Потери информации могут произойти непосредственно в момент архивации данных. Единственный способ защиты – это правильно разработанная стратегия архивации данных.

5. Ошибки обслуживающего персонала и пользователей.

Они делятся на две категории:

* случайное изменение или уничтожение данных при вводе или коррекции
* некорректное использование программного или аппаратного обеспечения, приводящие к изменению или уничтожению данных

Меры противодействия:

1. Обучение персонала
2. Разграничение доступа и полномочий пользователей
3. Резервное копирование

**Преднамеренные угрозы**

Точки приложения преднамеренных угроз в компьютерной системе – это входы и выходы системы.

К преднамеренным угрозам принято относить:

1. Несанкционированный доступ к ресурсам компьютерной системы
2. Перехват побочных электромагнитных излучений
3. Заражение программного обеспечения компьютерными вирусами либо закладки

**Несанкционированный доступ**

К проявлению несанкционированного доступа принято относить:

* Ознакомление с конфиденциальной информацией
* Несанкционированное копирование информации
* Подделывание информации
* Уничтожение информации

В качестве мер противодействия - системы разграничения доступа и полномочий. Назначение таких систем состоит – создание условий, при которых зарегистрированные процессы и физические лица могут выполнять только то, что им разрешено и не более того.

Любой механизм разграничения доступа и полномочий решает следующие задачи:

1. Регистрация пользователей и процессов – идентификация
2. Определяет, кто именно имеет право доступа к ресурсам системы, - аутентификация
3. К каким ресурсам предоставлен доступ, в каких условиях предоставлен доступ, что можно делать с ресурсами, - авторизация
4. Определяет реакцию системы на неразрешённые или неправильные действия

**Перехват побочных электромагнитных излучений**

Все сигналы в компьютерной системе передаются по линиям связи, которые можно рассматривать как излучающая антенна, поэтому работа любой компьютерной системы сопровождается электромагнитным излучением радиодиапазона. Такое побочное электромагнитное излучение (ПЭМИН) несёт некоторую информацию, обрабатываемую в компьютерной системе. Перехват ПМИ может нарушить безопасность информации.

Для защиты от перехвата ПЭМИН предусматривают:

* Генератор белого шума, которые излучает широкополосный шумовой сигнал, уровень которого превышает уровень ПЭМИН (активная радиотехническая маскировка)
* Снижение уровня логической единиц
* Электромагнитное экранирование помещений
* Шифрование информации

**Заражение компьютерного обеспечения вирусами и закладками**

Анализ угроз безопасности информации позволяет следующие моменты:

1. Преднамеренные угрозы, направленные непосредственно на изменение статуса безопасности информации, а случайные влияют косвенно посредством изменения нормального функционирования других ресурсов компьютерной системы. Поэтому защита от преднамеренных угроз направленна непосредственно на сохранение безопасности информации, а защита от случайных угроз – это результат поддержки нормального функционирования компьютерной системы.
2. Преднамеренные угрозы направленны на нарушение всех трёх принципов безопасности информации (конфиденциальности, целостности и доступности). Случайные угрозы приводят к нарушению только целостности информации. Поэтому преднамеренные угрозы более опасны, а способы защиты от преднамеренных угроз должны быть более широкими и разнообразными.
3. Источники преднамеренных угроз скрывают себя и свои действия, маскируясь под зарегистрированных пользователей процесса, поэтому обнаружение и ликвидация источников преднамеренных угроз происходит гораздо сложнее.

Из преднамеренных угроз наиболее опасны - несанкционированный доступ. Поскольку даже заражение компьютерными вирусами можно рассматривать как несанкционированный доступ. Поэтому защита информации от НСД (несанкционированного доступа) является важной защитой компьютерной системы.

**Способы (методы) и средства защиты от несанкционированного доступа**

Формальные

Технические

Физические

Препятствия

Управление доступом

Средства защиты

Побуждение

Принуждение

Регламентация

Маскировка

Программные

Аппаратные

Способы защиты

Организационные

Законодательные

Морально-этические

Неформальные

Препятствие – это способ защиты, который связан с физическим преграждением пути злоумышленнику защищаемой информации.

Управление доступом – это способ защиты, связанный с регулированием использования ресурсов системы.

Маскировка – это либо радиотехническая маскировка, либо криптографическое закрытие информации.

Регламентация, как способ защиты, заключается в разработке и реализации комплексов мероприятий, создающих такие условия обработки и хранения защищаемой информации, при которых возможности нарушения безопасности информации сводились бы к минимуму.

Принуждение – это способ защиты, при котором лица соблюдают правила обращения с информацией под угрозой материальной, административной или уголовной ответственностей.

Побуждение — это способ защиты, при котором лица соблюдают правила обращения с информацией в силу сложившихся в обществе морально-этических норм.

Все средства защиты, реализующие методы защиты, делятся на формальные и неформальные.

К **формальным** относятся средства защиты, которые выполняют защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека.

К неформальным относятся средства защиты, которые либо определяются целенаправленно деятельностью людей, либо регламентируют эту деятельность.

Формальные средства делятся на технические и программные.

К техническим относятся физические средства, которые создают различного рода препятствия дестабилизирующим факторам (двери, замки, сейфы).

Физические средства могут быть как механическими, так и электромеханическими.

Аппаратные средства – это электронные устройства, схемно-встраиваемые или внешне-сопрягаемые с аппаратурой компьютерной системы для решения задач защиты информации (это могут быть либо платы шифрования, которые вставляются в слот, или внешние электронный ключ).

Программные средства – пакеты программ и тому подобное для защиты (управление доступом, программы шифрования, антивирусные средства и так далее).

**Неформальные.**

Организационные – это функционально-технические программы, предусматриваемые с целью решения задач защиты информации (создание отделов в организационной структуре, отвечающих за информационную безопасность ЛИБО отдельное лицо).

Законодательные средства – это нормативно-правовые акты (законы, постановления, приказы и распоряжения), с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации лиц, имеющих отношение к функционированию компьютерных систем, а также устанавливается ответственность за действия (или бездействие), следствием которых может быть нарушение безопасности информации.

Морально-этические средства – это сложившиеся в обществе, либо в данном коллективе, моральные нормы и этические правила, соблюдение которых способствует защите информации.

Поскольку существует большое число способов и средств защиты информации от несанкционированного доступа, то для обеспечения заданного уровня защищенности информации необходим комплексный подход, который может привести к положительному результату только при взаимодействии специалистов в различных областях знаний.