Псковский
государственный университет
Факультет
медицинского образования

Медицинская информатика: основы защиты данных

Псков,
2019/2020 учебный год
Лекция 4

Белов В.С.,
заведующий кафедрой Медицинской информатики и кибернетики

Информационная безопасность в медицинской информатике -

Лекция 4. Содержание

Информационная безопасность в медицинской информатике - 12.Разрушающие программные средства:

A1.Функциональность РПС:

- *Сокрытия признаков своего присутствия в программной среде;*
- *Реализации самодублирования, ассоциирования себя с другими программами и/или переноса своих фрагментов в иные (не занимаемые изначально указанной программой) области оперативной или внешней памяти;*
- *Разрушения (искажения произвольным образом) кода программ в оперативной памяти вычислительной системы;*
- *Перемещения (сохранения) фрагментов информации из оперативной памяти в некоторые области оперативной или внешней памяти прямого доступа;*
- *Искажения произвольным образом, блокировки и/или подмены выводимых во внешнюю память или в канал связи массивов информации, образовавшихся в результате работы прикладных программ или уже находящихся во внешней памяти, либо изменения их параметров.*

Информационная безопасность в медицинской информатике - 12.Разрушающие программные средства:

А2.Классификация РПС:

- *Закладки, отключающие защитные функции МИС;*
- *Перехватчики паролей:*
  - *Первого рода - перехват с подменного экрана,*
  - *Второго рода - перехват с клавиатуры,*
  - *Третьего рода - подмена подсистемы проверки паролей.*
- *Программные закладки, превышающие полномочия пользователя.*
- *Логические бомбы - разрушители системы защиты и МИС.*
- *Закладки-мониторы - перехватчики данных, способные:*
  - *Полностью или частично сохранять перехваченную информацию в доступном злоумышленнику месте;*
  - *Искажать потоки данных;*
  - *Помещать в потоки данных навязанную информацию;*
  - *Полностью или частично блокировать потоки данных;*
  - *Использовать мониторинг потоков данных для сбора информации об атакованной системе.*
- *Сборщики информации об атакуемой среде МИС.*

Информационная безопасность в медицинской информатике - 12.Разрушающие программные средства:

В.1.Взаимодействие РПС с МИС:

- Перехват
- Троянский конь или Логическая бомба
- Наблюдатель
- Компрометация
- Искажение или Инициатор ошибок
- Сборка мусора

Общая характеристика всех этих действий:

НАЛИЧИЕ ОПЕРАЦИИ ЗАПИСИ, ПРОИЗВОДИМОЙ РПС, В ОПЕРАТИВНУЮ ИЛИ ВНЕШНЮЮ ПАМЯТЬ

Информационная безопасность в медицинской информатике - 12.Разрушающие программные средства:

B.2.Методы внедрения РПС в МИС:

- Маскировка закладки под «безобидное» программное обеспечение,
- Маскировка закладки под «безобидный» модуль расширения программной среды,
- Подмена закладкой одного или нескольких программных модулей атакуемой среды,
- Прямое ассоциирование,
- Косвенное ассоциирование.

B.3.Деструктивные действия РПС:

- Сохранение фрагментов информации
- Изменение алгоритмов функционирования прикладных программ
- Навязывание некоторого нестандартного режима работы МИС.

Информационная безопасность в медицинской информатике - 12.Разрушающие программные средства:

В.4.Жизненный цикл реализованной угрозы несанкционированного доступа (НСД):

1) ***ЗАРОЖДЕНИЕ - в момент логического НСД,***
2) ***РАЗВИТИЕ - выявление возможностей и способов НСД к информационным ресурсам МИС,***
3) ***ПРОНИКНОВЕНИЕ в МИС - НСД к ресурсам МИС при помощи штатных средств,***
4) ***ПРОНИКНОВЕНИЕ В КРИТИЧНУЮ ИНФОРМАЦИЮ - путем обхода средств разграничения доступа***
5) ***ИНИЦИАЛИЗАЦИЯ - в момент НСД,***
6) ***РЕЗУЛЬТАТ ДЕЙСТВИЯ - в соответствии с целями НСД,***
7) ***РЕГЕНЕРАЦИЯ - при повторном НСД.***

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

А.1.1.Цели сетевых атак:

1. ***Сетевое хулиганство:***
   - *Самоутверждение,*
   - *Комплекс неполноценности,*
   - *Преднамеренный вред на профессиональном уровне,*
   - *Профессионалы-»исследователи».*
2. ***Мелкое воровство через сеть:***
   - *Воровство регистрационных и персональных данных,*
   - *Внедрение программных закладок из хулиганских побуждений.*

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

А.1.2.Цели сетевых атак:

3. ***Криминальный бизнес (группами лиц:***
   - ***Обслуживание спама,***
   - ***Организация отказа в обслуживании Web-сайтами ЛПУ (интернет-рэкет за прекращение атак),***
   - ***Внедрение закладок в МИС через сеть «зомби-машин»,***
   - ***Воровство экономико-финансовых данных из ЛПУ,***
   - ***Воровство конфиденциальных данных из МИС,***
   - ***Кибер-шантаж (интернет-рэкет за восстановление изъятой при НСД информации).***
4. ***Полулегальный бизнес:***
   - ***Принудительная реклама,***
   - ***Навязывание платных Web-ресурсов,***
   - ***Распространение ложных анти-шпионских или антивирусных утилит.***

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

В.1.Классификация сетевых атак:

1. *Характер воздействия на МИС:*
   1.1. Пассивные, 1.2.Активные.
2. *Цель воздействия на МИС - нарушение:*
   2.1. Конфиденциальности, 2.2. Целостности,
   2.3. Работоспособности.
3. *Условие начала осуществления воздействия:*
   3.1. По запросу от атакуемого объекта,
   3.2. При наступлении события на атакуемом объекте,
   3.3. Безусловная атака.
4. *Наличие ОС с атакуемым объектом:*
   4.1. С ОС, 4.2. Однонаправленная атака (без ОС).
5. *Расположение атакуемого объекта:*
   5.1. Внутрисегментное, 5.2. Межсегментное
6. *Уровень модели OSI:*
   6.1. F(1)-физический, 6.2. K(2)-канальный, 6.3. N(3)-сетевой,
   6.4. T(4)-транспортный, 6.5. S(5)-сеансовый,
   6.6. P(6)-представления, 6.7. A(7)-прикладной

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

В.2.Характеризация типовых сетевых атак:

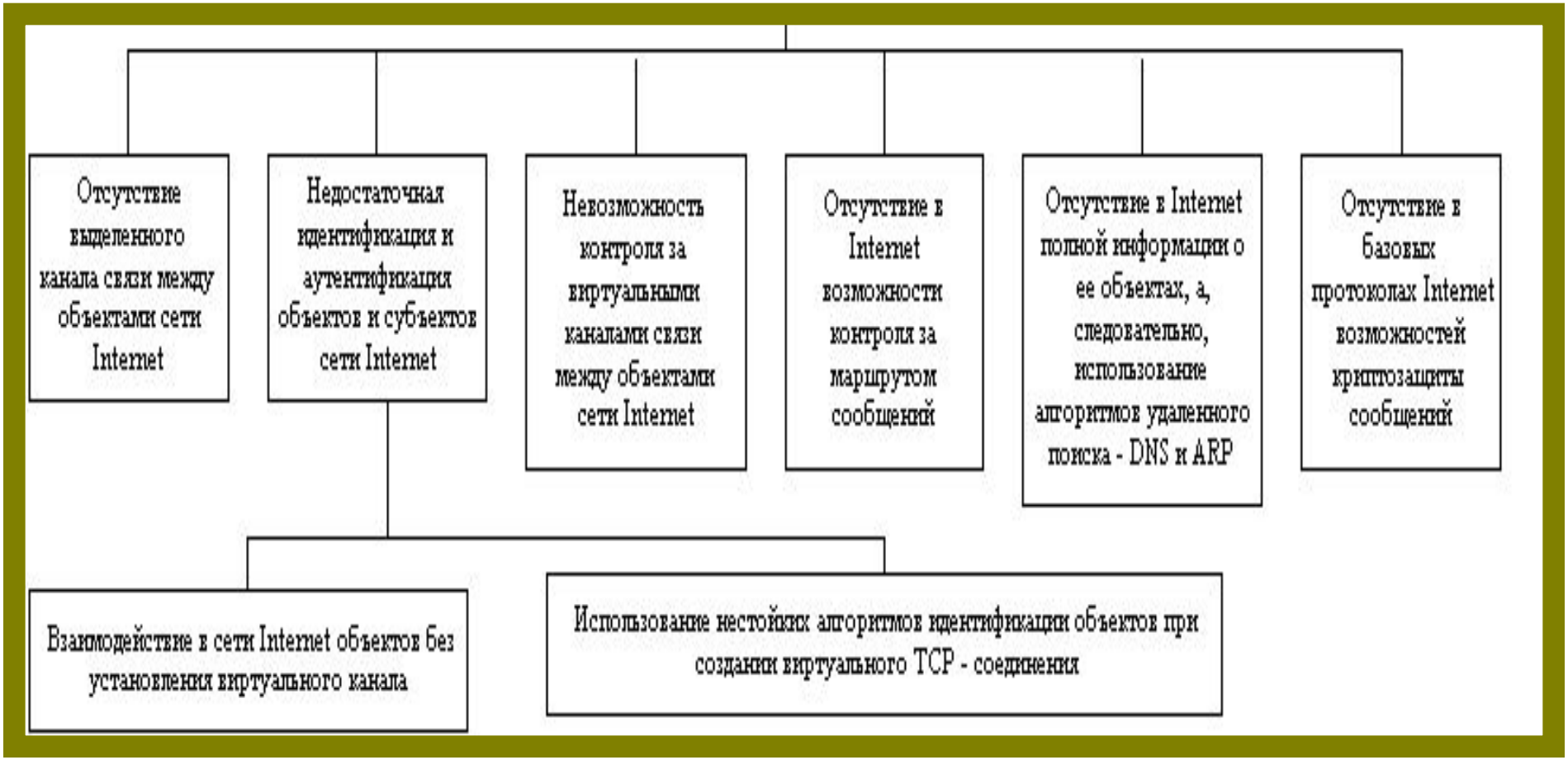
1. ***Атака «Анализ сетевого трафика»:***
   - ***Пассивная, нарушение Конфиденциальности, Безусловная, Однонаправленная, Внутрисегментная, на Канальном уровне***
2. ***Атака «Внедрение ложного хоста»:***
   - ***Активная, Нарушение Конфиденциальности/Целостности, При наступлении события на атакуемом хосте, с ОС и без ОС, Внутри- и Меж- сегментная, уровни 3 и 4;***
3. ***Атака «Навязывание ложного маршрута»:***
   - ***Активная, нарушение Конфиденциальности/Целостности/ Работоспособности, Безусловная, с ОС и без ОС, Внутри- и Меж- сегментная, на Сетевом уровне;***
4. ***Атака «Подмена объектов сети при поиске хостов»***
   - ***Активная, Нарушение Конфиденциальности/Целостности, по Запросу и при Наступлении события на атакуемом объекте, с ОС, Внутри- и Меж- сегментная, уровни 2,3,4;***
5. ***Атака «Отказ в обслуживании»:***
   - ***Активная, Нарушение Работоспособности, Безусловная, Однонаправленная, Внутри- и Меж- сегментная, уровни 2-7.***

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

В.3.Причины успеха сетевых атак на распределенные вычислительные системы:

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

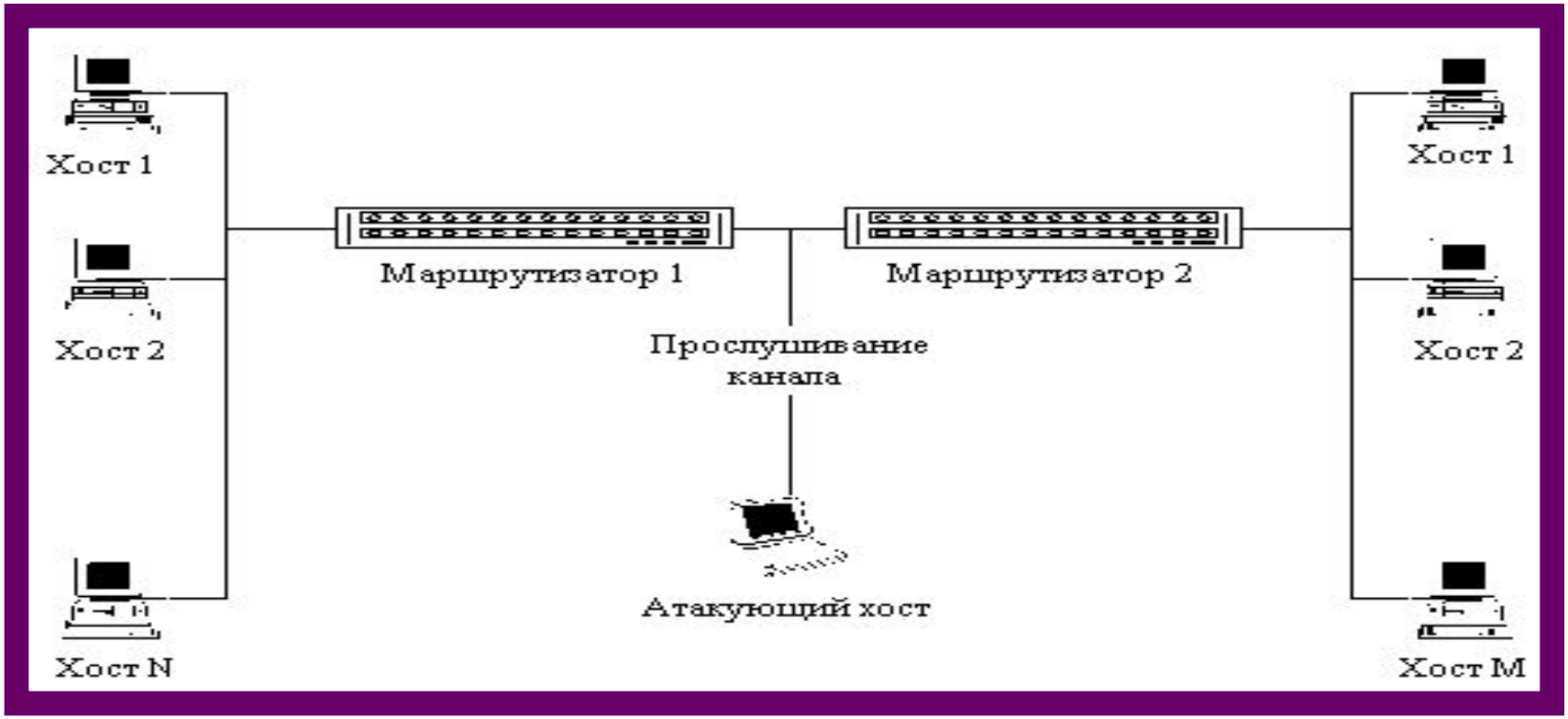
В.4.Причины успеха удаленных сетевых атак:



Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

С.1.Примеры реализации:

- ***Получение паролей и идентификаторов с помощью СРЕДСТВ АНАЛИЗА СЕТЕВОГО ТРАФИКА:***



Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

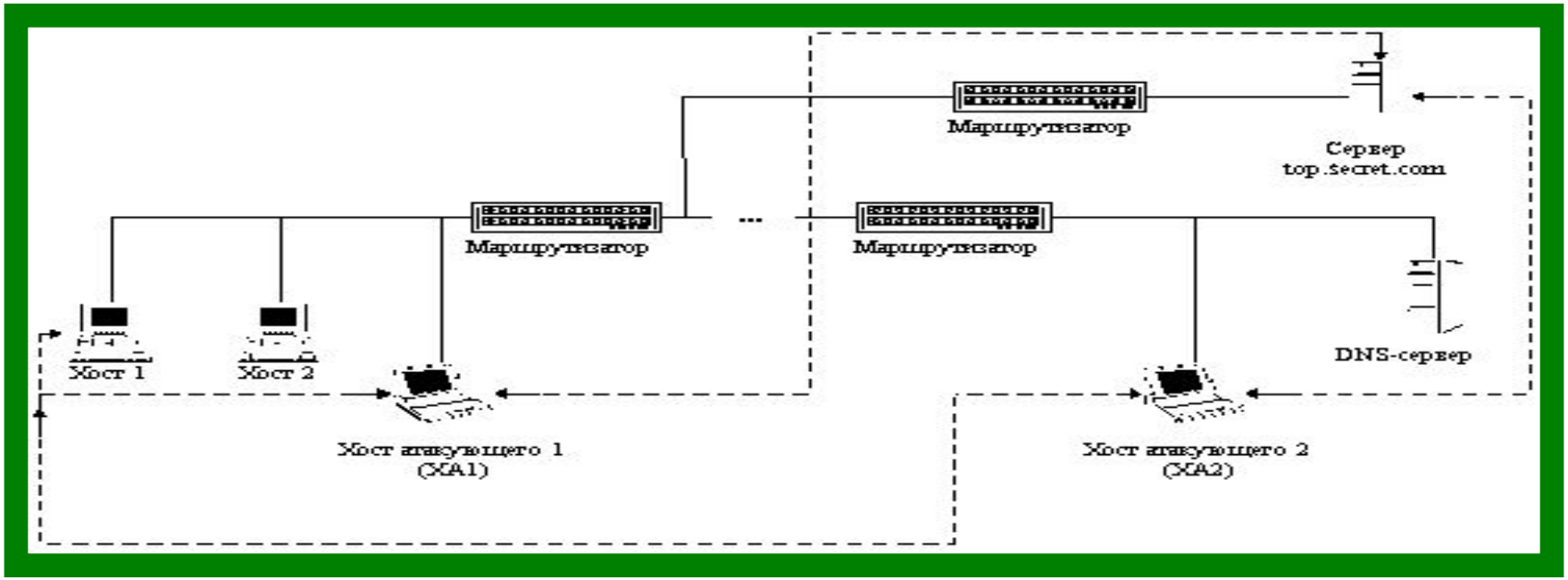
С.2.Примеры реализации:

- ***Внедрение ложного хоста сети с помощью ЛОЖНОГО ARP-СЕРВЕРА (ARP-Adress Resolution Protocol)***
  - ***Фаза 1. Прослушивание канала (ожидание ARP-запроса)***
  - ***Фаза 2. Перехват и подмена ARP-запроса***
  - ***Фаза 3. Связь хоста 1 проходит через ложный ARP-сервер***

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

С.3.Примеры реализации:

- ***Внедрение ложного хоста сети с помощью ЛОЖНОГО DNS-СЕРВЕРА (DNS-Domain Name System)***
  - ***Фаза 1. Прослушивание канала (ожидание DNS-запроса)***
  - ***Фаза 2. Перехват и подмена DNS-запроса***
  - ***Фаза 3. Связь хоста 1 проходит через ложный DNS-сервер***

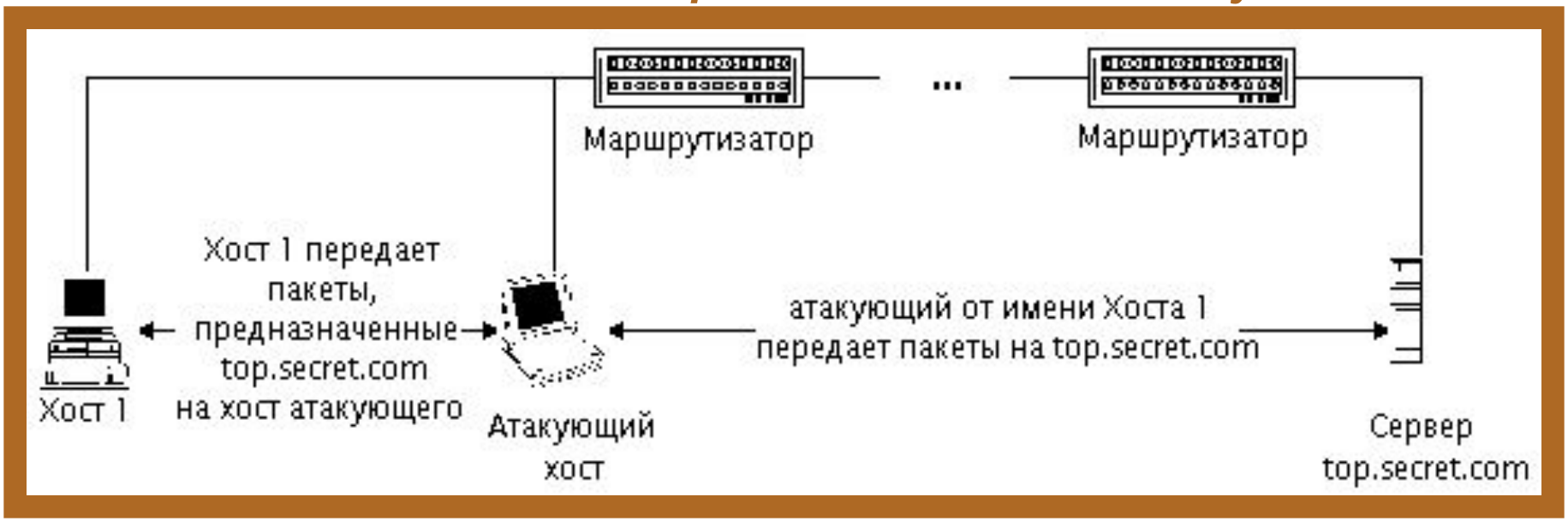


Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

С.4.Примеры реализации:

- ***Навязывание хосту ложного маршрута с помощью ЛОЖНОГО МАРШРУТИЗАТОРА (недочеты протокола ICMP - Internet Control Message Protocol)***

  Фаза 1. Отправка на хост 1 ложного ICMP Redirect Host сообщениеz с данными о ложном маршруте
  Фаза 2. Связь хоста 1 проходит с ложным получателем



Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

С.5.Примеры реализации:

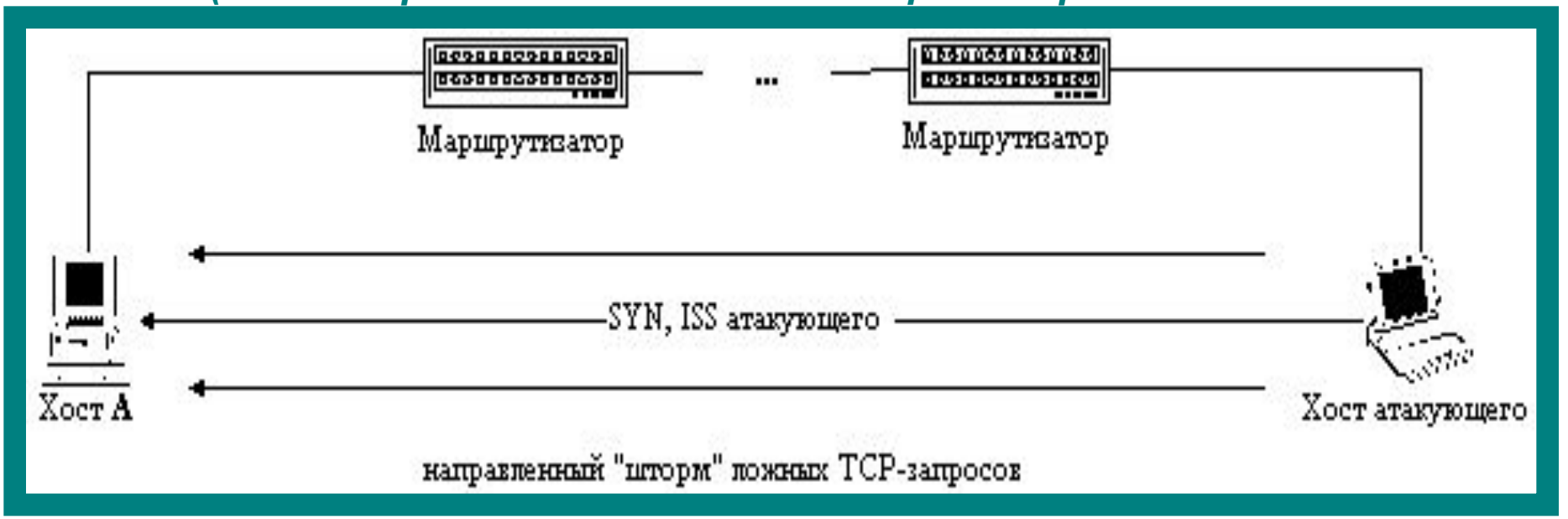
- ***Навязывание хосту ложного маршрута с целью ОТКАЗА В ОБСЛУЖИВАНИИ – НЕДОСТАВКИ СООБЩЕНИЯ АДРЕСАТУ (недочеты протокола ICMP)***

  Фаза 1. Отправка на хост 1 ложного ICMP Redirect Host сообщениez с данными о ложном маршруте
  Фаза 2. Пакету с хоста 1 идут на несуществующий адресат

Информационная безопасность в медицинской информатике - 13.Сетевые атаки на МИС:

С.6.Примеры реализации:

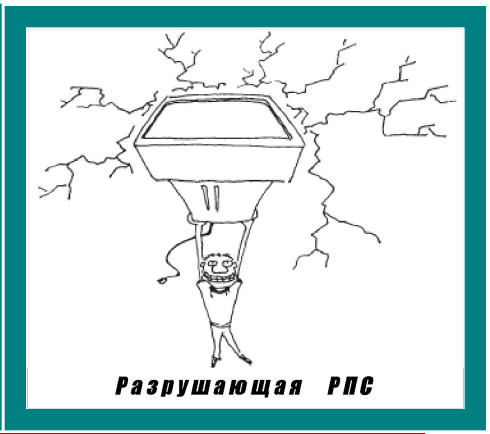
- ***Нарушение работоспособности хоста в сети Internet при использовании направленного "шторма" ложных TCP-запросов на создание соединения, либо при переполнении очереди запросов(TCP – Transfer Control Protocol)***
  - ***SYN (Synchronize Sequence Number) – служебный бит синхронизации***
  - ***ISS (Initial Sequence Number - идентификатор-счетчик пакетов***

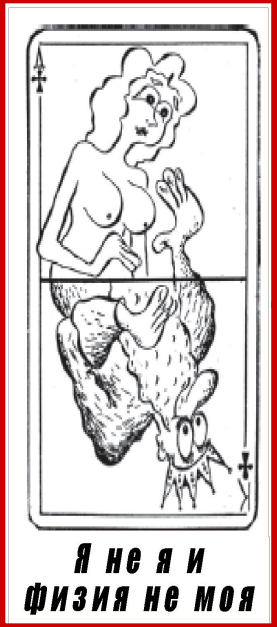


Информационная безопасность в медицинской информатике

Лк.4: ВЫВОДЫ

1. РПС направлены на:
✔ Отключение СИБ,
✔ Превышение полномочий,
✔ Разрушение МИС,
✔ Перехват данных,
✔ Сбор информации о СИБ





2. Методы внедрения РПС:
✔ Маскировка,
✔ Подмена (маскарад),
✔ Ассоциирование

Информационная безопасность в медицинской информатике

3. Виды сетевых атак:
- ✔ Пассивные и активные,
- ✔ Анализ трафика,
- ✔ Подмена трафика,
- ✔ Подмена объектов сети,
- ✔ Отказ в обслуживании,
- ✔ Подмена маршрута.

Информационная безопасность в медицинской информатике

Лекция 4 закончена.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!