1. Понятие «Информационная безопасность»

***Информационная безопасность*** – это **защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий** естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

1. Что такое «Защита информации»

**Защита информации** - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

1. Что понимается под «Компьютерной безопасностью»

Компьютерная безопасность - это защита информации на компьютере, на мобильных устройствах от различного рода случайных или умышленных её повреждений, удаления, а также защита персональных данных на компьютере от взлома и кражи. К задачам компьютерной безопасности относится стабильность работы программ, операционных систем, компьютерных сетей.

Компьютерная безопасность - это область знаний, охватывающая модели, методы, программные, аппаратно-программные средства, системы защиты информации при ее обработке, хранении и передаче с использованием информационных технологий.

**Компьютерная безопасность** — меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет).

Поле деятельности системных администраторов охватывает все процессы и механизмы, с помощью которых цифровое оборудование, информационное поле и услуги защищаются от случайного или несанкционированного доступа, изменения или уничтожения данных, и приобретает всё большее значение в связи с растущей зависимостью от компьютерных систем в развитом сообществе

1. Определение Конфиденциальность

**Конфиденциальность** – самый проработанный аспект информационной безопасности. Практическая реализация мер по обеспечению конфиденциальности современных информационных систем связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные технические проблемы.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

**Конфиденциальность** – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации, нарушение конфиденциальности приводит к раскрытию информации.

1. Определение Целостность

Целостность информации условно подразделяется на статическую и динамическую.

**Статическая** целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

**Динамическая** целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и т. д.

Например, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью.

**Целостность** – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

1. Классификация опасностей в компьютерных системах

Под угрозой информационной безопасности принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, несанкционированному распространению, ограничению или блокированию к ним доступа. В настоящее время известно достаточно большое количество угроз, которые классифицируют по различным признакам.

По природе возникновения различают **естественные** и **искусственные** угрозы.

К **естественной группе** относятся те, что вызваны воздействием на компьютерную систему объективных физических процессов или стихийных природных явлений.

**искусственные** – те угрозы, которые обусловлены деятельностью человека.

По степени преднамеренности проявления**,** угрозы разделяют на **случайные** и **преднамеренные**.

Источник угроз может иметь разное положение.

В зависимости от этого фактора также выделяют **три группы**:

*— Угрозы, источник которых находятся вне контролируемой группы компьютерной системы*

*(пример – перехват данных, передаваемых по каналам связи)*

*— Угрозы, источник которых – в пределах контролируемой зоны системы*

*(это может быть хищение носителей информации)*

*— Угрозы, находящиеся непосредственно в самой системе*

*(например, некорректное использование ресурсов).*

Угрозы способны по-разному воздействовать на компьютерную систему.

Это могут быть **пассивные воздействия**, реализация которых не влечет за собой изменение структуры данных

(например, копирование).

**Активные угрозы** — это такие, которые, меняют структуру и содержание компьютерной системы

(внедрение специальных программ).

В соответствии с разделением угроз **по этапам доступа пользователей или программ к ресурсам системы** существуют такие опасности, которые проявляются на этапе доступа к компьютеру.

**Случайными**, или **непреднамеренными** называются такие угрозы, которые не связаны с действиями злоумышленников.

Аварии и стихийные бедствия представляют особую опасность для компьютерных систем.

Вследствие физического разрушения систем информация становится недоступной, либо утрачивается.

Кроме того, невозможно полностью избежать сбои в сложных системах, в результате которых, хранящаяся на них информация искажается или уничтожается, нарушается алгоритм работы технических устройств.

Небрежное или невнимательное выполнение функциональных обязанностей сотрудниками на предприятиях приводит к уничтожению, нарушению целостности и конфиденциальности информации.

Выделяют также **преднамеренные угрозы**, которые связаны с целенаправленными действиями нарушителя.

Для проникновения в компьютерную систему с целью дальнейшего хищения или уничтожения информации используются такие методы как прослушивание, хищение программ, документов и носителей информации.

При несанкционированном доступе к данным обычно используют аппаратные и программные средства компьютерных систем. Самые распространенные нарушения – это перехват паролей (производится с помощью специально разработанных программ).

1. Внутренние угрозы

Источниками **внутренних** угроз являются:

**1. Сотрудники организации.**

**2. Программное обеспечение.**

**3. Аппаратные средства.**

Внутренние угрозы могут проявляться в следующих формах:

**- ошибки пользователей и системных администраторов;**

**- нарушения сотрудниками фирмы установленных правел, обработки, передачи и уничтожения информации;**

**- ошибки в работе программного обеспечения;**

**- отказы и сбои в работе компьютерного оборудования.**

1. Внешние угрозы

К **внешним** источникам угроз относятся:

**1. Компьютерные вирусы и вредоносные программы.**

**2. Организации и отдельные лица.**

**3. Стихийные бедствия.**

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами или вредоносными программами;

- несанкционированный доступ к корпоративной информации;

- информационный мониторинг со стороны конкурирующих структур, специальных служб;

- действия государственных структур и служб, сопровождающиеся сбором, изъятием и уничтожением информации;

- аварии, пожары, технические катастрофы, стихийные бедствия.

1. Способы обеспечения ИБ

# Способы обеспечения ИБ

**По способам воздействия** на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические.

К **информационным** угрозам относятся:

- несанкционированный доступ к информационным ресурсам;

- незаконное копирование данных в информационных системах;

- хищение информации из библиотек, архивов, банков и баз данных;

- нарушение технологии обработки информации;

- противозаконный сбор и использование информации;

К **программным** угрозам относятся:

- использование ошибок в программном обеспечении;

- компьютерные вирусы и вредоносные программы;

К **физическим** угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;

- хищение носителей информации;

- хищение программных или аппаратных ключей и средств криптографической защиты данных;

1. Средства обеспечения ИБ

Организация информационной безопасности предполагает разработку определённых принципов её обеспечения.

Средства обеспечения информационной безопасности подразделяются на **формальные и неформальные.**

1. **Формальные средства защиты** – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

**К ним относятся:**

**Физические средства** - механические, электрические, электронные, устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия.

**Аппаратные средства** - механические, электрические, электронные, оптические, лазерные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

**Программные средства** - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем.

**Специфические средства -** к ним относятся криптографические методы защиты информации.

В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи.

Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную

1. **Неформальные средства защиты** – регламентируют деятельность человека.

**К ним относятся:**

**Законодательные средства** – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

**Организационные средства** - организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы.

Проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем.