Лекция №1

Введение в информационную безопасность. Методы защиты информации. Основные понятия и подходы.

Информационная безопасность – состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. (за 2001 год)

Информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства (5 декабря 2016г).

В более узком смысле, под информационной безопасностью понимают состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Защита информации **–** комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

Важно отметить, что *информационная безопасность* – это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.

Основные понятия и определения

- Под информацией (в узком смысле) понимают сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах.
- Под субъектом информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.
- К поддерживающей инфраструктуре относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, **обслуживающий персонал** (текущие, будущие и прошлые).
- Информационная угроза **–** потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации.
- Ущерб может быть **приемлемым** или **неприемлемым**.

Концепция информационной безопасности должна отвечать на три вопроса:

- Что защищать?
- От чего (кого) защищать? (создание модели угроз)
- Как защищать?

Объекты обеспечения информационной безопасности

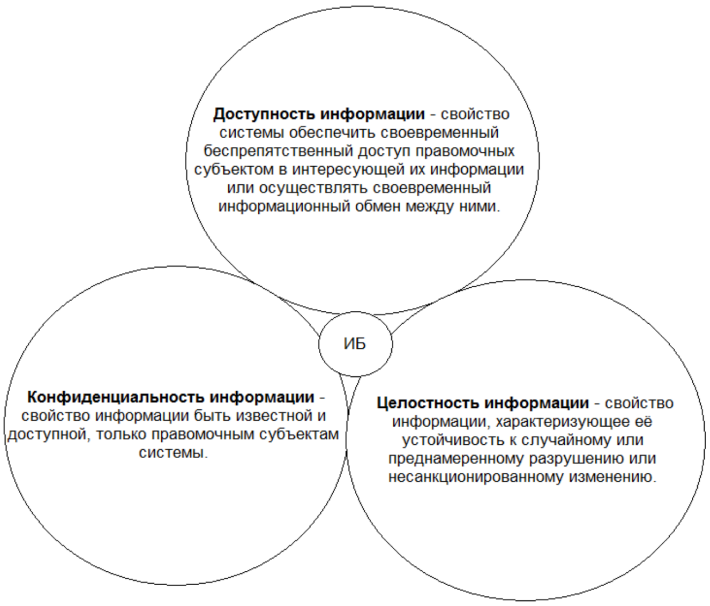
- информационные ресурсы;
- система создания, распространения и использования информационных ресурсов;
- информационная инфраструктура общества (информационные коммуникации, сети связи, центра анализа и обработки данных, системы и средства защиты информации);
- средства массовой информации;
- права человека и государства на получение, распространение и использование информации;
- защита интеллектуальной собственности и конфиденциальной информации.

Основные составляющие информационной безопасности

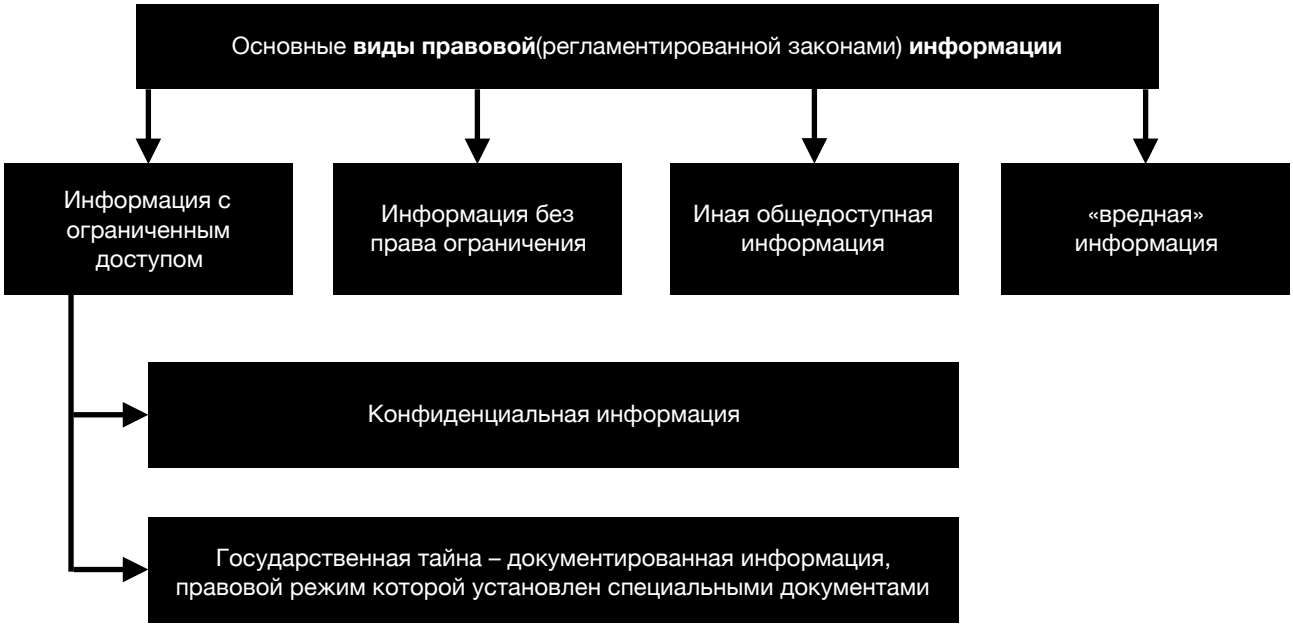
Обеспечение безопасности информации складывается из трёх составляющих:
- Конфиденциальности;
- Целостности;
- Доступности.

Точками приложения процесса защиты информации к информационной системе являются:
- аппаратное обеспечение,
- программное обеспечение
- обеспечение связи(коммуникации)

Сами процедуры (механизмы) защиты разделяются на
- защиту физического уровня,
- защиту персонала
- организационный уровень



Виды, категории информации. ИсОД



Виды конфиденциальной информации

- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца по официальной публикации информации о них;
- персональные данные;(Закон РФ «О персональных данных» права субъектов персональных данных:
  - Информационное самоопределение;
  - Доступ к своим персональным данным;
  - Внесение изменений в свои персональные данные;
  - Блокирование персональных данных;
  - Обжалование неправомерных действий в отношении персональных данных;
  - Возмещение ущерба.)
- любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу;
- это информация ограниченного доступа, но она является полностью открытой для субъекта персональных данных.

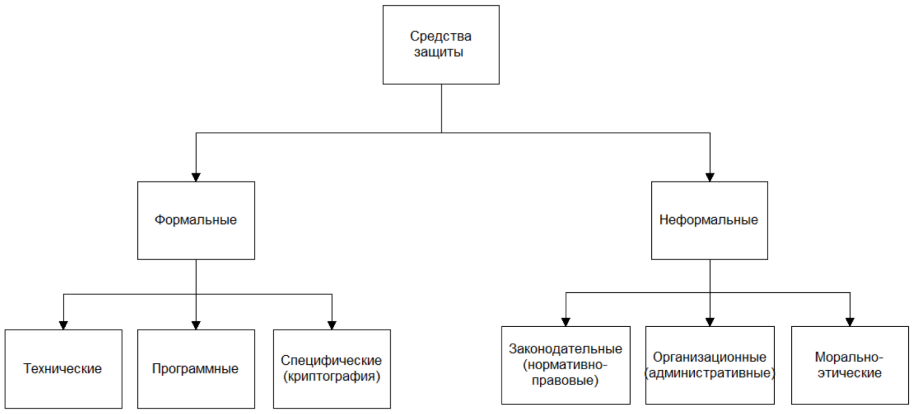
Угроза безопасности компьютерной системы – это потенциально возможное происшествие (преднамеренное или нет), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Источники информационных угроз	
Внешние	Внутренние
Политика стран	Отставание по уровню информатизации
Информационная война	Отставание по технологии
Преступная деятельность	Недостающий уровень образования
Прочие источники	Прочие источники

Виды информационных угроз	
Преднамеренные	Случайные
Хищение информации	Ошибки пользователя
Компьютерные вирусы	Ошибки профессионалов
Физические воздействие на аппаратуру	Отказы и сбои аппаратуры
	Форс-мажорные обстоятельства

Политика безопасности – это комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность.

↓ Законодательный уровень
↓ Административный уровень
↓ Процедурный уровень
↓ Программно-технический уровень(техническая, аппаратная, программная защита)



Организационная защита

- *организация режима и охраны*;
- *организация работы с сотрудниками* (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.);
- *организация работы с документами* и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации);
- *организация использования технических средств* сбора, обработки, накопления и хранения конфиденциальной информации;
- *организация работы по анализу внутренних и внешних угроз* конфиденциальной информации и выработке мер по обеспечению её защиты;
- *организация работы по проведению систематического контроля за работой персонала* с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.
-

Технические средства защиты информации

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдении
- система контроля и управления доступом(СКУД).
- Защита информации от её утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:
- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем зашумления;
- создание контролируемых зон.

Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, кодов, грифов, уровней секретности.

- Устройства измерения индивидуальных характеристик человека периодической проверки адреса выдачи данных.
- Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- Устройства для шифрования информации (криптографические методы).
- Системы бесперебойного питания:
  - Источники бесперебойного питания;
  - Резервирование нагрузки;
  - Генераторы напряжения.

1. Идентификация **–** название лицом себя системе.(Ты кто такой?)
2. Аутентификация – установления соответствия лица названному им идентификатору. (Чем докажешь?)
3. *Авторизация* – предоставления этому лицу возможностей в соответствие с положенным ему правами ли проверка наличия прав при попытке выполнить какое-либо действие. (Что можешь делать?)

Программные средства защиты информации

- Средства защиты от несанкционированного доступа(НСД):
  - Средства авторизации;
  - Мандатные к правление доступом;
  - Избирательное управление доступом;
  - Управление доступом на основе ролей;
  - Журналирование (так же называется Аудит).
- Система анализа и моделирования информационных потоков (CASE – системы).
- Системы мониторинга сетей:
  - Системы обнаружения и предотвращения вторжений(IDP/IPS);
  - Системы предотвращения утечек конфиденциальной информации(DLP-системы).
- Анализаторы протоколов.
- Антивирусные средства.
- Межсетевые экраны.
- Криптографические средства:
  - Шифрование;
  - Цифровая подпись.
- Системы резервного копирования.
- Системы аутентификации:
  - Пароль;
  - Ключ доступа(физический или электронный);
  - Сертификат;
  - Биометрия.
- Инструментальные средства анализа систем защиты:
  - Мониторинговый программный продукт.