**Информационные процессы -** процессы сбора, хранения, передачи, распространения, обработки информации

**Информационные технологии –** методы и СРЕДСТВА реализации информационных процессов.

**Стратегия развития информационного общества в РФ на 2017-2030 годы**

* Обеспечение прав граждан на доступ к информации
* Обеспечение свободы выбора средств получения знаний при работе с информацией
* Законность и разумная достаточность при сборе, хранении, накоплении и распространении информации
* Обеспечение государственной защиты интересов граждан РФ в информационной сфере

**Информационная сфера –** совокупность информации, информационных процессов, информационных технологий, главной целью которой является обеспечение общества информационными ресурсами

* Сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг
* Приоритет традиционных российских духовно-нравственных ценностей с соблюдением основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий

**Информационная безопасность –** состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз

**Защита информации –** комплекс организационных, технических и правовых мер, методов и средств, направленных на обеспечение конфиденциальности, целостности и доступности информации

**Информация –** сведения независимо от формы их представления

Свойства информации:

* **Доступность –** свойство информации находиться в состоянии готовности и используемости по запросу

Примеры тайн: служебная, коммерческая, тайна страхования, медицинская и т.д.

**Персональные данные –** любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу.

**Интеллектуальная собственность** – совокупность охраняемых результатов интеллектуальной деятельности и средств индивидуализации.

* **Конфиденциальность –** свойство информации быть недоступной и закрытой для неавторизованного пользователя, объекта или процесса
* **Целостность –** свойство информации быть невидоизмененной, а также ее защищенность от разрушения и несанкционированного изменения

Информационные процессы:

* **Хранение –** распространение информации во времени и пространстве
* **Обработка –** представление информации из одного вида в другой по определённому правилу
* **Передача –**перемещение информации от одного пользователя к другому

**Информационная безопасность автоматизированных систем –** область науки и техники, охватывающая совокупность программно-аппаратных, криптографических, технических и организационно-правовых методов и средств обеспечения безопасности информации в автоматизированных системах при ее сборе, хранении и передаче с использованием современных информационных технологий.

**Угроза –** потенциально-возможное событие, которое может нанести ущерб

**Угроза ИБ –** потенциально-возможное событие, которое может нанести ущерб состоянию защищенности данных

Виды угроз ИБ:

* **Естественные –** угрозы, вызванные окружающей средой, не связанные с деятельностью человека(короткое замыкание, природные катаклизмы, деятельность животных и др.)
* **Искусственные –** угрозы, связанные с деятельностью человека. Они делятся на:
  + - **Преднамеренные (умышленные)** – заранее спланированные с целью получения выгоды
    - **Непреднамеренные (случайные)**

**Информационная система –** совокупность технических средств и баз данных

ИС + персонал = АС

**Автоматизированная система –** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

АС + функция выдачи информации по запросам = АИС

**Автоматизированная информационная система –** комплекс программных и технических средств, предназначенных для сбора, хранения, поиска, выдаче информации по запросам.

**Злоумышленник –** нарушитель, намеренно идущий на нарушение из корыстных побуждений. (**нарушитель –** лицо, предпринявшее попытку выполнения запрещенных операций(действий) по ошибке, незнанию или осознанию со злым умыслом(из корыстных интересов) или без такового и использующее для этого различные возможности, методы и средства.)

**Государственная тайна –** защищаемые государством сведения в области:

* Военной
* Внешнеполитической
* Экономической
* Разведывательной
* Контрразведывательной
* Оперативно-розыскной

деятельности, распространение которых может нанести ущерб безопасности РФ

Уполномоченные лица:

* Президент РФ (глава совета безопасности)
* Правительство РФ
* Министерство обороны
* Палаты Федерального собрания
* Органы судебной власти

**Три грифа секретности:**

* 1форма. Особой важности
* 2форма. Совершенно секретно
* 3форма. Секретно

**Персональные данные –** любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу.

**ПД** делятся:

* **Общие ПД –** основные, базовые данные (ФИО, место регистрации и жительства, сведения об образовании, информация о месте работы/учёбы)
* **Биометрические ПД –** информация, которая есть с рождения(дактилоскопия, анализ ДНК, рост, цвет глаз, вес)
* **Специальные ПД** (национальная принадлежность и раса, вероисповедание, убеждения философского характера, информация о судимости, состояние здоровья, предпочтения в интимной жизни)
* **Обезличенные (общедоступные) ПД –** персональные данные, которые можно найти в адресной книге и справочниках.

**\*Обработка только для биометрических и специальных ПД не допускается без согласия в письменной форме субъекта ПД!!!!!**

**Ф.З:**

1)N 149-ФЗ. «Об информации, информационных технологиях и о защите информации». Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.

2) N 152-ФЗ «О персональных данных». Рассматривает основные термины и определения в области обеспечения безопасности самих ПД и процессов, связанных с их обработкой.

3) N 54-85 ФЗ. «О государственной тайне». Регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

4) N 390-ФЗ. «О безопасности». Раскрывает основы обеспечения безопасности личности, общества и государства.

**Компьютерный вирус –** вредоноснаяпрограмма, предназначенная для внедрения в файлы и системные области памяти ПК, иногда распространения по каналам связи. Важное свойство – способность размножаться

По среде обитания:

· **Сетевые** – распространяются по сетям.

· **Файловые** – инфицируют исполняемые файлы с расширениями .exe, .com.

· **Загрузочные** – внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record - MBR).

· **Файлово-загрузочные** – способны заражать и загрузочные секторы и файлы.

По способу заражения:

· **Резидентные** – оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения программ к ОС и внедряется в них.

· **Нерезидентные** – не заражают оперативную память и проявляют свою активность лишь однократно при запуске зараженной программы.

По степени опасности:

· **Неопасные** – например, на экране появляется сообщение: «Хочу чучу». Если набрать на клавиатуре слово «чуча», то вирус временно «успокаивается».

· **Опасные** – уничтожают часть файлов на диске.

· **Очень опасные** – самостоятельно форматируют жесткий диск.

По особенностям алгоритма:

· **Вирусы-компаньоны** – создают для ехе-файлов новые файлы-спутники, имеющие то же имя, но с расширением com. При запуске такого файла ОС первым обнаружит и выполнит com-файл, т.е. вирус, который затем запустит и ехе-файл.

· **Паразитические** – изменяют содержимое дисковых секторов или файлов.

· **Репликаторы (черви)** – распространяются в сети. Они проникают в память компьютера из сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

· **Невидимки (стелс)** – маскируют свое присутствие в ЭВМ, их трудно обнаружить.

· **Мутанты (призраки, полиморфные вирусы, полиморфики**) – их трудно обнаружить, т.к. их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды (мусор), которые не изменяют алгоритм работы вируса, но затрудняют их выявление.

· **Макро-вирусы** – используют возможности макроязыков, встроенных в системы обработки данных (Word, Excel).

· **«Троянские кони»** – маскируются под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT) или собирает на компьютере информацию, не подлежащую разглашению. Не обладают свойством самовоспроизводства.

По целостности:

· **Монолитные** – программа вируса - единый блок, который можно обнаружить после инфицирования.

· **Распределённые** – программа разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус.

**Роскомнадзор –** Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникацийявляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы. Согласно постановлению Правительства РФ от 16.03.2009 №228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»

Задачи:

1. Организация занимается тем, что внимательно следит за всей информацией, которая на государственном уровне поступает в средства массовой информации.
2. Электронные и массовые коммуникации постоянно проверяются на соответствие использования персональных данных каждого человека, пребывающего на территории государства.

Полномочия

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций осуществляет следующие полномочия:

1) **осуществляет:**

-государственный контроль и надзор: за соблюдением законодательства РФ в сфере средств массовой информации и массовых коммуникаций, телевизионного вещания и радиовещания; в сфере связи; в сфере информационных технологий; в сфере защиты детей от информации;

-лицензирование деятельности, в том числе контроль за соблюдением лицензионных условий и требований:

в области телевизионного вещания и радиовещания; в области оказания услуг связи;

- аккредитацию экспертов и экспертных организаций для проведения экспертизы информационной продукции в целях обеспечения информационной безопасности

- создание, формирование и ведение единой автоматизированной информационной системы

- принятие мер по ограничению доступа к информационным ресурсам в информационно-телекоммуникационных сетях,

-координацию обеспечения устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет";

- предоставление на безвозмездной основе операторам связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования;

- проведение мониторинга функционирования информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования в целях выявления угроз устойчивости, безопасности и целостности функционирования указанных сетей на территории Российской Федерации;

- обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям Федерального закона "О персональных данных" и принятых в соответствии с ним нормативных правовых актов;

**2) ведет:**

- реестр операторов

- реестр зарегистрированных средств массовой информации;

- реестры лицензий;

- реестр экспертов и экспертных организаций

- реестр зарегистрированных радиоэлектронных средств и высокочастотных устройств;

**3) устанавливает:**

- порядок представления в лицензирующий орган сведений об операторах связи

- порядок ведения регистрирующим органом реестра зарегистрированных средств массовой информации;

- порядок аккредитации экспертов и экспертных организаций на право проведения экспертизы информационной продукции

- порядок подачи заявления о регистрации средства массовой информации

- порядок аннулирования разрешения на распространение продукции зарубежного периодического печатного издания на территории Российской Федерации;

- перечень групп доменных имен, составляющих российскую национальную доменную зону;

- технические условия установки технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования

**4) организует:**

-проведение работ по изысканию новых радиочастотных каналов и разработке радиочастотного спектра и орбитальных позиций спутников для целей телевизионного вещания и радиовещания;

- деятельность радиочастотной службы;

- проведение торгов на получение лицензий в области связи;

- проведение экспертизы информационной продукции в целях обеспечения информационной безопасности;

**5) регистрирует:**

- средства массовой информации;

- радиоэлектронные средства и высокочастотные устройства гражданского назначения;

- сети электросвязи, входящие в сеть связи общего пользования, подлежащие регистрации в соответствии с законодательством Российской Федерации;

**6) выдает разрешения:**

- на строительство, реконструкцию, проведение изыскательских работ для проектирования и ликвидацию сухопутных линий связи при пересечении государственной границы Российской Федерации и на приграничной территории;

- на судовые радиостанции, используемые на морских судах, судах внутреннего внешнего плавания;

**Роскомнадзор с целью реализации полномочий в установленной сфере ведения имеет право**:

-запрашивать и получать в установленном порядке сведения, необходимые для принятия решений по вопросам, отнесенным к компетенции Службы;

- проводить необходимые расследования, испытания, экспертизы, анализы и оценки, а также научные исследования по вопросам, отнесенным к компетенции Службы;

- привлекать в установленном порядке для проработки вопросов, отнесенных к компетенции Службы, научные и иные организации, а также ученых и специалистов;

- давать государственным органам, органам местного самоуправления, юридическим и физическим лицам разъяснения по вопросам, отнесенным к компетенции Службы;

- в порядке и случаях, которые установлены законодательством Российской Федерации, применять в установленной сфере ведения меры профилактического и пресекательного характера

- создавать совещательные и экспертные органы