**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ**

**Кафедра радиотехнических систем**

**РЕФЕРАТ**

**На тему:**

**«Группы опасных факторов. Внешние и внутренние источники угроз. Угроза информационным ресурсам»**

**МИНСК, 2008**

**1. Понятие «Угроза безопасности». Группы опасных факторов**

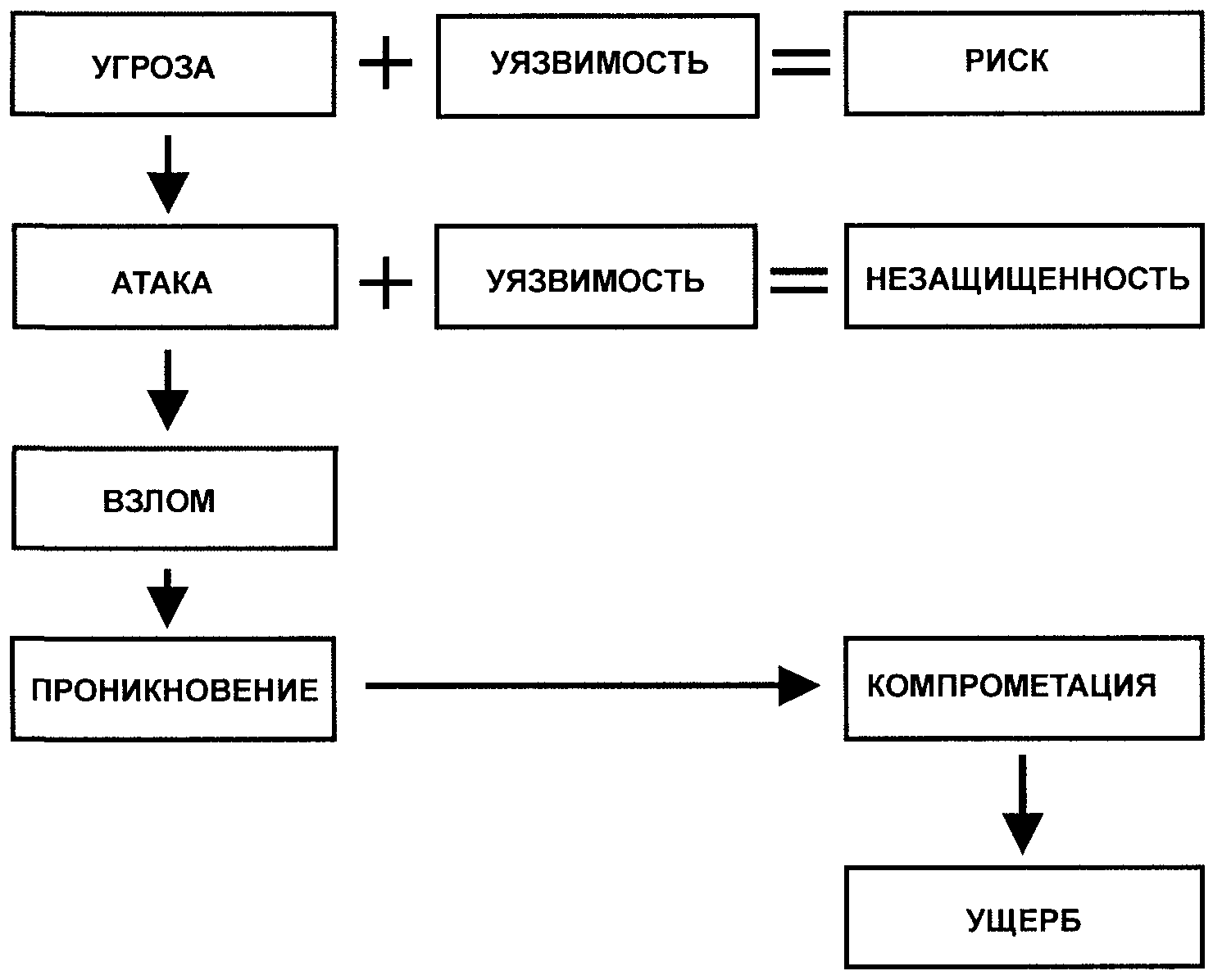
**Угроза безопасности** – потенциальное нарушение безопасности, любое обстоятельство или событие, которое может явиться причиной нанесения ущерба (защищаемому ресурсу) предприятию.

Угрозы можно классифицировать по различным основаниям и измерять в количественных параметрах. Возможны следующие типы угроз: экономические, социальные, правовые, организационные, информационные, экологические, технические и криминальные.

Рассмотрим механизм осуществления угрозы.

Источники угроз:

Потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности



**Уязвимость –** это присущие предприятию причины обусловленными особенностями хранения, использования, транспортировки, охраны и защиты ресурсов, приводящие к нарушению безопасности конкретного ресурса**.**

**Атака –** реализация угрозы.

**Ущерб –** невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. (материальный, физический, моральный).

**2.** **Внешние и внутренние источники угроз. «Модель» нарушителя.**

В любом рассматриваемом времени и месте существует ряд факторов, которые каким-либо образом влияют на вероятность возникновения и возможность осуществления угроз.

Портрет потенциального НАРУШИТЕЛЯ безопасности информационного ресурса может быть представлен следующим образом: Нарушитель – это лицо, по ошибке, незнанию или осознанно предпринявшее попытку выполнения запрещенных операций и использующее для этого различные возможности, методы и средства.

Уровни технической оснащенности нарушителя и его знаний о физических принципах работы систем охраны, установленных на объекте, определяют возможность и время, необходимое ему на преодоление средств инженерной защиты и обход сигнализационной техники.

Наиболее вероятными путями физического проникновения "нарушителя" в здание являются:

* через двери и окна первого этажа;
* по коммуникационным и техническим проемам подвала или цокольного этажа;
* с крыши через окна или другие проемы верхних этажей;
* путем разрушения ограждений (разбивание стекол, пролом дверей, решеток, стен, крыши, внутренних перегородок, пола и т.п.).

Рассматривают две группы способов реализации угроз (враждебных действий) - контактные, бесконтактные.

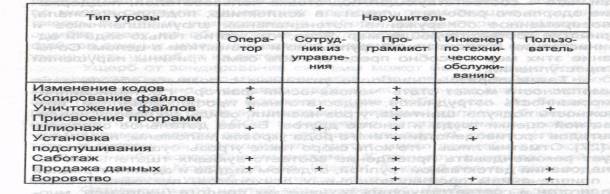
Способы проникновения на объект, в его здания и помещения могут быть самые различные (это описано во многих литературных источниках), например:

* разбитие окна, витрины, остекленной двери или других остекленных проемов;
* взлом (отжатие) двери, перепиливание (перекус) дужек замка и другие способы проникновения через дверь;
* пролом потолка, подлежащего блокировке;
* пролом капитального потолка, не подлежащего блокировке;
* пролом стены, подлежащей блокировке;
* пролом капитальной стены, не подлежащей блокировке;
* пролом (подкоп) капитального пола, не подлежащего блокировке;
* пролом (подкоп) пола, подлежащего блокировке;
* проникновение через разгрузочный люк;
* проникновение через вентиляционное отверстие, дымоход или другие строительные коммуникации;
* проникновение подбором ключей;
* оставление нарушителя на объекте до его закрытия;
* свободный доступ нарушителя на объект в связи с времен­ным нарушением целостности здания из-за влияния природно-техногенных факторов или в период проведения ремонта;
* проникновение через ограждение (забор, сетку, решетку), ис­пользуя подкоп, перелаз, разрушение, прыжок с шестом и т.д.

Каждый тип нарушителей (неподготовленный, подготовленный, квалифицированный) будет осуществлять проникновение на объект по разному - менее или более грамотно используя различные условия, способствующие проникновению, как то:

* взрыв;
* пожар (поджог);
* разбойное нападение;
* наводнение;
* химическое заражение;
* общественные беспорядки;
* отключение электроэнергии на объекте, в районе, городе;
* постановка нарушителем помех ТСО на объекте;
* постановка нарушителем помех в канале связи объекта с охраной;
* предварительный вывод из строя ТСО на объекте;
* предварительный вывод из строя канала связи объекта с охраной;
* предварительный сговор нарушителя с персоналом объекта;
* предварительный сговор нарушителя с персоналом службы охраны объекта;
* создание и использование многих и многих других условий для проникновения на охраняемый объект, например: использование дрессированных животных и птиц, специальных технических средств обхода ТСО, специальных технических средств для предварительного изучения объекта и т.д.

**Модель нарушителя информационной безопасности может** быть дополнена некоторыми показателями, определяемыми особенностями человеческого характера. Сотрудники охраняемого объекта, участвующие в процессах движения информации, могут быть возможными нарушителями. Типы угроз компьютерной информации и возможные нарушители представлены в таблице.



Любой нарушитель для реализации своих замыслов руководствуется определенной мотивацией и намерениями, владеет совокупностью знаний, умений и навыков (способов) совершения противоправных действий с применением технических средств, имеет в своем распоряжении соответствующие технические средства. Он знает систему защиты информации на объекте или имеет Возможность доступа к конкретным информационным ресурсам, сам выбирает время и место предполагаемого нарушения.

3. Угрозы персоналу

Правовое положение работника на предприятии определяется положениями Конституции РБ, а также условиями контракта (трудового соглашения) и организационно-распорядительными документами, действующими на данном предприятии, в т.ч. и в части обеспечения безопасности на своем участке работы. Работодатель обязан предпринять меры для защиты работника от возможных угроз его здоровью, жизни, интересам, а работник, в свою очередь – добросовестно выполнить обязательства, взятые на себя при оформлении контракта во время приема на работу.

Угрозы Персоналу (человеку) могут быть выражены явлениями и действиями такими как:

1) Стихийные бедствия;

2) Вредные условия труда; попытки внесения изменений в технологические процессы производства, с целью подготовки и совершения технологических аварий; техногенные аварии;

3) Психологический террор, угрозы, компромат, распространение ложной информации (то ли он украл, то ли у него украли), запугивание, шантаж, вымогательство;

4) Нападение, с целью завладения денежными средствами, ценностями, сведениями конфиденциального характера и документами;

5) Внесение опасных для здоровья изменений в окружающую среду (радиоактивное, химическое, бактериологическое заражение и т.п.);

8) Убийства, сопровождаемые насилием, издевательствами и пытками и другие.

Способы осуществления угроз персоналу разнообразны и зависят от исполнителя угрозы, его подготовки и оснащенности.

**4. Угрозы материальным ресурсам**

Ценным ресурсам предприятия с физической формой существования могут угрожать:

* Стихийные бедствия;
* Пожар;
* Хищения – совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества;
* Повреждение – изменение свойств имущества, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становиться полностью или частично непригодным для целевого использования. Повреждение осуществляется с помощью поджогов, взрывов, обстрелов из огнестрельного оружия и другими способами ограждений, входных дверей, ворот, решеток, витрин, и т.п.; транспортных средств, технологического транспорта и оборудования; средств и систем связи и сигнализации; систем жизнеобеспечения предприятия.
* Уничтожение - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводится в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.
* Заражение радиоактивными, химическими, бактериологическими веществами;
* Пикетирование, блокирование входов, вторжение, захват и другие.

Способы осуществления угроз ценным ресурсам, существующим в физической форме, также разнообразны и зависят от исполнителя угрозы, его подготовки и оснащенности.

**5. Угрозы информационным ресурсам**

5.1. Классификация угроз информационным ресурсам.

Угрозы информационным ресурсам можно в общем случае классифицировать:

1). По цели реализации угроз:

* угрозы конфиденциальности:
* хищение (копирование) информации и средств ее обработки (носителей);
* утрата (неумышленная потеря, утечка) информации и средств ее обработки (носителей);
* угрозы доступности:
* блокирование информации;
* уничтожение информации и средств ее обработки (носителей);
* угрозы целостности:
* модификация (искажение) информации;
* отрицание подлинности информации;
* навязывание ложной информации, обман

При этом:

Хищение и Уничтожение информации понимается аналогично по применению к материальным ценным ресурсам. Уничтожение компьютерной информации – стирание информации в памяти ЭВМ.

Копирование информации – повторение и устойчивое запечатление информации на машинном или ином носителе.

Повреждение – изменение свойств носителя информации, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и он становиться полностью или частично непригодным для целевого использования.

Модификация информации – внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных для компьютерной информации.

Блокирование информации – несанкционированное затруднение доступа пользователей к информации, не связанное с ее уничтожением;

Несанкционированное уничтожение, блокирование, модификация, копирование информации – любые, не разрешенные Законом, собственником или компетентным пользователем указанных действий с информацией.

Обман (отрицание подлинности, навязывание ложной информации) – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество, и таким образом добиться от него добровольной передачи имущества, а также сообщений с этой целью заведомо ложных сведений.

2) По принципу воздействия на носители информации - систему обработки и передачи информации (АСОИ):

* с использованием доступа нарушителя (злоумышленника, пользователя АСОИ, процесса) к объекту (в комнату переговоров, к файлу данных, каналу связи и т.д.);
* с использованием скрытых каналов – с применением ЗУ, РЗУ, путей передачи информации, позволяющих двум взаимосвязанным процессам (легитимному и внедренному злоумышленником) обмениваться информацией таким способом, который приводит к у теске информации.

3) По характеру воздействия на систему обработки и передачи информации:

- активные угрозы, связанные с выполнением нарушителем каких-либо действий, (копирование, несанкционированная запись, доступ к наборам данных, программам, вскрытие пароля и т.д.);

- пассивные угрозы, осуществляются путем наблюдения пользователем каких-либо побочных эффектов процессов движения информации и их анализа.

4) По факту наличия возможной для использования ошибки защиты угроза может быть обусловлена одной из следующих причин:

* неадекватностью - несоответствием режиму безопасности защиты зоны охраны.
* ошибками административного управления- режима безопасности;
* ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программ или комплекса программ и из-за которых эти программы могут быть использованы совсем не так, как описано в документации.
* ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапах реализации, отладки и могут служить источником недокументированных свойств.

5) По способу воздействия на объект атаки (при активном воздействии):

* непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например: непосредственный доступ в зоны слышимости и видимости, к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой;
* воздействие на систему разрешений (в том числе захват привилегий). При этом несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом;
* опосредованное воздействие (через других пользователей):
* "маскарад". В этом случае пользователь присваивает себе каким-либо образом полномочия другого пользователя, выдавая себя за него;
* "использование вслепую". При таком способе один пользователь заставляет другого выполнить необходимые действия (для системы защиты они не выглядят несанкционированными, ибо их выполняет пользователь, имеющий на это право), причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться вирус (он выполняет необходимые действия и сообщает о их результате тому, кто его внедрил).

Два последних способа очень опасны. Для предотвращения подобных действий требуется постоянный контроль как со стороны администраторов и операторов за работой АСОИ в целом, так и со стороны пользователей за своими собственными наборами данных.

6) По способу воздействия на АСОИ:

* в интерактивном режиме – в процессе длительной работы с программой;
* в пакетном режиме – после долговременной подготовки быстрым внедрением пакета программ направленного действия.

Работая с системой, пользователь всегда имеет дело с какой-либо ее программой. Одни программы составлены так, что пользователь может оперативно воздействовать на ход их выполнения, вводя различные команды или данные, а другие так, что всю информацию приходится задавать заранее. К первым относятся, например, некоторые утилиты, управляющие программы баз данных, в основном - это программы, ориентированные на работу с пользователем. Ко вторым относятся в основном системные и прикладные программы, ориентированные на выполнение каких-либо строго определенных действий без участия пользователя.

При использовании программ первого класса воздействие оказывается более длительным по времени и, следовательно, имеет более высокую вероятность обнаружения, но более гибким, позволяющим оперативно менять порядок действий. Воздействие с помощью программ второго класса (например, с помощью вирусов) является кратковременным, трудно диагностируемым, гораздо более опасным, но требует большой предварительной подготовки для того, чтобы заранее предусмотреть все возможные последствия вмешательства.

7) По объекту атаки:

* АСОИ в целом: злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Используют обычно "маскарад", перехват или подделку пароля, взлом или доступ к АСОИ через сеть;
* объекты АСОИ - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности (например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения);
* субъекты АСОИ - процессоры пользователей. Целью таких атак является либо прямое воздействие на работу процессора — его приостановка, изменение характеристик (например, приоритета), либо обратное воздействие - использование злоумышленником привилегий, характеристик другого процесса в своих целях. Воздействие может оказываться на процессы пользователей, системы, сети;
* каналы передачи данных - прослушивание канала и анализ графика (потока сообщений); подмена или модификация сообщений в каналах связи и на узлах-ретрансляторах; изменение топологии и характеристик сети, правил коммутации и адресации.

8) По используемым средствам атаки:

**-** с использованием стандартного программного обеспечения;

-с использованием специально разработанных программ.

9) По состоянию объекта атаки.

* Объект атаки хранится на диске, магнитной ленте, в оперативной памяти или в любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;
* Объект атаки находится в состоянии передачи по линии связи между узлами сети или внутри узла. Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), либо просто прослушивание с использованием скрытых каналов;
* Объект атаки (процесс пользователя) находиться в состоянии обработки.

Приведенная классификация показывает сложность определения возможных угроз и способов их реализации.

**Источники угроз информационным ресурсам**  аналогичны ранее рассмотренным источникам угроз для материальных ресурсов и могут быть представлены в таблице, как:

|  |
| --- |
| АНТРОПОГЕННЫЕ ИСТОЧНИКИ |
| - Криминальные структуры |
| - Потенциальные преступники и хакеры |
| - Недобросовестные партнеры |
| - Представители надзорных организаций и аварийных служб |
| - Представители силовых структур |
| -Основной персонал (пользователи, программисты, разработчики) |
| - Представители службы защиты информации (администраторы) |
| - Вспомогательный персонал (уборщики, охрана) |
| - Технический персонал (жизнеобеспечение, эксплуатация) |
|  |
| ТЕХНОГЕННЫЕ ИСТОЧНИКИ |
| Средства связи (передачи информации) |
| Сети инженерных коммуникаций (энергоснабжения, водоснабжения, отопления, вентиляции, канализации) |
| ВНУТРЕННИЕ ТЕХНОГЕННЫЕ ИСТОЧНИКИ УГРОЗ |
| Некачественные технические средства обработки информации |
| Некачественные программные средства обработки информации |
| Вспомогательные средства (охраны, сигнализации, телефонии) |
| Другие технические средства, применяемые в учреждении |
|  |
| СТИХИЙНЫЕ ИСТОЧНИКИ УГРОЗ |
| Пожары |
| Землетрясения |
| Наводнения |
| Ураганы |
| Различные непредвиденные обстоятельства |
| Необъяснимые явления  Другие форс-мажорные обстоятельства\*\* |

*\** Особую группу внутренних, антропогенных источников составляют специально внедренные и завербованные агенты из числа основного, вспомогательного, технического персонала и представителей службы защиты информации. Эта группа не рассматривается как самостоятельная, но при анализе, в случае возникновения потенциальной возможности внедрения агентов, необходимо учитывать особенности защиты от таких источников при рассмотрении возможностей внутренних антропогенных источников.

\*\* В данном случае под термином «другие форс-мажорные обстоятельства» понимается юридическая составляющая форс-мажора, то есть различные решения высших государственных органов, забастовки, войны, революции и т. п., приводящие к возникновению обстоятельств непреодолимой силы.

5.2. Условия и причины образования технических каналов утечки речевой информации

Речевая информация – информация, распространение которой осуществляется посредством звуковых (акустических), вибрационных, электромагнитных сигналов. Люди говорят друг с другом непосредственно и используют для общения средства связи.

**Речь характеризуется** (полученный речевой сигнал):

* разборчивостью – отношением числа правильно понятых элементов речи (звуков, слогов, слов) к общему числу принятых элементов;
* реверберацией звука – эффектом наложения речевых отрезков друг на друга в результате отражения сигнала от поверхностей конструкций;
* ослаблением звуковых колебаний – при прохождении речевых сигналов через различные среды (бетон, кирпич, стекло, воздух, вода …);
* присутствием шумов и помех – в месте возникновения речевой информации и по пути ее следования к пункту приема.

**Средства разведки**

Условиями для образования утечек в среде, окружающей источник речевой информации могут являться наличие в ней:

* акустических и виброакустических колебаний;
* радио-, оптических и электрических сигналов, содержащих сведения, в различных технических средствах обработки и передачи информации;
* нежелательных электромагнитных излучений систем и средств информатизации и связи;
* наводок электромагнитных излучений на различные токоведущие цепи и конструкции;
* специальных воздействий на элементы технических средств;
* различных закладных устройств;
* случайных электроакустических преобразователей в отдельных элементах технических средств.

В окружающей среде возникают виброакустические, гидроакустические, акустоэлектрические, электрические (в телефонной линии) сигналы, электромагнитные сигналы в эфире (разговор по радиотелефону), побочные электромагнитные излучения и наводки. Акустическая энергия, возникающая при разговоре, может вызвать акустические (механические) колебания элементов электронной аппаратуры, что, свою очередь, приводит появлению новых или изменению существующих электромагнитных сигналов.

**5.2.1 Утечка информации по акустическим и виброаккустическим каналам**

Различают прямой акустический канал- подслушивание (прямой перехват акустических колебаний в диапазоне частот от 16-25Гц до 18…20 КГц ) и канал с применением микрофонов, преобразующих акустические колебания в электрические сигналы.

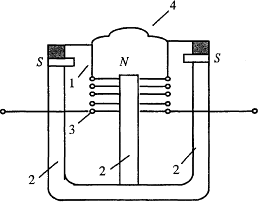
Наиболее простым способом перехвата речевой информации является подслушивание (прямой перехват). Разведываемые акустические сигналы могут непосредственно приниматься ухом человека, реагирующим на изменение звукового давления, возникающего при распространении звуковой волны в окружающем пространстве. Диапазон частот акустических колебаний, слышимых человеком, простирается от 16...25Гцдо 18... 20 кГц в зависимости от индивидуальных особенностей слушателя. Человек воспринимает звук в очень широком диапазоне звуковых давлений. Одной из опорных величин этого диапазона является стандартный порог слышимости. Под ним условились понимать эффективное значение звукового давления, создаваемое гармоническим звуковым колебанием частоты F= 1000 Гц, едва слышимым человеком со средней чувствительностью слуха. Порогу слышимости соответствует звуковое давление *Рзв0* = 2-10~5 Па. Верхний предел определяется значением *Pзв* = 20 Па, при котором наступает болевое ощущение (стандартный порог болевого ощущения).

В случаях, когда уровни звукового давления, создаваемого звуковой волной, ниже порога слышимости, когда нет возможности непосредственно прослушивать речевые сообщения или когда требуется их зафиксировать (записать), используют микрофон.

Микрофон является преобразователем акустических колебаний в электрические сигналы. В зависимости от физического явления, приводящего к такому преобразованию, различают основные типы микрофонов:

— электродинамические;

— электромагнитные;



— электростатические;

— пьезоэлектрические;

— магнитострикционные;

— контактные и т.д.

Действие электродинамического преобразователя основано на использовании явления электромагнитной индукции В кольцевом зазоре 1 магнитной системы, имеющей постоянный магнит 2, находится подвижная катушка *3,* соединенная с диафраг­мой *4.* При воздействии на диафрагму *4* звукового давления, она вместе с подвижной катушкой *3* совершает колебания в магнитном поле, создаваемом магнитной системой 2. В витках катушки 3, пересекающих магнитные силовые линии, возникает напряжение, являющееся выходным сигналом микрофона.

Структурная схема для иллюстрации прямого канала и канала с применением микрофона для перехвата акустической информации выглядит следующим образом: причины, приводящие к применению прямого канала утечки информации:

* Отсутствие или недостатки режима безопасности;
* Неадекватный обстановке подбор по функциональным возможностям технических средств защиты.
* Некачественное обслуживание технических средств и систем защиты, отказ в работе.
* Недостатки в работе с персоналом объекта.
* Высокопрофессиональные действия «нарушителя».

ВОЗДУШНАЯ СРЕДА

Микрофон

Проводной канал

Радиоканал

Оптический и др.каналы

Усилитель

Наушники

Магнитофон

**ЛИТЕРАТУРА**

1. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.
2. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия –Телеком, 2000. - 452 с., ил
3. Компьютерная преступность и информационная безопасность / А.П.Леонов [и др.]; под общ. Ред. А.П.Леонова. – Минск: АРИЛ, 2000. – 552 с.