Лекция 3,4. Причины кризиса информационной безопасности. Модель нарушителя. Модель угроз.

Профессор, д.т.н., П.Д. Зегжда
Санкт-Петербургский политехнический университет Петра Великого

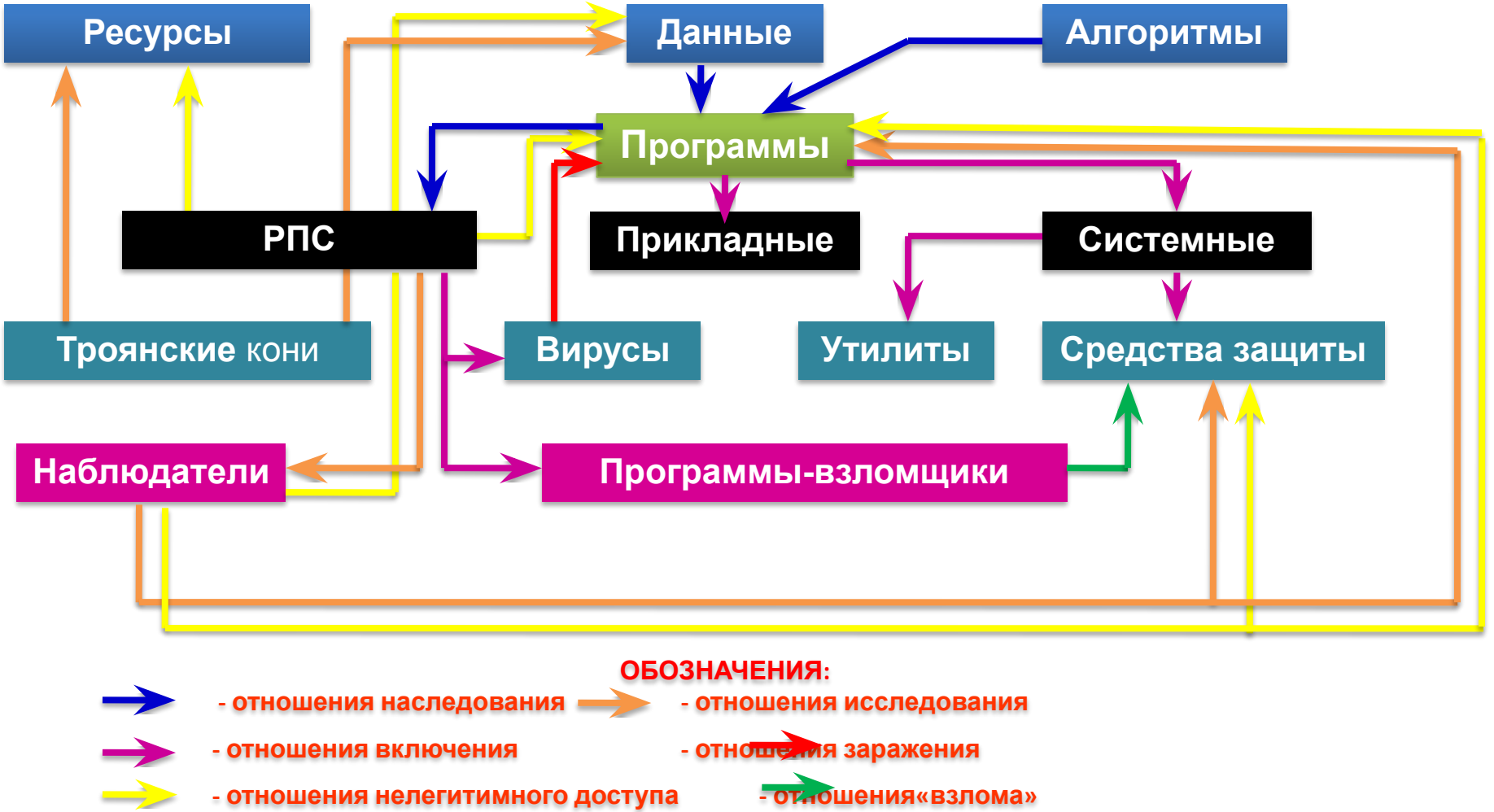
ОСНОВНЫЕ ФАКТОРЫ, ПРЕДОПРЕДЕЛИВШИЕ СУЩЕСТВОВАНИЕ ВРЕДОНОСНЫХ ПРОГРАММ (РПС)

1) Невозможность отделить исполняемый код от данных в компьютере фоннеймановской архитектуры. Поэтому всегда имеется возможность вместе с данными внести в компьютерную систему исполняемый код, выполнение которого в последствии непредсказуемо.
2) Невозможно указать формальные признаки, по которым РПС отличается от пользовательской программы. Многие пользовательские программы совершают действия сканирования или разрушения других программ, например, дизассемблеры, анализаторы трафика в распределённых сетях, системы сканирования защиты).
3) Наличие во всех сложных программных комплексах встроенных отладчиков. Вызов такого отладчика позволяет нарушителю отключить системы защиты, полностью разрушить систему или изменить права доступа.
4) Большинство сложных программных систем содержат встроенные интерпретаторы других языков (машинных). Фактически это приводит к тому, что внутри вычислительной системы строится другая вычислительная система. Защита должна быть на всех уровнях.
5) Наличие уязвимостей и ошибок, т.е. непредсказуемых свойств программной системы.

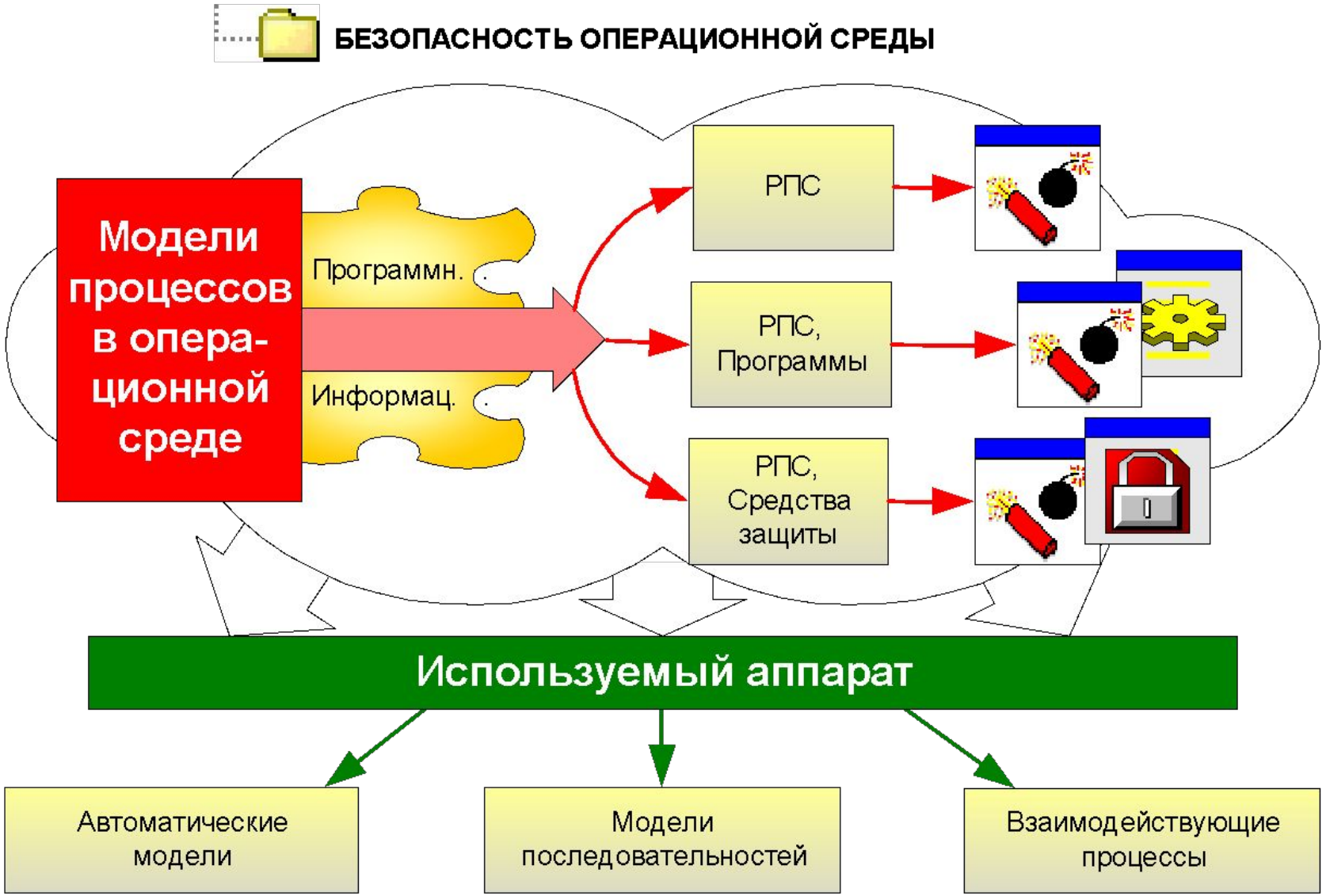
ТИПЫ РПС


РПС
Функция воспроизведения
Функция преодоления защиты
Функция нанесения ущерба
Функция сбора информации (разведка)
Компьютерные вирусы
Средства проникновения в удалённые системы
Троянские кони
Контроль действий
Сетевые черви
Программные закладки
Дублирование сообщений

КЛАССЫ ОБЪЕКТНО-КОНЦЕПТУАЛЬНОЙ МОДЕЛИ ВС И РПС И ОТНОШЕНИЯ МЕЖДУ НИМИ



ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИБКС

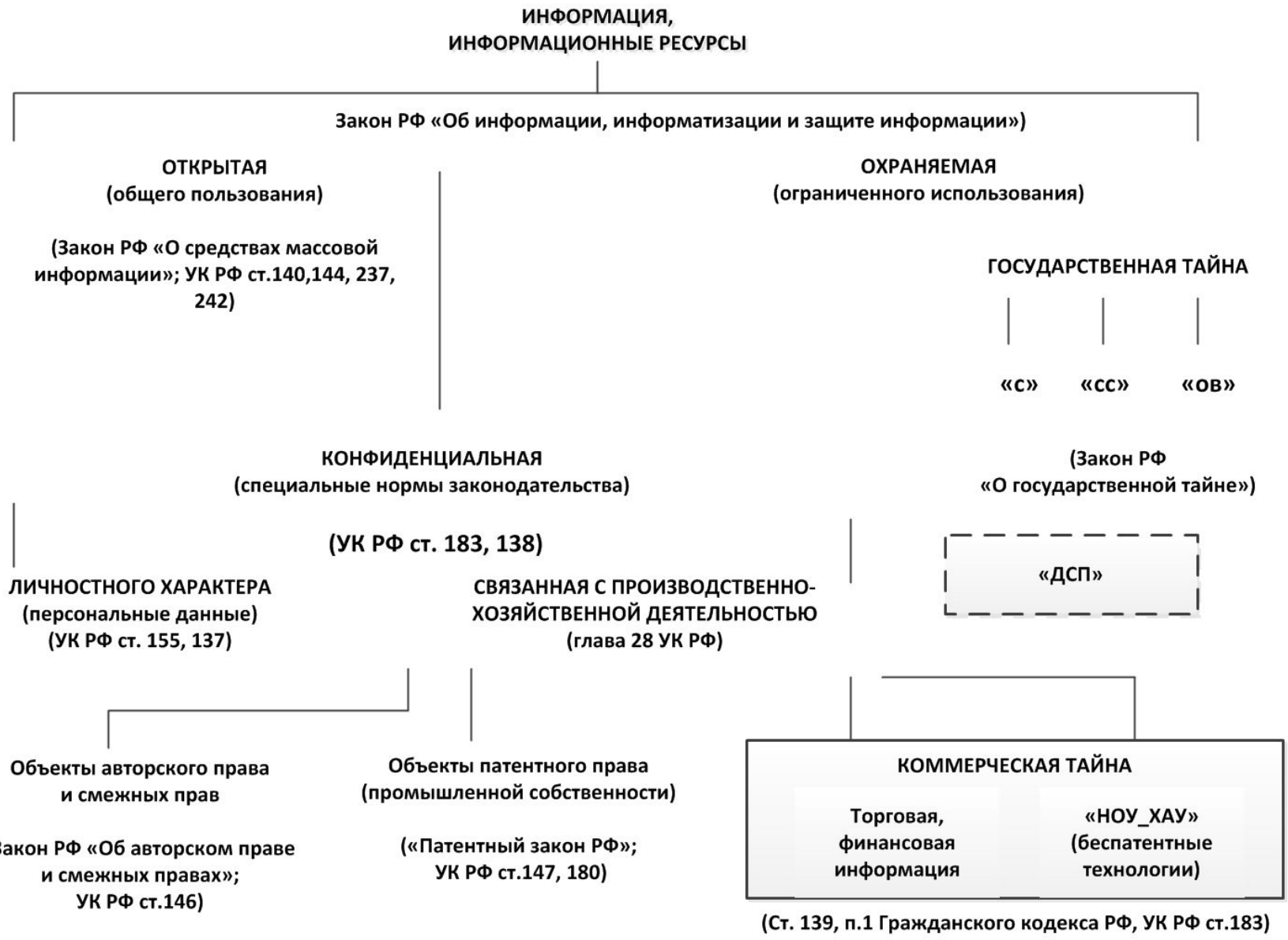


ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИБКС

Легче переносить терпеливо то, что нам не дано исправить.
Квинт Гораций Флакк

Специфика правового обеспечения информационной безопасности

СТРУКТУРА ИНФОРМАЦИОННЫХ РЕСУРСОВ



ОСОБЕННОСТИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

1) Трудности определения момента преступления и его локализации;
2) Трудности определения источника нападения;
3) Специфика доказательства участия.

ОТВЕТСТВЕННОСТЬ СТОРОН ИНФОРМАЦИОННОГО ОБМЕНА

Уголовную ответственность за нарушение информационной безопасности устанавливают статьи 272-274 Уголовного кодекса РФ. Статья 272 описывает ответственность за неправомерный доступ к компьютерной информации, статья 273 – ответственность за создание, использование и распространение вредоносных программ для ЭВМ, статья 274 – ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации несет лицо, оказывающее услуги по передаче информации.

ОСОБЕННОСТИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Обладатель информации, обязан обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов нарушения;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации;

5) возможность незамедлительного восстановления информации;

6) постоянный контроль за обеспечением уровня защищенности.

ЯВЛЕНИЕ ХАКЕРСТВА

- Неоднозначная роль хакеров и их цели;
- Хакерство как соревнование профессионалов, олимпиады и конкурсы;
- Систематизация хакеров (нарушителей);
- Опасность хакерства (связь с преступлением).

Сертификация и лицензирование в области защиты информации

СЕРТИФИКАЦИЯ

Сертификация средства защиты информации включает в себя процесс верификации того, что данное средство выполняет поставленные перед ним задачи и обеспечивает указанную степень безопасности. Такая верификация производится путем исследования и испытаний средства специальной лаборатории. По окончании сертификации при успешном прохождении испытаний производителю средства выдается документ – сертификат.

СИСТЕМА СЕРТИФИКАЦИИ

- Государственная
  - ФСТЭК
  - ФСБ
  - Минобороны
  - Государственные организации
  - …
- Отраслевая
  - Атомпром
  - Газпром
  - Минздрав
  - …
- Добровольная
  - Система ISO
  - Международная стандартизация
  - Страховая сертификация
  - …

УЧАСТНИКИ СЕРТИФИКАЦИИ

В сертификации принимают участие:

- Федеральный орган по сертификации;
- Центральный орган системы сертификации (создается при необходимости);
- Органы, проводящие сертификацию определенной продукции;
- Испытательные лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;
- Изготовители-продавцы, исполнители продукции.

НАРУШИТЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нарушитель, это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (возможно, из корыстных побуждений) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.
Очевидно, понятие нарушителя не всегда совпадает с понятием злоумышленника.

Классификация по поставленной задаче:

1. **Хакер** – оценка слабых мест системы
2. **Кракер** – нарушитель – злоумышленник
3. **Вандал** – разрушение ради сенсации
4. **Шутник** – разрушение без злого умысла
5. **Взломщик** – профессиональный кракер
6. **Вымогатель** – нарушители ради шантажа
7. **Террорист** – вывод системы из строя с политической целью

СИСТЕМАТИЗАЦИЯ НАРУШИТЕЛЕЙ

ЦЕЛИ И МЕТОДЫ НАРУШИТЕЛЕЙ

Цели нарушителя:

1. **Раскрытие информации или факта ее существования**
2. **Вызов отказа в обслуживании**
3. **Прерывание корректной операции пользователя**
4. **Получение неограниченного контроля над вычислительной системой**

Методы нарушителя:

1. **Перехват** – пассивное воздействие при котором нарушитель прослушивает канал связи
2. **Модификация** – активное воздействие – с целью подлога данных или отказа в обслуживании или получении контроля над системой
3. **Маскарад** – подделка данных идентифицирующих активную сущность
4. **Ложное опровержение авторства** (одна из форм подлога)
5. **Задержка обслуживания** – временное прекращение обслуживания
6. **Отказ в обслуживание** – форма монополизации контроля над вычислительной системой

МОДЕЛИ НАРУШИТЕЛЕЙ ПО ФСТЭК

1 УРОВЕНЬ:

определяет самый низкий уровень возможностей ведения диалога в автоматизированной системе – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

2 УРОВЕНЬ:

определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

3 УРОВЕНЬ:

определяется возможностью управления функционированием автоматизированных систем, т. е. воздействием на базовое программное обеспечение системы и на состав и кон- фигурацию ее оборудования.

4 УРОВЕНЬ:

определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированных систем, вплоть до включения б состав средств вычислительной техники собственных технических средств с новыми функциями по обработке информации.

Понятие угрозы
Систематизация и модели угроз

НЕДОСТАТКИ ОС, ДЕЛАЮЩИЕ НЕИЗБЕЖНЫМ СУЩЕСТВОВАНИЕ УГРОЗ

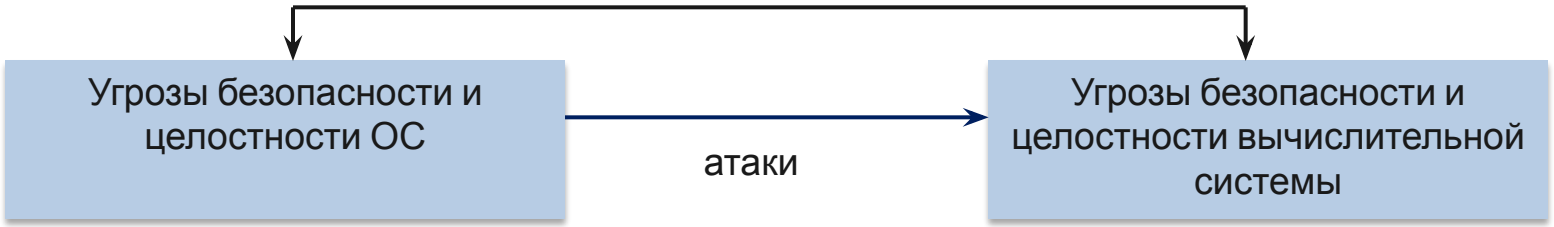


Рисунок - Связь между ОС и угрозами безопасности

Причины нарушения безопасности ОС	Требования ФСТЭК	Требования «оранжевой книги»
Неправильный выбор модели безопасности	**Управление доступом. Регистрация и учет**	**Политика безопасности**
Неправильное внедрение модели безопасности	**Управление доступом**	**Политика безопасности. Непрерывность защиты**
Ошибки в программной реализации системы защиты	**Обеспечение целостности**	**Непрерывность защиты**
Недостаточная надежность идентификации и аутентификации субъектов и объектов	**Управление доступом. Регистрация и учет**	**Идентификация и аутентификация**
Недостаточный контроль целостности механизмов, реализующих функции защиты	**Обеспечение целостности**	**Целостность. Адекватность. Непрерывность**
Наличие «люков», отладочных возможностей и т.д.	**Обеспечение целостности**	**Целостность. непрерывность**

ОШИБКИ В СИСТЕМАХ ЗАЩИТЫ

<table>
<tr><td rowspan="8">Ошибки в системах защиты, служащие источником появления уязвимостей</td><td rowspan="5">Преднамеренные</td><td rowspan="3">С наличием деструктивных функций (активные)</td><td rowspan="2">Разрушающие программные средства (РПС)</td><td>Не самовоспроизводящиеся РПС(“троянские кони”)</td></tr>
<tr><td>Самовоспроизводящиеся РПС (вирусы)</td></tr>
<tr><td colspan="2">Черные ходы, люки, Проникновения в скрытые возможности систему</td></tr>
<tr><td rowspan="3">Без деструктивных Функций (пассивные)</td><td rowspan="2">Скрытые каналы утечки информации</td><td>С использованием памяти</td></tr>
<tr><td>С использованием времени</td></tr>
<tr><td colspan="2">Другие</td></tr>
<tr><td rowspan="4">Непреднамеренные (случайные)</td><td colspan="3">Ошибки контроля допустимых значений параметров.</td></tr>
<tr><td colspan="3">Ошибки определения областей (доменов)</td></tr>
<tr><td colspan="3">Ошибки последовательности действий и использования нескольких имен для одного объекта</td></tr>
<tr><td colspan="3">Ошибки идентификации/аутентификации.</td></tr>
<tr><td colspan="4">Другие ошибки в логике функционирования</td></tr>
</table>

Виды угроз безопасности информации в компьютерных системах

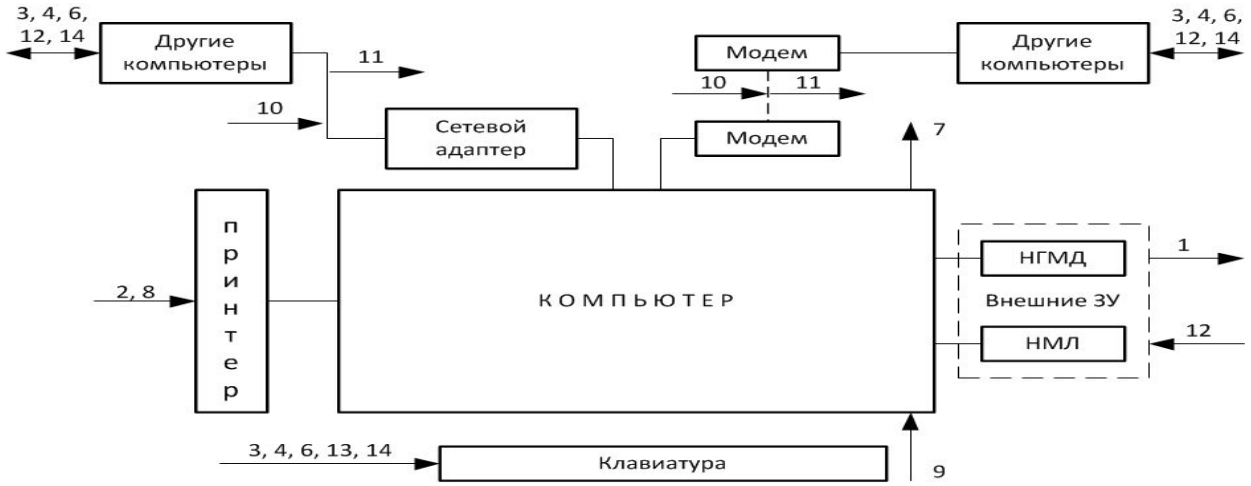


Схема угроз безопасности информации в компьютерных системах

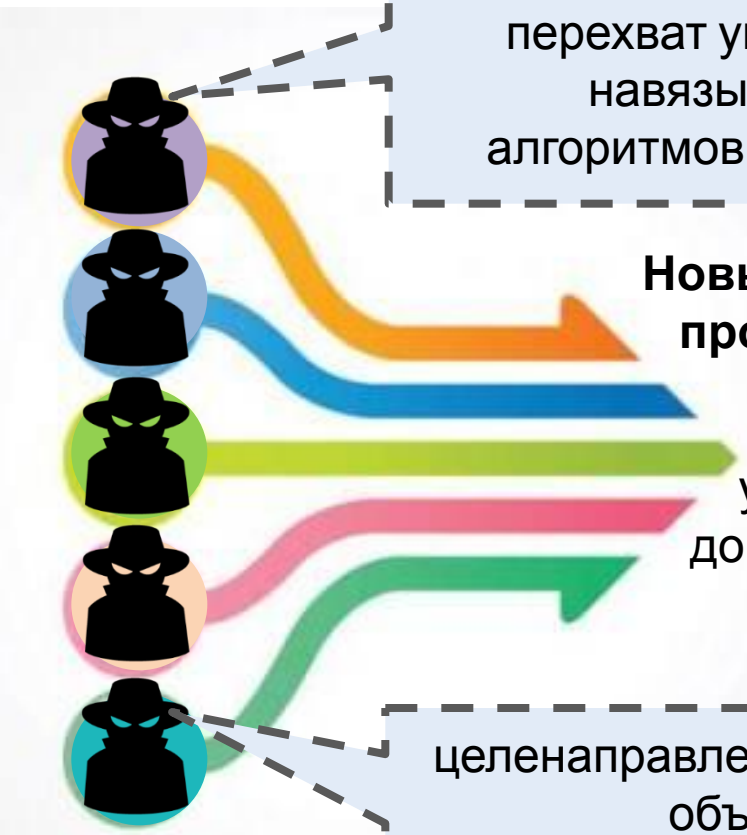
ПОНЯТИЕ КИБЕРУГРОЗЫ

Киберугроза – целенаправленное вредоносное воздействие на телекоммуникационные и компьютерные системы, **являющиеся элементами киберфизических систем**, реализованное с помощью компьютерных и информационных технологий.

ОТЛИЧИЯ КИБЕРУГРОЗ ОТ ТРАДИЦИОННЫХ УГРОЗ ИБ

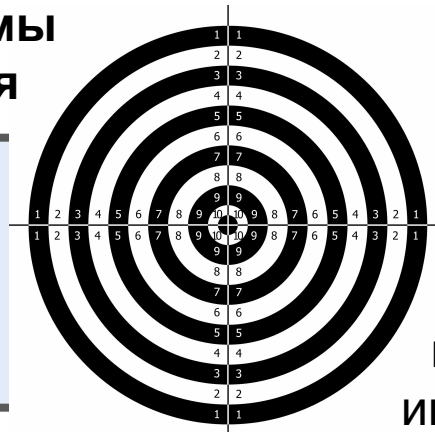
Новые цели

перехват управления и навязывание своих алгоритмов управления



Новые механизмы проникновения

от поиска уязвимостей до социальной инженерии



Новые объекты атаки

информационная инфраструктура → управляющие контроллеры → исполнительные механизмы →

целенаправленный выбор объекта атаки и планирование кибероперацій

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

это совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию информационных технологий или его владельцу

По источникам:

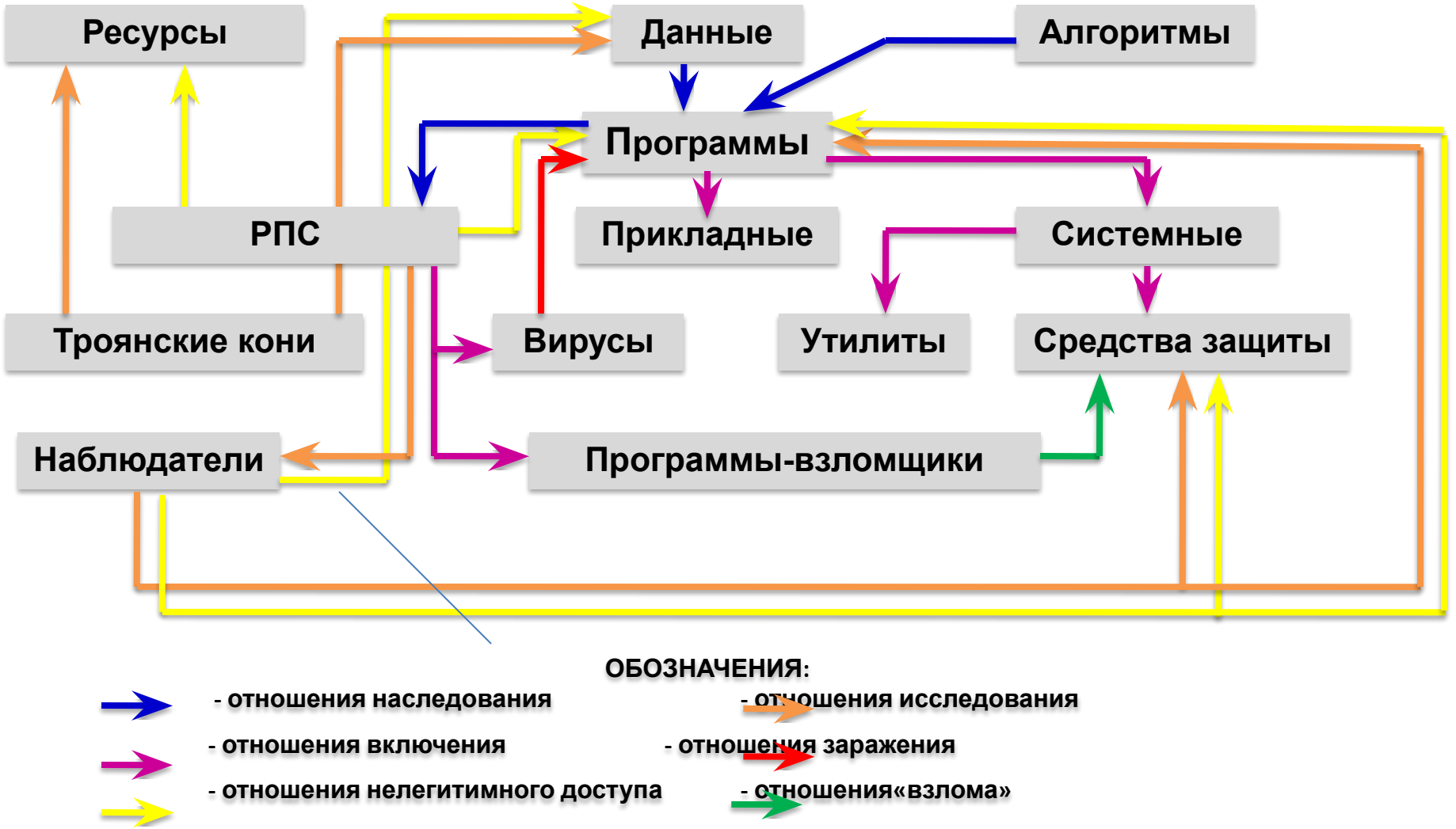
1. **Угрозы, существование которых обусловлено человеческим фактором.** К примеру, оператор может случайно удалить файлы, нечаянно сообщить пароль злоумышленнику и т.п.
2. **Угрозы, связанные с воздействиями через физические поля.** К таким угрозам относятся, например, угроза утечки информации из канала связи через электромагнитное поле, угроза съема данных через акустические поля и т. д.
3. **Угрозы, связанные с компьютерной обработкой информации.**
   а) угрозы со стороны технических средств вычислительной системы; это угроза внедрения в компьютерную систему или канал связи стороннего устройства (закладки)
   б) угрозы со стороны программно-алгоритмических средств, это угрозы внесения в компьютерную систему специальных программ

СИСТЕМАТИЗАЦИЯ УГРОЗ

1. **Угрозы направленные на нарушение конфиденциальности информации – угрозы раскрытия**
2. **Угрозы направленные на нарушение целостности информации**
3. **Угрозы направленные на нарушение доступности информации или другого ресурса вычислительной системы – угрозы отказа в обслуживании**

1. Угрозы, нарушения конфиденциальности (раскрытия) информации заключается в том, что информация становится известной не полномочному на то лицу
2. Угроза нарушения целостности информации подразумевает наличие любой возможности несанкционированного изменения информации
3. Угроза нарушения целостности в общем случае относится не только к данным но и к программам
4. Под целостностью информации необходимо иметь ввиду не только проблемы, связанные с несанкционированной модификацией данных но и вопросы связанные со степенью доверия к источнику
5. Угроза нарушения доступности (угроза отказа в обслуживании) – любая возможность блокирования доступа к некоторому ресурсу вычислительной системы

КЛАССЫ ОБЪЕКТНО-КОНЦЕПТУАЛЬНОЙ МОДЕЛИ ВС И РПС И ОТНОШЕНИЯ МЕЖДУ НИМИ

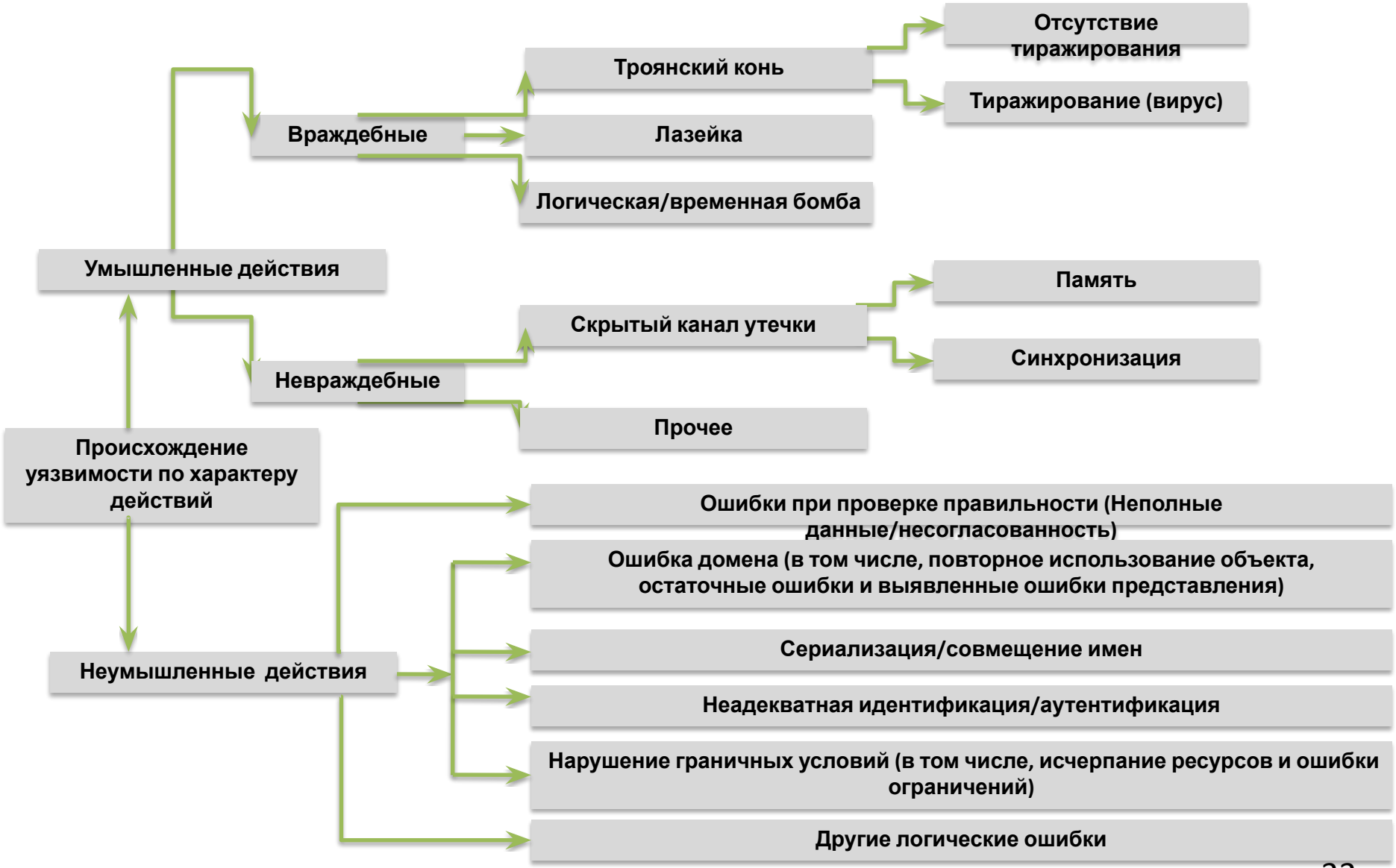


МОДЕЛЬ КИБЕРАТАК ГОВАРДА

МОДЕЛЬ АМОРОСО

Результат	Операторы	Программисты	Информационный вход	Изнутри	Извне	Нарушители
Физическое уничтожение	Встраивание бомб. Короткое замыкание					
Уничтожение информации	Стирание с дисков	Разрушающие программы			Разрушающие программы	Через модем
Подлог данных		Разрушающие программы	Ввод ложных данных			
Кража услуг		Кража от лица пользователя		Несанкционированное действие	Через модем	
Просмотр	Кража носителя			Несанкционированный доступ	Через модем	
Кража информации				Несанкционированный доступ	Через модем	

ТАКСОНОМИЯ УЯЗВИМОСТЕЙ ЛАНДВЕРА



ВОЗМОЖНЫЕ ПОКАЗАТЕЛИ УРОВНЯ БЕЗОПАСНОСТИ

1. **Нормативные.** Класс защиты по нормативным документам ФСТЭК или другим критериям
2. **Задания класса допустимых угроз.** По целям, источникам, механизмам
3. **Задания класса уровня нарушителей** (по документам ФСТЭК) исходя из возможности
4. **Введение вероятностных мер нарушения безопасности** исходя из вероятности угроз различного класса и надежности защиты
5. **Показатель оценки допустимого риска** (исходя из п.4) и принятие норм допустимости экономического (технического, административного) ущерба