание института имеется три входа: Главный вход, через здание магазина "Эльдорадо", через автомобильную стоянку.

У главного входа находится два охранника, у входа через здание магазина "Эльдорадо", у въезда на стоянку и у входа в здание со стоянки находится по одному охраннику.

В рабочее время по зданию ходит один патрулирующий охранник.

В здании также ведется видеонаблюдение.

Охранники не вооружены, не имеют раций.

Наличие у охранников лицензии необязательно.

Каналы утечки информации на ОАО "Челябгипромез"

Утечка информации по *материально-вещественному каналу* "перекрыта", так как на предприятии действует контрольно пропускной режим, а следовательно в здании предприятия отсутствуют посторонние лица.

Рассмотрим *технические* каналы утечки информации.

*Акустический канал* утечки информации:

*Воздушные*

* Установка радио-закладок в стенах и мебели;
* Съем информации с использованием диктофонов;
* Съем информации направленным микрофоном.

Отметим, что съем информации с помощью направленного микрофона возможна только с нижних этажей здания. Так как здание предприятия повышенной этажности, а близ лежащие здания с которых возможно производить съем информации данным методом гораздо ниже чем здание предприятия.

*Вибрационные*

* За счет структурного звука в стенах и перекрытиях;
* Утечка по сети отопления, газо- и водоснабжения.

Для реализации данного метода необходимо проникновение в здание и установка специального оборудование. В связи с контрольно-пропускным режимом и видеонаблюдением действующим на предприятии данная группа акустического канала утечки информации затруднительна.

*Электроакустические*

* Съем информации за счет наводок и "навязывания";
* Съем информации за счет использования "телефонного уха";
* Утечка по охранно-пожарной сигнализации.

Для реализации данных методов также необходимо проникновение в здание и установка спец. Оборудования. Что предотвращено контрольно-пропускным режимом и видеонаблюдением установленных на предприятии.

*Оптико-электронные*

* Лазерный съем акустической информации с окон.

Как и в случае с воздушным каналом утечки информации съем информации данным методом возможен только с нижних этажей здания предприятия. Так как здание предприятия повышенной этажности, а близ лежащие здания с которых возможно производить съем информации данным методом гораздо ниже, чем здание предприятия.

По мимо акустического канала утечки информации в технических каналах также существуют и другие каналы:

*Визуально-оптические*

* Наблюдение, фотографирование, видеосъемка объекта.

Для съема информации через визуально-оптический канал утечки, необходимо либо проникнуть в здание предприятия, либо осуществлять видео/фото съемку с близ лежащих домов. Проникновение в здание посторонних лиц пресекается физической защитой (охрана, КПП, видеонаблюдение). А съем информации по визуально-оптическому каналу утечки возможен только с нижних этажей здания предприятия. Так как здание предприятия повышенной этажности, а близ лежащие здания с которых возможно производить съем информации данным методом гораздо ниже, чем здание предприятия.

*Компьютерные*

* Программно-аппаратные закладки;
* Компьютерные вирусы, логические бомбы, троянские кони и т.п.;
* Подключение к удаленному компьютеру.

Возможна утечка информации через данный канал. Так как компьютеры предприятия имеют связь с внешним миром через сервер установленный на предприятии. Следовательно, возможно "проникновение" в компьютерную сеть с удаленного компьютера. Хотя и используется специальное программное и аппаратное обеспечение (антивирусы, firewall’ы), вероятность проникновения в компьютерную сеть все же остается, так как все время совершенствуются и находятся новые пути обхода защитного программного и аппаратного обеспечения.

*Агентурные*

* Вербовка агентов;
* Внедрение агентов.

Полностью защититься от этого канала утечки информации невозможно (если конечно не уволить всех рабочих). Учитывая, что на "Челябгипромезе" работает около 490 человек различной национальной принадлежности, контролировать данный канал утечки информации особенно сложно. Для уменьшения вероятности утечки информации через данный канал, необходимо разграничить доступ персонала к закрытой информации.

*Легальные*

* Литература;
* Периодические издание;
* Выведывание под благовидным предлогом информации у лиц, располагающих интересующей информацией;
* СМИ;
* Интернет.

Для предотвращения утечки информации через данный канал, необходима фильтрация данных предоставляемых для опубликования. Также необходимо разграничение доступа к защищаемой информации, например установление контрольно-пропускного режима. На рассматриваемом предприятие "Челябгипромез" реализован контрольно-пропускной режим, а также ведется видеонаблюдение, что предотвращает несанкционированное проникновение в архив предприятия.

# Заключение

Рассмотрев каналы утечки информации на предприятии ОАО "Челябгипромеза", можно сделать вывод, что предпринятые руководством меры по обеспечению информационной безопасности, в действительности способны противостоять лишь недостаточно опытным в данной среде лицам, покушающимся на закрытую информацию. Это связано с тем, что установка видеонаблюдения и контрольно-пропускного режима недостаточно для реализации хорошей информационной безопасности. Многие каналы утечки информации блокируются благодаря высокой конструкции здания. Хорошо "закрыт" компьютерный канал утечки информации, благодаря использованию специального программного и аппаратного обеспечения. Но существуют и другие каналы утечки информации, которые не защищены должным образом. При организации информационной безопасности необходимо учитывать, что *Защита информации* - это комплекс мероприятий, направленных на обеспечение информационной безопасности. Рассматривая "Челябгипромез" можно сказать, что при обеспечении на этом предприятии информационной безопасности не было учтено, что защита информации это комплексная процедура, и имеет смысл только при всесторонней защите.

# Список использованной литературы

1. В.И. Ярочкин "Безопасность информационных систем" М.: Ось-89, 1996
2. Роман Ронин "СВОЯ РАЗВЕДКА Практическое пособие" Минск: Харвест, 1997
3. Шиверский А.А. Защита информации: проблемы теории и практики. Юрист, 1996. - 112 с.5 - 7357-0108-8
4. Алексенцев А.И. "Безопасность информационных технологий" // 2000, №3.