# Постановка цели и задачи

## Описание предметной области

# Основные понятия

Ключевой термин в рамках данной работы – информация. Информация представляет собой любые сведения независимо от формы их представления.

Информация обладает следующими свойствами:

* объективность. Информация в любом своём проявлении объективна, она отображает объективную действительность;
* достоверность. Информация достоверна, если она отражает истинное положение дел. Достоверная информация помогает принять нам правильное решение;
* полнота. Информацию можно назвать полной, если ее достаточно для понимания и принятия решений. Неполная информация может привести к ошибочному выводу или решению;
* точность определяется степенью ее близости к реальному состоянию объекта, процесса, явления;
* актуальность – важность для настоящего времени, злободневность, насущность. Только вовремя полученная информация может быть полезна;
* полезность (ценность). Полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью.
* В силу того, что информация может обладать определенной ценностью, ее необходимо защищать. Согласно ФЗ от [27.07.2006 N 149-ФЗ (ред. от 18.03.2019) "Об информации, информационных технологиях и о защите информации"](http://www.consultant.ru/document/cons_doc_LAW_61798/) защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.

Такая защита обеспечивается соблюдение трех принципов – доступности, целостности и конфиденциальности.

Конфиденциальность – свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;

Целостность – свойство сохранения правильности и полноты активов;

Доступность – свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.

К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Совокупность операций ввода, вывода, сбора, записи, хранения, регистрации, накопления, уничтожения, преобразования, приема, передачи и отображения информации часто называют обобщенным термином обработка информации.

С этим же понятием связаны информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) и способы осуществления таких процессов и методов.

# Угрозы информации

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения [информационной безопасности](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты информационной системы может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Все источники угроз информационной безопасности можно разделить на три основные группы:

* обусловленные действиями субъекта – субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними, так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры;
* обусловленные техническими средствами – эти источники напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними;
* стихийные источники – данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить)

Попытка реализации угрозы называется атакой.

# Защита информации от утечки по техническим каналам

К техническим средствам передачи, обработки, хранения и отображения информации ограниченного доступа (ТСПИ) относятся: технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы; средства изготовления и размножения документов; аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода; системы внутреннего телевидения; системы видеозаписи и видеовоспроизведения; системы оперативно-командной связи; системы внутренней автоматической телефонной связи, включая и соединительные линии перечисленного выше оборудования и т.д. Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС).

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, на объектах ТСПИ также устанавливаются вспомогательные технические средства и системы (ВТСС), непосредственно не участвующие в ее обработке. К ним относятся: системы и средства городской автоматической телефонной связи; системы и средства передачи данных в системе радиосвязи; системы и средства охранной и пожарной сигнализации; системы и средства оповещения и сигнализации; контрольно-измерительная аппаратура; системы и средства кондиционирования; системы и средства проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, средства радиовещания; телевизоры и радиоприемники и т.д.); средства электронной оргтехники.

Совокупность объекта разведки (в данном случае - объекта ТСПИ), технического средства разведки, с помощью которого добывается информация, и физической среды, в которой распространяется информационный сигнал, называется техническим каналом утечки информации (рис. 1.1).

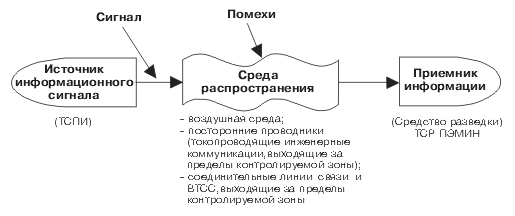


Рисунок 1.1 – Технический канал утечки информации

При работе технических средств возникают информативные электромагнитные излучения, а в соединительных линиях ВТСС и посторонних проводниках могут появляться наводки информационных сигналов. Поэтому, технические каналы утечки информации можно разделить на электромагнитные и электрические.

В данной работе основное внимание уделено именно электромагнитным каналам утечки конфиденциальной информации. К которым относятся возникающие вследствие движения электронов электрические и магнитные поля

# Теория ПЭМИН

В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно:

* побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСПИ и их соединительным линиям переменного электрического тока;
* побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;
* побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

* вывод информации на экран монитора;
* ввод данных с клавиатуры;
* запись информации на накопители на магнитных носителях;
* чтение информации с накопителей на магнитных носителях;
* передача данных в каналы связи;
* вывод данных на периферийные печатные устройства – принтеры, плоттеры;
* запись данных от сканера на магнитный носитель (ОЗУ).

Для перехвата побочных электромагнитных излучений ТСПИ “противником” могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Как правило, полагается, что ТСР ПЭМИН располагаются за пределами контролируемой зоны объекта.

Пространство вокруг ТСПИ, в пределах которого напряженность электромагнитного поля превышает допустимое (нормированное) значение, называется зоной 2 (R2). Фактически зона R2 – это зона, в пределах которой возможен перехват средством разведки побочных электромагнитных излучений ТСПИ с требуемым качеством.

Зона 2 для каждого ТСПИ определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия.

Причинами возникновения электрических каналов утечки информации могут быть:

* гальванические связи соединительных линий ТСПИ с линиями ВТСС и посторонними проводниками;
* наводки побочных электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники;
* наводки побочных электромагнитных излучений ТСПИ на цепи электропитания и заземления ТСПИ;
* “просачивание” информационных сигналов в цепи электропитания и заземления ТСПИ;
* “просачивание” информационных сигналов в цепи заземления ТСПИ.

Наводки (токи и напряжения) в токопроводящих элементах обусловлены электромагнитным излучением ТСПИ (в том числе, и их соединительными линиями), а также емкостными и индуктивными связями между ними. Соединительные линии ВТСС или посторонние проводники являются как бы случайными антеннами, при гальваническом подключении к которым средства разведки ПЭМИН возможен перехват наведенных в них информационных сигналов.

При распространении по случайной антенне наведенный информационный сигнал затухает. Коэффициент затухания информационного сигнала можно рассчитать, зная расстояние от места возможного подключения ТСР к случайной антенне до объекта ТСПИ и частоты побочных электромагнитных излучений.

# Сущность утечки конфиденциальной информации по каналу \_\_\_\_\_\_\_\_\_\_ПЭМИН

В области технической защиты информации перехват ПЭМИН потенциальным злоумышленником представляется как перехват одного двоичного разряда. При этом считается, что ему доступна ПЭМИН в диапазоне частот от 10 Гц до 1000 МГц, что обуславливается частотой работы компьютера и возможностями технических средств разведки, доступных потенциальному нарушителю, учитывая его возможности в данной области. Потенциал возможностей нарушителя определяется уровнем секретности информации – конфиденциальная информация, не составляющая государственную тайну.

При измерениях ПЭМИН оперируют понятием "информативность" сигнала. Информативными сигналами в общем случае считаются сигналы, амплитуда которых претерпевает изменения в зависимости от передаваемой информации. То есть если сигнал цифровой – это переход от "0" к "1" и от "1" к "0". Допустим, по цепи пересылается последовательность битов в один байт – например, 11111111, с некоторой тактовой частотой и длительностью импульса. Метод кодирования – последовательный импульсный код, то есть единица кодируется наличием импульса, ноль - отсутствием. Пауза между импульсами равна длительности импульса.