



Информационная безопасность

11 класс

Основные цели и задачи информационной безопасности

- **Информационная среда** – это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.
- **Информационная угроза** – это совокупность факторов, представляющих опасность для функционирования информационной среды.
- **Информационная безопасность** – совокупность мер по защите информационной среды общества и человека.



Основные определения

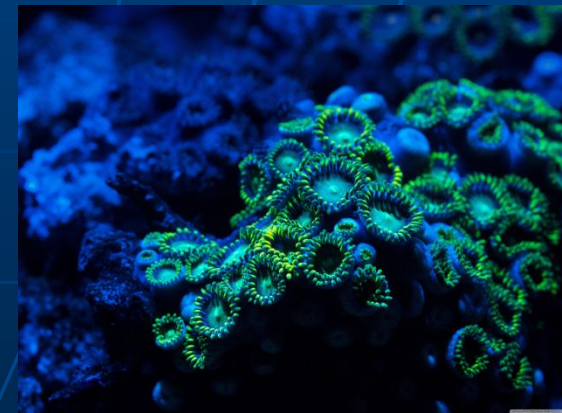
Уязвимость - это причины, обусловленные особенностями хранения, использования, передачи, охраны и ресурсов, приводящие к нарушению безопасности конкретного ресурса.

Угроза безопасности - потенциальное нарушение безопасности, любое обстоятельство, которое может явиться причиной нанесения ущерба предприятию.

Атака - реализация угрозы.

Ущерб - последствия, возникшие в результате правонарушения. Ущерб бывает материальный, физический, моральный.

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций и использующее для этого различные возможности



К объектам, которым следует обеспечить информационную безопасность, относятся:

- Информационные ресурсы;
- Система создания, распространения и использования информационных ресурсов;
- Информационная инфраструктура общества (информационные коммуникации, сети связи, центры 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



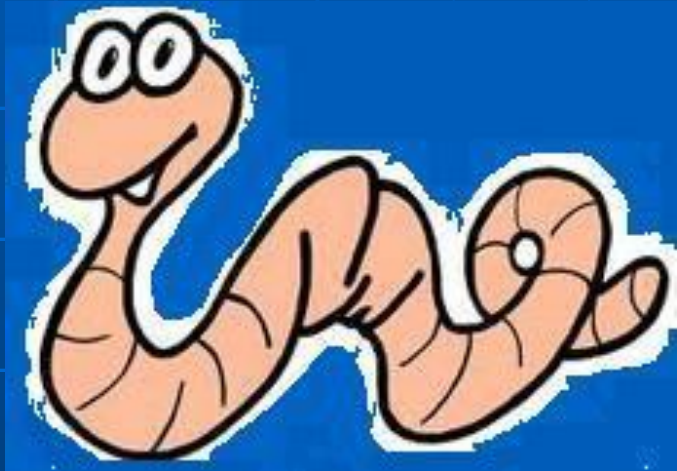
Источники основных информационных угроз для России



Преднамеренные угрозы

- Хищение информации
- Распространение компьютерных вирусов
- Физическое воздействие на аппаратуру

Компьютерные вирусы



«Троянские кони»

Сетевые атаки

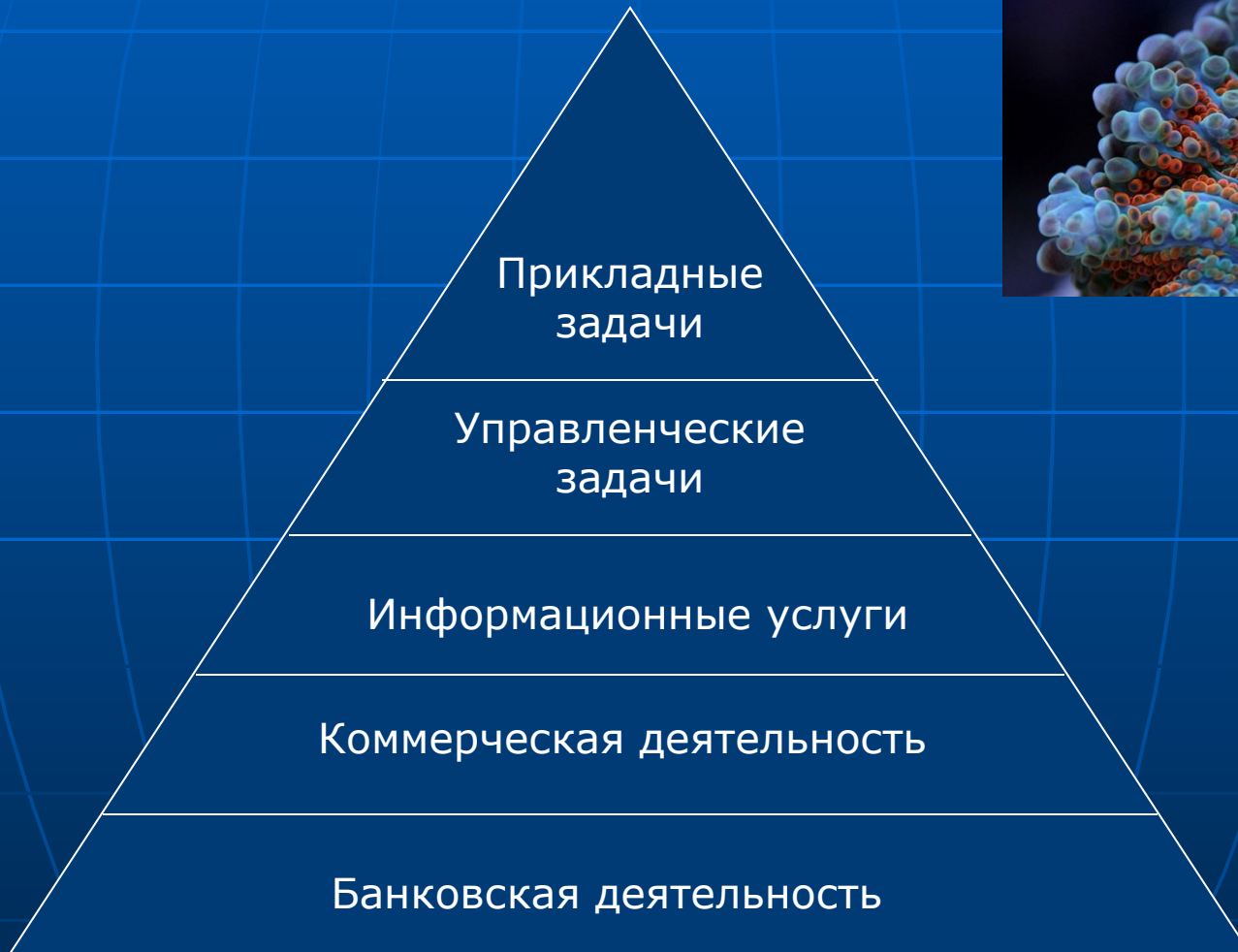


Случайные угрозы

- Ошибки пользователя компьютера;
- Ошибки профессиональных разработчиков информационных систем: алгоритмические, программные, структурные;
- Отказ и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;
- Форс-мажорные обстоятельства



Значимость безопасности информации для различных специалистов с позиции компании и заинтересованных лиц



Прикладные задачи

Сохранность личной информации пользователя

Управленческие задачи

Обеспечения полноты управленческих документов

Информационные услуги

Обеспечения доступности и безопасной работы

Коммерческая деятельность

Предотвращение утечки информации

Банковская деятельность

Обеспечения целостности информации

Политика безопасности – это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.

Методы защиты информации от преднамеренных информационных угроз

Ограничение доступа к информации

Шифрование информации

Контроль доступа к аппаратуре

Законодательные меры



Методы защиты информации от случайных информационных угроз

Повышение надёжности работы электронных и механических узлов и элементов

Структурная избыточность – дублирование или утроение элементов, устройств

Функциональный контроль с диагностикой отказов

2. Классификация угроз

1. По виду источника угроз
 - 1.1. Антропогенные источники угроз
 - 1.2. Техногенные источники
 - 1.3. Стихийные бедствия
2. По внутренним признакам топологии
3. По внешним признакам топологии
4. По признаку воздействия



2.1. Виды источников угроз

- 2.1.1. 2.1.1. Антропогенные источники
- 2.2.2. Техногенные источники
- 2.2.3. Стихийные бедствия



2.1.1. Атропогенные источники

- Криминальные структуры
- Потенциальные преступники и хакеры
- Недобросовестные партнеры
- Представители надзорных организаций и аварийных служб
- Представители силовых структур
- Основной персонал (пользователи, программисты, разработчики)
- Представители службы защиты информации (администраторы)
- Вспомогательный персонал (уборщики, охрана)
- Технический персонал (жизнеобеспечение, эксплуатация)



2.1.2. Техногенные источники

Внешние

- Средства связи (передачи информации)
- Сети инженерных коммуникаций (энергоснабжения, водоснабжения, отопления, вентиляции, канализации)

Внутренние

- Некачественные технические средства обработки информации
- Некачественные программные средства обработки информации
- Вспомогательные средства (охраны, сигнализации, телефонии)
- Другие технические средства, применяемые в учреждении

2.1.3. Стихийные бедствия

- Пожары,
- Землетрясения,
- Наводнения,
- Ураганы,
- Различные непредвидимые обстоятельства,
- Необъяснимые явления,
- Другие форс-мажорные обстоятельства



2.2. По признаку топологии

Внутренние угрозы:

- неквалифицированная внутренняя политика компании по организации
- информационных технологий и управлению безопасностью;
- отсутствие соответствующей квалификации персонала по обеспечению деятельности и управлению объектом защиты;
- преднамеренные и непреднамеренные действия персонала по нарушению безопасности;
- предательство персонала;
- техногенные аварии и разрушения, пожары.

2.2. По признаку топологии

Внешние угрозы

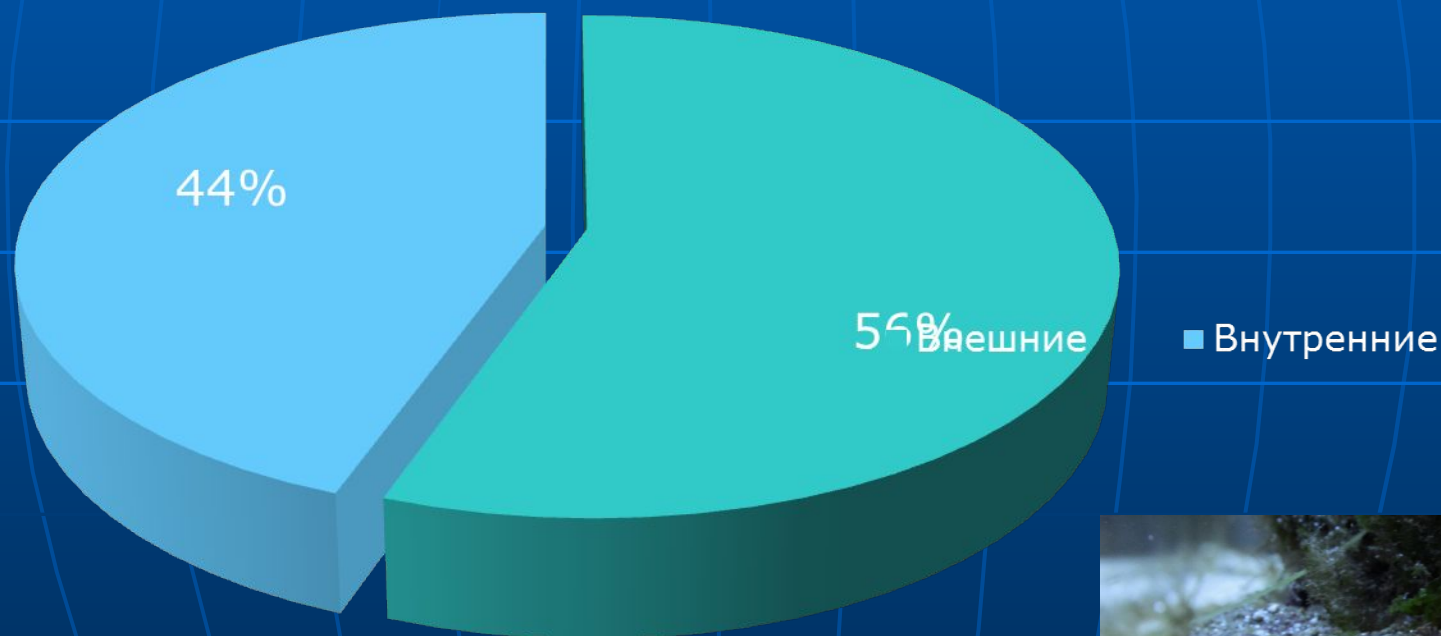
- негативные воздействия недобросовестных конкурентов и государственных структур;
- преднамеренные и непреднамеренные действия заинтересованных структур и физических лиц;
- утечка конфиденциальной информации на носителях информации и по каналам связи;
- несанкционированное проникновение на объект защиты;
- несанкционированный доступ к носителям информации и каналам связи с целью хищения, искажения, уничтожения, блокирования информации;
- стихийные бедствия и другие форсмажорные обстоятельства;
- преднамеренные и непреднамеренные действия поставщиков услуг по обеспечению безопасности и поставщиков технических и программных продуктов.

2.3. По признаку воздействия

- Угрозы конфиденциальности данных и программ
- Угрозы целостности данных, программ, аппаратуры
- Угрозы доступа к информационным ресурсам



3. Соотношение опасности по признаку топологии от общих внутренних и внешних угроз



4. Модель нарушения

Моделирование процессов нарушения информационной безопасности целесообразно осуществлять на основе рассмотрения логической цепочки: «угроза – источник угрозы – метод реализации – уязвимость – последствия»



4. Модель нарушения



- **Требования к модели нарушения**

Служба безопасности должна построить модель типичного злоумышленника. Необходимо оценить, от кого защищаться в первую очередь. Опираясь на построенную модель злоумышленника можно строить адекватную систему информационной защиты. Правильно разработанная модель нарушителя является гарантией построения адекватной защиты.

4. Модель нарушения

- **Требования к системе защиты информации**

Система защиты информации должна быть адекватной уровню важности, секретности и критичности защищаемой информации.

Ее стоимость не должна превосходить возможный ущерб от нарушения безопасности охраняемой информации.

Преодоление системы защиты должно быть экономически нецелесообразно по сравнению с возможной выгодой от получения доступа, уничтожения, модификации или блокировки защищаемой информации.