

# РАЗНОВИДНОСТИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1) Конфиденциальность

2) Целостность

3) Доступность

# КЛАССИФИКАЦИЯ ВИДОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Внутренний отказ информационной системы

- нарушение от установленных правил эксплуатации
- выход системы из штатного режима эксплуатации
- ошибки при (пере)конфигурировании системы
- Вредоносное программное обеспечение
- отказы программного и аппаратного обеспечения
- разрушение данных
- разрушение или повреждение аппаратуры

## Отказ поддерживающей инфраструктуры

- нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
- разрушение или повреждение помещений
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности

## Статическая

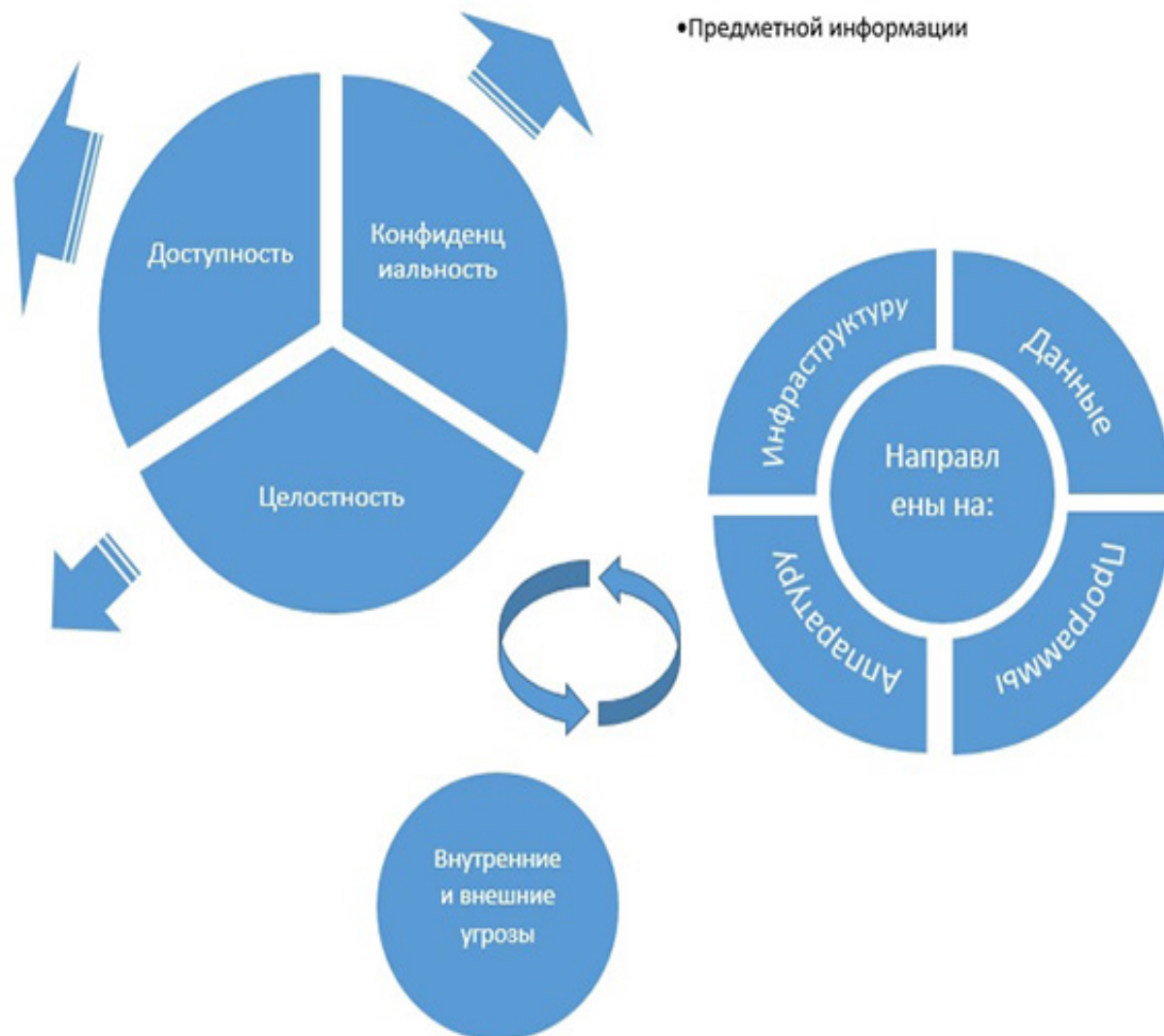
- Добавление неверных данных
- Изменение данных

## Динамическая

- переупорядочение
- кража
- дублирование
- внесение дополнительных сообщений

## Угрозы

- Служебной информации
- Предметной информации



# ВИДЫ ИНФОРМАЦИОННЫХ УГРОЗ



# ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

- 1) Аппаратное обеспечение
- 2) Программное обеспечение
- 3) Обеспечение коммуникации.

# КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1) По аспекту информационной безопасности, на который направлены угрозы:

- ✓ Угрозы конфиденциальности (неправомерный доступ к информации).
- ✓ Угрозы целостности (неправомерное изменение данных).
- ✓ Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

2) По расположению источника угроз:

- ✓ Внутренние (источники угроз располагаются внутри системы);
- ✓ Внешние (источники угроз находятся вне системы).

3) По размерам наносимого ущерба:

- ✓ Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);
- ✓ Локальные (причинение вреда отдельным частям объекта безопасности);
- ✓ Частные (причинение вреда отдельным свойствам элементов объекта безопасности).

# КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4) По степени воздействия на информационную систему:

Пассивные (структура и содержание системы не изменяются);

Активные (структура и содержание системы подвергается изменениям).

5) По природе возникновения:

- Естественные (объективные) — вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;

- Искусственные (субъективные) — вызванные воздействием на информационную сферу человека. Среди искусственных угроз в свою очередь выделяют:

- а) Непреднамеренные (случайные) угрозы — ошибки программного обеспечения, персонала, сбои в работе систем, отказы вычислительной и коммуникационной техники;

- б) Преднамеренные (умышленные) угрозы — неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д.

# ОСНОВНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ

- 1) Анализ угроз  
информационной  
безопасности 2016-2017
- 2) Исследование: угрозы  
информационной  
безопасности.



# ГРУППЫ ИСТОЧНИКОВ УГРОЗ ИБ

**1) Обусловленные действиями субъекта (антропогенные источники)** – субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры.

**2) Обусловленные техническими средствами (техногенные источники)** – эти источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними.

**3) Стихийные источники** – данная группа объединяет обстоятельства, составляющие непреодолимую силу, такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию и, поэтому меры против них должны применяться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

# КЛАССИФИКАЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ



# КОМПЬЮТЕРНЫЕ ВИРУСЫ

Это вредоносные программы способные создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

# КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

1) по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

2) файловые вирусы делят по механизму заражения;

3) по поражаемым операционным системам и платформам;

4) по технологиям, используемым вирусом\алгоритму работы (полиморфные вирусы, стелс-вирусы, руткиты);

5) по языку, на котором написан вирус;

6) по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты).

**Троянская программа** — разновидность вируса, проникающая в компьютер под видом легального программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, её разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях.

**Сетевой червь** — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.