

# Защита компьютерной информации

Михальцов П.А.

20 января 2020 г.

## 1 Защита информации в информационно вычислительных системах

### 1.1 Проблемы защиты компьютерной информации

Вопросы

1. Основные понятия об угрозах информационной безопасности
2. Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации
3. Задачи информационной безопасности

#### 1.1.1 Основные понятия об угрозах информационной безопасности

**Информационная безопасность** — такое состояние системы, при которой она может противостоять против дестабилизирующим воздействиям внешних и внутренних угроз, а также — её функционирования не создаёт информационных угроз для элементов самой системы и внешней среды

Обеспечение информационной безопасности проблемы может быть достигнуто лишь при взаимоувязанном решении трёх составляющих проблем:

- защита находящееся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации
- защита элементов системы от дестабилизирующих воздействия внешних и внутренних информационных угроз
- защита внешней среды от информационной угроз со стороны рассматриваемой системы

Под **защитой информации** понимать совокупность мероприятий и действий, направленных на обеспечение её безопасности – конфиденциальность и целостность – в процессе сбора, перердачи, обработки и хранения.

**Безопасность информации** - это свойство (состояние) передаваемой накапливаемой, обрабатываемой и хранимой информации, характеризующие её степень защищенности от дестабилизирующего воздействия внешней среды и внутренних угроз то есть её конфиденциальность, сигнальная скрытность (энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам.

Под **защитой информации** в более широком смысле понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

**Защита информации направлена на:**

- предупреждение угроз как превентивных мер по обеспечению безопасности в интересах учреждения возможности их возникновения.

- выявление угроз, которое выражается в систематическом анализе и контроле возможности появления реальных и потенциальных угроз и своевременных мер по их предупреждению.
- обнаружение угроз, целью которого является определение реальных угрозы или конкретных преступных деятельности.
- ликвидацию последствий угроз и преступных действий и восстановления статуса-кво.

**Обнаружение угроз** — это действие по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба.

**Пресечение или локализация угроз** — это действие, направленное на устранение действующей угрозы и конкретных преступных действий

Ликвидация последствий имеет целью восстановлению состояния, предшествовавшего наступлению угрозы.

### **1.1.2 Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации**

Актуальность и важность информационной безопасности (ИБ) обусловлена следующими факторами:

- высокие темпы роста парка ПК, применимых в разных сферах деятельности, и как следствие, резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным сетям и информационным ресурсам.
- увеличение объемов информации с помощью ПК и др. средств автоматизации
- бурное развитие аппаратно-программных средств и технологий не удовлетворяющих современных ТБ.
- несоответствию развития средств обработки информации и проработки теорий ИБ разработки международных стандартов и

правовых норм, обеспечивающих необходимый уровень ЗИ защиты информации

- повсеместное распространения сетевых технологий, создание единого информационно-коммуникативной сети Интернет, которая не может обеспечить достойного уровня ИБ.

### **Цели защиты информации являются**

- предотвращения утечки хищения утраты искажения подделки информации
- предотвращение угроз безопасности личности, общества, государства.
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копирования, блокировки информации.
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы
- обеспечение правового режима документированной информации как объекта собственности
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах
- сохранение государственной тайны документированной информации в соответствии с законодательством
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения

### 1.1.3 Задачи информационной безопасности

**Основные задачи системы ИБ являются**

- своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующей нанесению финансовой или другого ущерба.
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия.
- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и технических мер и средств обеспечения безопасности
- Создание условий для возмещения и локализации нанесённого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушений безопасности на достижение целей организаций

## 1.2 Угрозы безопасности в информационно вычислительных системах

Вопросы

- Понятия угрозы безопасности
- Актуальность проблемы обеспечения информационной безопасности
- Задачи защиты информации
- Задачи информационной безопасности

**Угроза** — это потенциальное возможное событие, действия (воздействия), процесс или явления, которые могут привести к нанесению ущерба чьим-либо интересам.

Существуют три разновидности угроз

- Угрозы нарушения конфиденциальности
- Угрозы нанесения целостности
- Угрозы отказа служб

**Угроза нарушения конфиденциальности** — информация становится известна тому, кто не располагает полномочиями к ней

**Угроза нарушения целостности** — включает в себя любое умышленное изменение информации, хранящейся в себе (вычислительной системы) или передаваемой из одной системы в другую.

**Угроза отказа служб** — когда в результате преднамеренных действий предпринимаемый другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

**Доступность информации** — это свойство системы (среды, средств и технологий обработки), в которой циркулирует информация, характеризующая способность обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и

готовность соответствующему автоматизированных служб к обслуживанию от субъектов запросов всегда, когда в обращении к ним.

Классификация угроз информационной безопасности

- По природе возникновения
- По степени преднамеренности появления
  1. появление ошибок в программно-аппаратных средств АС
  2. некомпетентное использование или настройка или неправомерное средств защиты персоналом службы безопасности
  3. неумышленное действие, приводящая к частичному или полному отказу системы или разрушения аппаратных, программных, информационных ресурсов системы
  4. Неправомерное включение оборудования или изменение режимов работы устройств и программ
  5. Неумышленная порча носителей информации
  6. Пересылка данных по ошибочному адресу абонента(устройства)
  7. Ввод ошибочных данных
  8. Неумышленное повреждение каналов связи
- Угрозы преднамеренного действия
  1. Традиционный или универсальный шпионаж и диверсия.
  2. Несанкционированный доступ к информации
  3. Несанкционирование модификация структур
  4. Информационные инфекции
  - 5.