

# 1 Основные понятия и определения в области информационной безопасности и технической защиты информации

---

## 1.1. Виды, формы представления и носители защищаемой информации

Информация как объект защиты — это сведения (сообщения, данные о лицах, предметах, фактах, событиях, явлениях и процессах) независимо от формы их представления. В более общем смысле информация — это сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования для определенных целей.

Информацию, в зависимости от категории доступа, делят на *общедоступную* и информацию *ограниченного доступа*, к которой доступ ограничен Федеральными законами [1, 3].

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Несекретная (открытая) информация не относится к государственной, служебной, коммерческой или личной тайне и может быть опубликована в открытой печати. На пользование несекретной информацией не накладывается никаких ограничений. Несекретная информация, если она представлена в форме документов или банка данных ЭВМ, должна защищаться от нарушения целостности и блокирования.

К информации ограниченного доступа относятся сведения, составляющие государственную тайну, и конфиденциальная информация (персональная информация, сведения, составляющие коммерческую тайну, служебную и иную тайну).

По своему характеру информация может быть *политической, военной, экономической, научно-технической, производственной* или *коммерческой* и быть *секретной, конфиденциальной* или *несекретной*.

Защищаемая информация обладает следующими свойствами:

- уровень доступа к ней, ограничения на порядок распространения и использования может устанавливать только государство или владелец;
- чем ценнее информация, тем тщательнее она защищается и тем меньше число лиц имеет доступ к этой информации.

Защищаемая информация разделяется в зависимости от степени ее конфиденциальности (степени ограничения доступа). Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

*Государственная тайна* — вид секретной информации, содержащей защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства.

К *служебной тайне* относятся охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам государства. Служебная тайна относится к секретной информации и имеет гриф «секретно».

К *конфиденциальной информации* относят сведения, содержащие коммерческую тайну, адвокатскую и следственную тайну, некоторые виды служебной тайны, врачебную тайну, тайну переписки, телефонных переговоров, почтовых и телеграфных отправок, а также некоторые сведения о частной жизни и деятельности граждан (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Конфиденциальную информацию составляют сведения, порядок доступа к которым определен их собственником в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной только санкционированным лицам, объектам или процессам.

Понятие «*коммерческая тайна*» определено как информация, которая «составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности».

Разглашение коммерческой тайны может серьезным образом повлиять на результаты деятельности предприятия или фирмы, поэтому коммерческая тайна должна быть охраняемой. Руководитель предприятия или организации должен издать приказ, в котором указываются сведения, составляющие коммерческую тайну.

Отличие сведений, составляющих государственную тайну, от коммерческой тайны заключается в том, что они регламентированы соответствующим перечнем и защищаются государством. Коммерческая тайна не имеет перечня, так как она различна для каждого предприятия или фирмы. Ее защиту осуществляют службы безопасности предприятия. Коммерческая тайна может в отдельных случаях относиться и к государственным секретам, если эти секреты имеют важное значение для государства.

*Носители (источники) защищаемой информации* классифицируются как документы; изделия (предметы); вещества и материалы; электромагнитные, тепловые, радиационные и другие излучения; гидроакустические, сейсмические и другие физические поля, представляющие особые виды материи; сам объект с его видовыми характеристиками и т. п. В качестве носителя защищаемой информации может быть также человек.

Информация по форме представления, способам кодирования и хранения может быть графической, звуковой, текстовой, цифровой (компьютерной), видеоинформацией и т. п. Наиболее важными свойствами информации являются прежде всего ее достоверность, полнота, объективность, своевременность, важность.

*Формы представления информации* зависят от ее характера и физических носителей, на которых она представлена. Основными формами информации, подлежащими защите, являются [1]:

- документальная;
- акустическая;
- телекоммуникационная;
- визуальная.

*Документированная информация* (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать — установить характер документа и его собственника. Информация, записанная на носителе, может быть графической и текстовой. На документе-носителе защищаемой информации указывается степень конфиденциальности информации в зависимости от ее важности.

*Источниками речевой (акустической) информации* являются разговоры в помещениях и системы звукоусиления и звуковоспроизведения. Речевая информация распространяется в газовой, твердотельной и гидравлической средах. Носителем речевой информации являются акустические колебания частиц в виде звуковых волн различной длины в упругих средах. Слышимый речевой сигнал находится в диапазоне частот 20 Гц... 20 кГц.

*Изделия* (предметы) как носители защищаемой информации могут представлять собой засекреченные образцы военной техники, опытные образцы вновь разрабатываемых высокотехнологичных изделий и систем, определяющих уровень научно-технического развития промышленности страны.

*Материалы и вещества*, применяемые в производстве и эксплуатации новых образцов техники и в военных изделиях. Иностранные разведки могут получать информацию о материалах и веществах наиболее доступными способами — по отходам производства режимных предприятий, по составу воздушной среды и водных осадков в непосредственной близости от предприятия.

*Электромагнитные излучения* различной частоты могут содержать информативные сигналы от защищаемого объекта при его функционировании. Источником электромагнитного излучения в большинстве случаев являются технические средства обработки информации, а также кабельные и проводные линии каналов ее передачи. Опасность могут представлять и вспомогательные средства и системы объектов информатизации, которые фактически образуют сосредоточенные или распределенные случайные антенны.

*Носителем видовой информации объекта* является сам объект, а также его фото- и видеоизображения на материальных носителях.

С развитием информационного общества все большее значение приобретают проблемы, связанные с защитой конфиденциальной информации. Каждое государство защищает свои информационные ресурсы. Общая тенденция такова — чем выше уровень секретности информации, тем выше и уровень ее защиты, тем больше средств тратится на ее защиту.

## 1.2. Угрозы безопасности информации

Под безопасностью информации следует понимать условия хранения, обработки и передачи информации, при которых обеспечивается ее защита от угроз *хищения (разглашение, утечки, раскрытия)*, приводящее к потере конфиденциальности, *изменения (нарушения целостности)* и *уничтожения (отказа в обслуживании)*. Нарушение целостности информации — частный случай ее изменения (рис. 1.1).

*Раскрытие информации* — это перехват и расшифровка конфиденциальной информации, в результате перехвата возможно неправомерное ознакомление с информацией посторонних лиц.

*Угроза нарушения целостности* включает в себя любое изменение (модификацию или даже удаление) данных, хранящихся в средствах вычислительной техники (СВТ) или передаваемых из одной системы в другую.

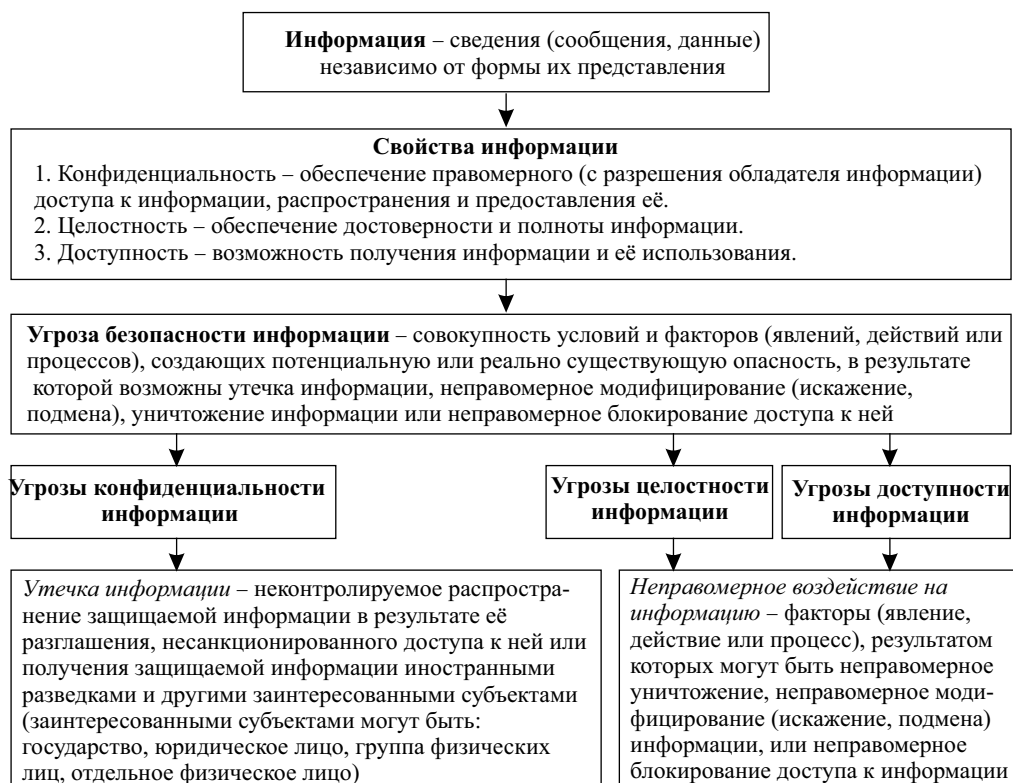


Рис. 1.1. Классификация угроз безопасности информации

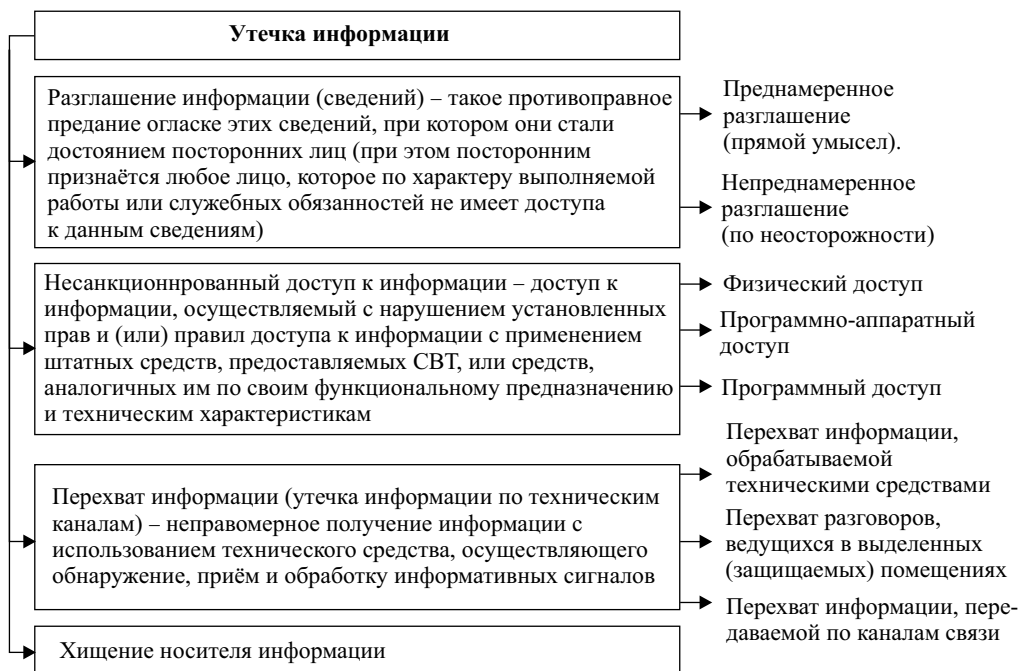


Рис. 1.2. Формы утечки информации

Угроза отказа в обслуживании возникает, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным или вызвать только задержку запрашиваемого ресурса.

Утечка обрабатываемой информации по техническим каналам происходит за счет (рис. 1.2):

- побочных электромагнитных излучений информативного сигнала от технических средств и линий передачи информации;
- наводок информативного сигнала, обрабатываемого техническими средствами, на провода и линий, выходящие за пределы контролируемой зоны предприятия (учреждения), в том числе на цепи заземления и электропитания;
- изменения тока потребления, обусловленного информативными сигналами, формируемыми техническими средствами обработки информации;
- радиоизлучений, модулированных информативными сигналами, возникающими при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучений или электрических сигналов от внедренных в технические средства и выделенные помещения специальных электронных устройств перехвата информации (закладок), модулированных информативным сигналом;

- электрических сигналов или радиоизлучения, обусловленных воздействием на технические средства высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т. п.) и модуляцией их информативным сигналом (облучение, «навязывание»);
- радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- акустических излучений информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации (компьютеры, ноутбуки, клавиатуры, принтеры, банккоматы, мобильные телефоны и т. п.);
- электрических сигналов, возникающих посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям передачи информации;
- вибрационных сигналов, возникающих посредством преобразования информативного акустического сигнала при его воздействии на строительные конструкции и инженерно-технические коммуникации выделенных помещений;
- просмотра информации с экранов дисплеев и других средств ее отображения с помощью оптических средств разведки;
- выявления внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств).

Несмотря на различную физическую природу образования технических каналов утечки информации (ТКУИ), ее техническая защита базируется на методах снижения отношения мощности опасного сигнала к мощности шума в точке размещения аппаратуры разведки. Защита информации от утечки осуществляется с применением пассивных и активных методов и средств. Цель защиты — уменьшение отношения сигнал/шум ( $C/\Pi$ ) на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки противника опасного информационного сигнала. В пассивных методах защиты уменьшение отношения  $C/\Pi$  достигается путем уменьшения уровня сигнала, в активных методах — путем увеличения уровня шума. К ним относятся пространственное и линейное зашумление.

Задача защиты информации (ЗИ) на объекте считается выполненной, если исключена возможность съема информации по всем возможным каналам ее утечки.

По методам воздействия на информацию угрозы подразделяются на *естественные* и *искусственные*. В свою очередь искусственные угрозы состоят из *преднамеренных* и *непреднамеренных* (рис. 1.3).

*Естественные угрозы* — это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов или стихийных природ-

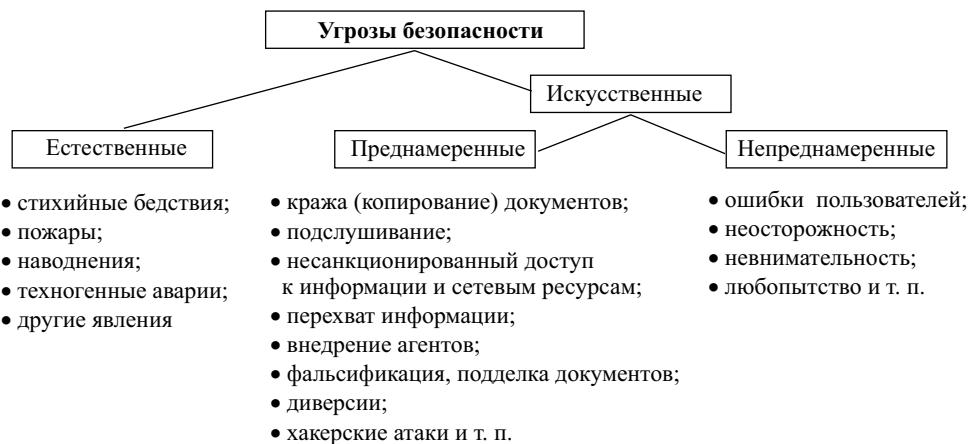


Рис. 1.3. Угрозы безопасности информации

ных явлений, независящих от человека: стихийные бедствия, пожары, наводнения, техногенные аварии и другие явления.

*Искусственные угрозы* — это угрозы информации, вызванные деятельностью человека.

*Искусственные преднамеренные (умышленные)* угрозы — это угрозы, связанные с корыстными, идейными или иными устремлениями людей:

- кража (копирование) документов;
- подслушивание переговоров;
- несанкционированный доступ к информации и сетевым ресурсам;
- перехват информации;
- внедрение (вербовка) агентов;
- фальсификация, подделка документов;
- диверсии;
- хакерские атаки и т. п.

*Искусственные непреднамеренные угрозы (неумышленные, случайные)* — это угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и пользователей, неосторожность, невнимательность, любопытство и т. п.

Наибольшую угрозу представляют *преднамеренные действия* — действия нарушителей и злоумышленников — шпионов, диверсантов, персонала, преступников.

Все каналы проникновения в систему и утечки информации разделяют на косвенные и прямые. Под *косвенными* понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования *прямых* каналов такое проникновение необходимо. Варианты реализации каналов негласного получения информации приведены на рис. 1.4.

По способу получения информации каналы доступа можно разделить:

- на физические;



Рис. 1.4. Варианты негласного получения информации, циркулирующей в информационных системах

- электромагнитные (перехват излучений);
- информационные (программно-математические).

Безопасность информации оценивается двумя показателями: вероятностью предотвращения угроз и временем, в течение которого обеспечивается определенный уровень безопасности. Эти показатели взаимозависимые. При заданных конкретных мерах по защите обеспечить более высокий уровень безопасности возможно в течение более короткого времени.

Для обеспечения эффективной защиты необходимо оценивать величину угрозы. Величину конкретной угрозы  $C_{yi}$  для рассматриваемого  $i$ -го элемента информации в общем случае можно представить в виде произведения потенциального ущерба от реализации угрозы по  $i$ -му элементу информации  $C_{пуi}$  и вероятности ее реализации  $P_{yi}$ , т. е.

$$C_{yi} = C_{пуi}P_{yi}.$$

Приближенная оценка величины угрозы возможна при следующих ограничениях и условиях.

Во-первых, можно предположить, что максимальный ущерб от хищения информации соответствует ее цене. Действительно, в случае попадания информации к конкуренту владелец информации может лишиться не только ожидаемой прибыли, но и не компенсировать ее себестоимость.

Во-вторых, в условиях полной неопределенности знаний о намерениях злоумышленника по добыванию информации ошибка прогноза минимальная, если принять вероятность реализации угрозы в течение рассматриваемого периода времени (например, одного года) равной 0,5.

В результате усреднения по всем  $i$ -м элементам информации верхняя граница угрозы составит половину цены защищаемой информации. Очевидно, что чем выше цена информации и больше угроза ее безопасности, тем больше ресурсов потребуются для защиты этой информации.

Оценивать величину угрозы можно по степени ограничения доступа (в зависимости от тяжести ущерба, который может быть нанесен безопасности государства в случае распространения указанных сведений). Устанавливаются обычно три группы секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений.

К первой группе относят сведения в области военной, внешнеполитической, экономической, научно-технической и др., распространение которых может нанести ущерб интересам государства в одной или нескольких из перечисленных областей.

К сведениям второй группы относят сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики государства в одной или нескольких из перечисленных областей.

К третьей группе следует относить все иные сведения из числа сведений, составляющих государственную тайну.

### 1.3. Направления, формы, цели, объекты и задачи иностранных разведок

**Направления разведывательной деятельности.** По направлениям разведывательной деятельности иностранные разведки подразделяется на политическую, экономическую, военную и научно-техническую разведки [5].

*Политическая разведка* осуществляет деятельность по добыванию сведений внутриполитического и внешнеполитического характера в стране, являющейся объектом разведки, организует действия по подрыву политического строя государства. Примером могут служить организация «цветных революций» в некоторых странах постсоветского пространства, свержение неугодных режимов на Ближнем Востоке.

*Экономическая разведка* занимается сбором сведений, раскрывающих экономический потенциал определенной страны. К таким сведениям относятся характеристики природных ресурсов, промышленности, транспорта, финансовой системы, торговли и т. п.

*Военная разведка* направлена на сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники. Особое внимание иностранные разведки уделяют добыванию информации о научно-исследовательских центрах, видных ученых и специалистах.

*Научно-техническая разведка* занимается добыванием сведений по новейшим теоретическим и практическим разработкам в области науки и техники.

**Формы и цели разведывательной деятельности.** Основные формы разведывательной деятельности: агентурная, легальная, техническая разведки и аналитическая обработка первичной развединформации.

*Агентурная разведка* использует для добывания информации и проведения диверсионных акций специально подобранных, завербованных и профессионально подготовленных агентов. Агентурная разведка также предполагает добывание информации путем проникновения агента-разведчика к источнику информации на доступное расстояние для применения технических средств разведки.

*Легальная разведка* добывает информацию при различных официальных связях и контактах с нашей страной, из легальных источников информации.

Существует три основные формы *легальной разведки*:

- анализ всех открытых публикаций, которые издаются в стране-объекте разведки;
- получение информации во время непосредственных контактов агентов с интересующими их лицами на приемах, встречах, конференциях;
- визуальное наблюдение, кино- и фотосъемка при перемещении иностранцев по стране.

*Техническая разведка* предполагает сбор информации с использованием технических разведывательных средств.

*Аналитическая обработка* первичной информации позволяет на основе анализа несистематизированной первичной разведывательной информации с помощью специально разработанных программ обработки получать новые и более объективные разведданные.

#### 1.4. Техническая разведка, классификация, цели, объекты и задачи

Под *технической разведкой* (ТР) понимается целенаправленная деятельность по добыванию информации из различных источников с помощью специальных технических средств (СТС). Средство технической разведки — аппаратура технической разведки, размещенная на стационарном или мобильном объекте (помещении, транспортном средстве и т. д.). Аппаратура технической разведки — совокупность технических устройств, предназначенных для обнаружения, приема (перехвата), регистрации и обработки сигналов, содержащих важную (защищаемую) информацию. Возможности технической разведки определяют характеристики способности обнаружения, распознавания, приема и регистрации информативных сигналов средствами технической разведки. Информативные (опасные) сигналы — это электрические или электромагнитные сигналы и другие физические поля, по параметрам которых может быть раскрыта информация, обрабатываемая с помощью технических средств. Пространство вокруг объекта, в пределах которого реализуются возможности технической разведки, называется зоной разведдоступности.

Модель технической разведки — описание средств технической разведки, содержащее их технические характеристики и тактику применения в объеме, достаточном для оценки возможностей технической разведки.

Предпосылками возникновения ТР являлось прежде всего стремление снизить риск физического задержания агента за счет дистанционного контакта с источником интересующей информации.

Техническую разведку можно классифицировать по нескольким признакам:

- по решаемым задачам, видам;
- природе физических явлений, лежащих в основе образования технических каналов утечки информации;
- месту размещения аппаратуры разведки.

К числу основных объектов ТР относятся:

- Вооруженные силы;
- оборонная промышленность, НИИ, научно-исследовательские центры, полигоны, военные базы, посольства;
- транспорт, связь, энергосистемы;
- системы охраны наиболее важных правительственных и военных объектов.

При добывании информации техническими средствами могут использоваться каналы утечки информации, основанные на появлении:

- в пространстве и веществах — собственных или отраженных от источников сигналов электромагнитных излучений и полей в оптическом диапазоне (видовые сигналы) и радиодиапазоне, а также статических полей;
- в воздушной среде и твердых телах — акустических и вибрационных колебаний при механическом воздействии на них источников звуковых сигналов;
- в окружающей среде — радиоактивного излучения, характеризующего специфику функционирования объекта;
- в окружающей среде и телах — изменений температуры, характеризующих изменение режимов и специфику функционирования объектов;
- в окружающей среде — специфических промышленных и прочих отходов.

Каналы утечки информации делятся на прямые и побочные.

Под *прямым каналом* понимается канал утечки, органически присущий нормальному функционированию (эксплуатации) объекта защиты:

- электромагнитное излучение передатчиков линий радиосвязи и телеметрии;
- электрические сигналы в линиях электросвязи, при возможности гальванического подключения и т. п.;
- инфракрасное излучение линий ИК-связи;
- излучение РЛС, средств радионавигации и наведения;
- акустические волны линий гидроакустической связи в толще воды;
- видовые характеристики объектов и местности, не скрытые от визуального наблюдения и фотографирования в оптическом и радиодиапазоне;
- акустические волны, возникающие в воздушной среде при ведении переговоров, с возможностью их подслушивания.

Под *побочным каналом* понимается канал утечки, не являющийся необходимым для нормального функционирования объекта защиты и возникающий в процессе работ:

- побочные электромагнитные излучения в пространство технических средств и наводки опасного сигнала на случайные антенны, имеющие цепи, выходящие за пределы охраняемой территории;
- акустические волны инфразвукового, звукового и ультразвукового диапазонов, распространяющиеся в воздушной и водной среде, в ограждающих конструкциях, вызванные шумами работающих двигателей машин, агрегатов и различного оборудования;

- тепловое излучение объектов, регистрируемое в инфракрасном и радиодиапазоне, вызванное работой машин, агрегатов и оборудования, движением транспортных средств, ракет и т.п.;
- сейсмические волны, вызванные взрывами, выстрелами, работой машин, агрегатов и оборудования, движением транспортных средств, людей и т.п.;
- радиоактивные излучения, связанные с выбросами и отходами производства, хранением и транспортировкой радиоактивных материалов, ядерных зарядов и боеприпасов, производством и эксплуатацией ядерных реакторов и двигателей, а также излучения, возникающие при ядерных взрывах и радиоактивном заражении местности;
- изменение химического состава окружающей среды, возникающие под воздействием выбросов и отходов производства, в результате работы различных машин и намеренного применения химического оружия;
- локальное изменение магнитного поля Земли, вызванное сосредоточением военной техники и оружия, подводными лодками, ядерными фугасами и т.п.

Выделяют также параметрические каналы утечки информации, например следующие:

- акустические колебания в помещении, вызванные разговором, вызывают изменение параметров элементов электрической схемы технического средства, что приводит к изменению токов и напряжений в нем, появлению паразитных генераций;
- переизлучения вспомогательных технических средств и систем (ВТСС) и основных технических средств и систем (ОТСС), промодулированные информативным сигналом, после их ВЧ-облучения, преднамеренного или случайного, через пространство или электрические цепи выходящие за охраняемые границы (ВЧ-навязывание);
- отражение от объектов и местности сигналов радиолокации, инфракрасной (лазерной) подсветки;
- промодулированные информативным акустическим сигналом отражения от стекол и предметов интерьера, лазерного луча при ведении акустической разведки.

В зависимости от природы образования ТКУИ можно разделить на естественные и специально (преднамеренно) создаваемые.

По оценкам американских специалистов, в настоящее время с помощью средств ТР добывается более 30 % всей разведывательной информации и до 85 % информации, касающейся национальных стратегических объектов, вооружений и средств связи.

Источником информации для технических разведок могут быть различные электромагнитные излучения и звуковые колебания. Электромагнитное излучение принято делить по частотным диапазонам, которые классифицируют согласно рекомендациям Международного консультативного комитета по радио (МККР) (табл. 1.1). В самом верхнем диапазоне частот