Псковский
государственный университет
Факультет
медицинского образования

Медицинская информатика: основы защиты данных

Псков,
2019/2020 учебный год
Лекция 2

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

Информационная безопасность в медицинской информатике -

Лекция 2. Содержание

6. *Проблемы и направления защиты – сл.1*
7. *Угроза, атака, проникновение, ущерб – сл.2,3*
8. *Источники и цели возникновения угроз– сл.4,5*
9. *Пути реализации угроз безопасности МИС–сл.6-9*
0. *Критичные угрозы безопасности для МИС – сл.10-18*

Информационная безопасность в медицинской информатике -

6.Проблемы и направления защиты:

A.Проблемы обеспечения защиты данных:

- *Утечки закрытой информации;*
- *Утрата конфиденциальной и служебной информации;*
- *Несанкционированная модификация закрытых и служебных данных.*

B.Направления обеспечения защиты данных:

- *Обеспечение целостности данных;*
- *Защита данных от утери, т.е. обеспечение сохранности данных;*
- *Обеспечение доступности данных зарегистрированным (легальным) пользователям по первому требованию;*
- *Поддержка конфиденциальности данных;*
- *Защита от утечек и перехвата закрытых сведений на всех стадиях технологического процесса сбора, обработки, хранения и передачи информации внутри сети ЛПУ и на внешние МИС.*

Информационная безопасность в медицинской информатике - 7.Угроза, атака, проникновение, ущерб:

А.1.УГРОЗА – это:

- *Нарушение или опасность нарушения физической целостности информации;*
- *Искажение или опасность искажения логической структуры информации;*
- *Несанкционированная модификация или опасность такой модификации информации;*
- *Несанкционированное получение или опасность такого получения информации;*
- *Несанкционированное размножение или опасность такого размножения информации.*

А.2.УЯЗВИМОСТЬ МИС - это:

- *Недостатки системы информационной безопасности, вызванные отсутствием механизмов защиты, ошибками или слабостями в механизмах защиты при реализации средств защиты информационной системы либо при внутреннем контроле системы, которые могут быть использованы для нарушения работоспособности системы при появлении одной или нескольких угроз.*

Информационная безопасность в медицинской информатике -

7.Угроза, атака, проникновение, ущерб:

А.3.АТАКА (НАПАДЕНИЕ, ИНЦИДЕНТ) - это:

- *Действие, предпринятое злоумышленником или иным субъектом с целью поиска и использования той или иной уязвимости защищенной информационной системы.*
- *Т.о., атака – это реализованная угроза безопасности. Несанкционированное размножение или опасность такого размножения информации.*

А.4.ПРОНИКНОВЕНИЕ - это:

- *Успешное преодоление средств защиты информационной системы в процессе осуществления акта нападения на нее.*

В.Что такое УЩЕРБ (ПОТЕРИ) от нарушения безопасности МИС:

- *объем информационных, технических, финансовых и иных реальных и потенциальных потерь, понесенных владельцем конфиденциальной (секретной) информации в результате получения несанкционированного доступа злоумышленника (субъекта) к этой информации.*

Информационная безопасность в медицинской информатике -

8.Источники и цели возникновения угроз:

А.1.Источники УГРОЗ:

- *Нарушители или злоумышленники (нелегальные субъекты);*
- *Технические устройства;*
- *Программные элементы (в т.ч. алгоритмы и модели, определяющие их функционирование);*
- *Программные закладки, компьютерные вирусы;*
- *Технологические схемы обработки информации;*
- *Каналы информационного взаимодействия и обмена данными;*
- *Элементы внешнего окружения (в т.ч. и внешняя среда).*

Информационная безопасность в медицинской информатике -

8.Источники и цели возникновения угроз:

А.2.Цели воздействия УГРОЗ:

- *Нарушение целостности информации;*
- *Нарушение сохранности информации;*
- *Нарушение работоспособности МИС или отказы в предоставлении ее служб;*
- *Нарушение конфиденциальности информации;*
- *Невыполнение всех трех основных задач Защиты информации в МИС;*
- *Получение несанкционированного доступа к закрытым данным;*
- *Манипулирование техническими средствами МИС;*
- *Манипулирование закрытыми данными МИС.*

Информационная безопасность в медицинской информатике -

9.Пути реализации угроз безопасности МИС:

А.1.Через аппаратуру:

- *При нарушении целостности данных МИС:*
  - *подключение к хранилищам закрытых данных,*
  - *модификация закрытых данных,*
  - *изменение режимов работы МИС,*
  - *несанкционированное использование ресурсов хранилищ МИС.*
- *При нарушении работоспособности МИС:*
  - *изменение режимов работы МИС,*
  - *разрушение компонентов МИС,*
  - *вывод из строя МИС.*
- *При нарушении конфиденциальности МИС:*
  - *хищение носителей закрытой информации,*
  - *подключение к закрытым данным,*
  - *использование информационных ресурсов.*

Информационная безопасность в медицинской информатике -

9.Пути реализации угроз безопасности МИС:

А.2.Через ПО, Иформ-ные технологии, данные:

- ***При нарушении целостности данных МИС:***
  - ***искажение, модификация закрытых данных,***
  - ***внедрение компьютерных вирусов и РПС,***
  - ***внедрение программных закладок.***
- ***При нарушении работоспособности МИС:***
  - ***искажение, удаление ключевых параметров МИС,***
  - ***подмена, модификация конфигурационных параметров системы безопасности МИС.***
- ***При нарушении конфиденциальности МИС:***
  - ***хищение, копирование закрытой информации,***
  - ***подмена, модификация закрытой информации,***
  - ***удаление закрытых данных,***
  - ***перехват закрытых сообщений.***

Информационная безопасность в медицинской информатике -

9.Пути реализации угроз безопасности МИС:

А.3.Через каналы связи и протоколы взаимодействия:

- ***При нарушении целостности данных МИС:***
  - ***подключение к хранилищам закрытых данных,***
  - ***модификация закрытых данных,***
  - ***изменение режимов работы МИС.***
- ***При нарушении работоспособности МИС:***
  - ***нарушение нормального хода работы МИС,***
  - ***искажение, удаление ключевых параметров МИС,***
  - ***подмена, модификация конфигурационных параметров системы безопасности МИС.***
- ***При нарушении конфиденциальности МИС:***
  - ***хищение, копирование закрытой информации,***
  - ***подмена, модификация закрытой информации,***
  - ***Перехват закрытых сообщений.***

Информационная безопасность в медицинской информатике -

9.Пути реализации угроз безопасности МИС:

А.4.Через персонал:

- ***При нарушении целостности данных МИС:***
  - ***вербовка,***
  - ***подкуп,***
  - ***маскарад.***
- ***При нарушении работоспособности МИС:***
  - ***отвлечение (удаление, уход) с рабочего места,***
  - ***физическое устранение.***
- ***При нарушении конфиденциальности МИС:***
  - ***халатность (при работе с закрытыми данными в присутствии третьих лиц, с незащищенного рабочего места и т.п.),***
  - ***разглашение (из-за безответственности),***
  - ***агентурная передача сведений.***

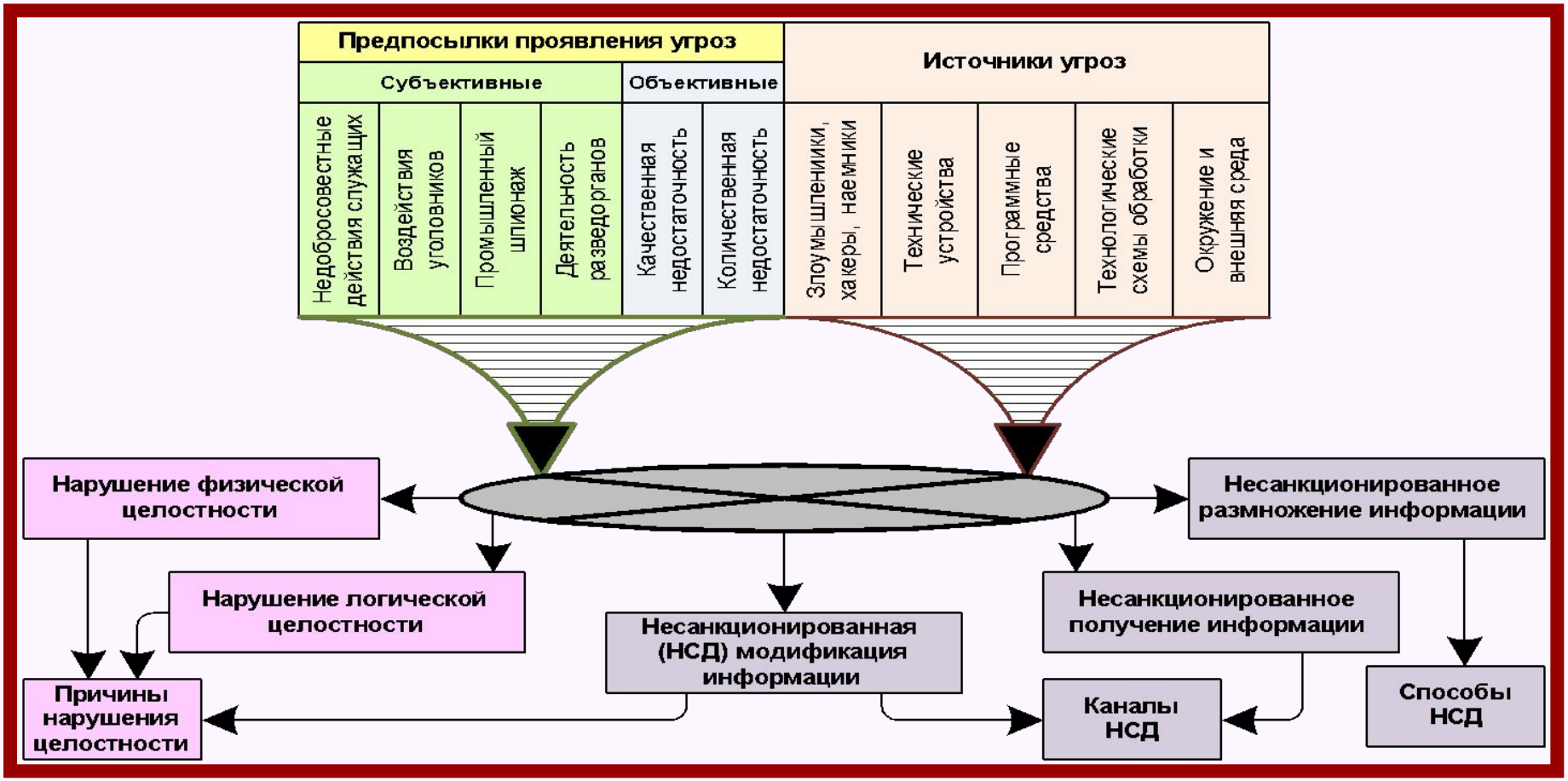
Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

В.5.Поведение МИС при реализации УГРОЗЫ:

- *Помехи или нарушения нормального хода работы;*
- *Подмена или маскировка («маскарад») данных, действий, результатов выполнения процедур;*
- *Модификация информации;*
- *Повторение (навязывание) процедур обмена или обработки данных;*
- *Атака типа «троянский конь», «логическая бомба»;*
- *Нарушение нормального хода работы из-за срабатывания ловушки.*

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

С.1.Взаимодействие предпосылок и источников угроз:



Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

D.1.Тяжкие угрозы (обзор):

- *Проникновения в МИС, в т.ч. через каналы связи;*
- *Захват или несанкционированное получение паролей;*
- *Изменение служебной базы данных системы защиты;*
- *Получение несанкционированных привилегий;*
- *Угрожающее использование ресурсов МИС;*
- *Проникновение в МИС компьютерных вирусов;*
- *Нарушение целостности информации;*
- *Нарушение конфиденциальности информации;*
- *Хищение служебной и конфиденциальной информации;*
- *Искажение семантического и синтаксического содержания закрытых и ключевых данных;*
- *Внедрение дезинформации;*
- *Отключение механизмов защиты информации;*
- *Ухудшение эффективности функционирования МИС;*
- *Нарушение работы МИС,*
- *Приведшее МИС к отказу в пользователей в обслуживании;*
- *Блокирование использования информации.*

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

D.2.1.Проявления реализованных угроз:

- *Нарушение целостности информации в МИС:*
  - *Подключение скрытого ретранслятора,*
  - *Введение ложной информации в протоколы обмена данными,*
  - *Расширение полномочий пользователей по управлению информацией,*
  - *Изменение полномочий других пользователей (без санкции на это действие),*
  - *Маскировка под другого пользователя в целях НСД,*
  - *Модификация ПО путем внедрения программных закладок,*
  - *Подрыв доверия к протоколу обмена данными путем инициализации нарушений,*
  - *Сокрытие факта наличия ложной информации.*

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

D.2.2.Проявления реализованных угроз:

- *Нарушение конфиденциальности информации в МИС:*
  - *Получение сведений о владельцах закрытой информации и ее характере,*
  - *Нарушение секретности или конфиденциальности закрытой информации,*
  - *Заявление о сомнительности обеспечения в МИС конфиденциальности информации через раскрытие закрытых данных,*
  - *Копирование и распространение закрытой информации.*

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

D.2.3.Проявления реализованных угроз:

- *Нарушение работоспособности МИС:*
  - *Затруднения процессов обмена данными между рабочими станциями и сервером МИС,*
  - *Ложный отказ МИС от факта предоставления закрытой информации,*
  - *Ложное утверждение о получении/отправки информации от определенного пользователя как внутри МИС, так и при взаимодействии с удаленными пользователями ч/з публичную сеть,*
  - *Ложный отказ от факта получения информации при взаимодействии с удаленными пользователями ч/з публичную сеть,*
  - *Сбои в работе системы обеспечения безопасности МИС.*

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

Е.1.Каналы утечки информации:

- ***Агентурные каналы:***
  - ***Легальные пользователи МИС – ч/з разглашение (преднамеренное, непреднамеренное), халатность (нарушение политики безопасности), подкуп;***
  - ***Внедренные в коллектив ЛПУ злоумышленники.***
- ***Информационные каналы:***
  - ***Пассивные – электромагнитные, акустические (виброакустические), визуальные каналы, каналы восприятия электрических наводок (внешние для МИС токопроводящие объекты и цепи, в т.ч. цепи электропитания, заземления, телефонизации и пр.);***
  - ***Активные – внутрисистемные каналы связи, телекоммуникационные (проводного, беспроводного, модемного сетевого соединения), встроенные в систему шпионские источники информационных сигналов (аппаратные, программные закладки).***

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

F.1.Критичные угрозы безопасности МИС:

Уровень	Угроза	Источник	Ущерб
Физический	Отказ, Выход из строя, Уничтожение хранилищ, серверов, раб.станций, носителей информации	Техногенные аварии, Нарушения правил эксплуатации	Уничтожение информации, Потеря доступности данных
Сетевой и сетевых приложений	Блокировка доступа к общесетевому ресурсу, Несанкционированный доступ к сетевому ресурсу	Ошибочные настройки сетевых сервисов	Утечка закрытых данных, Потеря доступности данных,
Операционных систем	Уничтожение прикладного ПО, Нарушение правильной работы МИС, Уничтожение закрытых данных	Заражение вирусом, Нарушение правил обмемена данными	Потеря целостности данных, Потеря доступности данных, Утечка закрытых данных

Информационная безопасность в медицинской информатике - 10.Угрозы безопасности МИС:

F.2.Критичные угрозы безопасности МИС:

Уровень	Угроза	Источник	Ущерб
Управления базами данных	Нарушение работоспособности СУБД, Изменение системных настроек СУБД	Нарушение политик безопасности, Утечки административных данных	Уничтожение информации, Потеря целостности данных, Потеря доступности данных, Утечка закрытых данных
Технологического процесса обработки данных	Ввод фиктивной информации, Несанкционированный вывод и разглашение закрытой информации	Нарушение политик безопасности, Утечки административных данных	Подмена закрытой информации, Потеря целостности данных, Потеря доступности данных, Утечка закрытых данных

Информационная безопасность в медицинской информатике

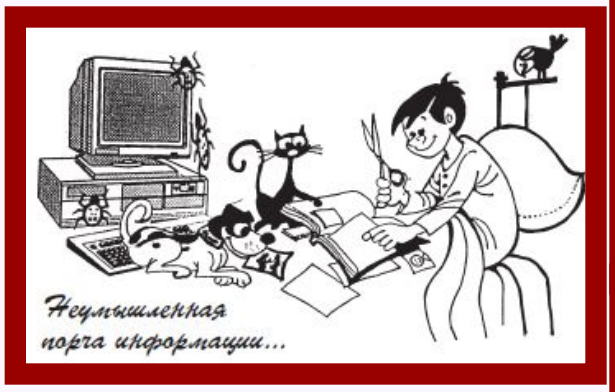
Лк.2: ВЫВОДЫ

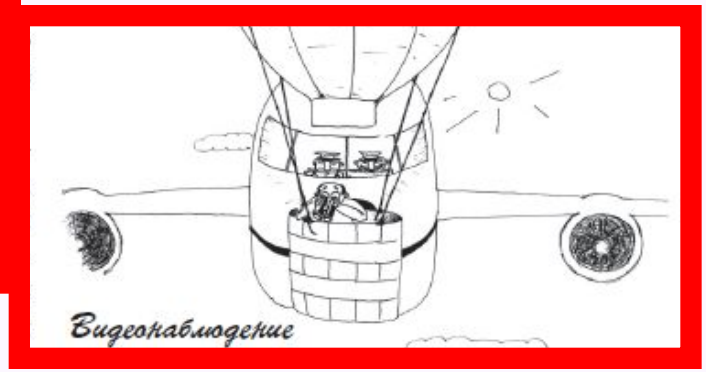
1. Основные проблемы защиты МИС – угрозы, утечки, утрата данных, несанкционированный доступ к данным
2. Угрозы безопасности очень разнообразны и направлены на нарушение:

✔ Целостности данных,
✔ Конфиденциальности данных,
✔ Работоспособности МИС.

Информационная безопасность в медицинской информатике

3. Утечка данных происходит через:
- ✔ Агентурные каналы:
  - ☐ Неумышленные,
  - ☐ Преднамеренные,
  - ☐ Халатность администратора;
- ✔ Информационные пассивные каналы:
  - ☐ Побочные излучения;
- ✔ Информационные активные каналы:
  - ☐ Сетевой,
  - ☐ Программные закладки и вирусы.





Информационная безопасность в медицинской информатике

Лекция 2 закончена.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!