Псковский
государственный университет
Факультет
медицинского образования

# Медицинская информатика: основы защиты данных

Псков,
2019/2020 учебный год
Лекция 3

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

# Информационная безопасность в медицинской информатике -

## Лекция 3. Содержание

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## А.Внутренние нарушители:

***Группа 1.*** ***Пользователи МИС:***

- *управленческий персонал ЛПУ,*
- *врачебный персонал,*
- *средний медицинский персонал.*

***Группа 2.*** ***Инженерно-технический персонал:***

- *системные и сетевые администраторы,*
- *администраторы СУБД и прикладного ПО,*
- *администраторы безопасности,*
- *операторы, программисты и инженеры сопровождения.*

***Группа 3.*** ***Посетители ЛПУ:***

- *пациенты,*
- *лица, сопровождающие пациентов.*

***Группа 4.*** ***Вспомогательный персонал ЛПУ:***

- *охранники,*
- *обслуживающий персонал,*
- *персонал хозяйственных служб.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## A1.Ограничения внутр.нарушителей групп 1,3 и 4:

1) *Нарушитель не может реализовывать угрозы, зная, что подобные попытки будут обнаружены сотрудниками, эксплуатирующими МИС, а также администраторами безопасности МИС;*
2) *Возможность установки и использования нарушителем технических средств съема и передачи информации, в т.ч. замаскированных под штатные технические средства (путем подмены), исключается режимными мерами ограничения доступа лиц на территорию ЛПУ и в помещения, где расположено оборудование МИС;*
3) *Нарушитель не будет использовать особенности ПО (включая прикладное ПО), способные нарушить защищенность МИС, которые не описаны в документации на ПО и не известны сотрудникам, эксплуатирующим и сопровождающим МИС.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## A2.Ограничения внутр.нарушителей группы 2:

1) *… см. 1) для нарушителей групп 1,3,4,*
2) *… см. 2) для нарушителей групп 1,3,4,*
3) *… см. 3) для нарушителей групп 1,3,4,*
4) *Работа по подбору кадров ЛПУ и специальные мероприятия исключают возможность создания коалиций нарушителей из числа сотрудников указанной категории, т.е. объединения и целенаправленных действий по преодолению системы защиты с участием двух и более сотрудников.*
5) *Потенциальные внутренние нарушители второй категории осуществляют доступ к информационным и вычислительным ресурсам МИС посредством системного, базового и прикладного ПО, установленного на технических средствах МИС.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## А3.Знания внутренних нарушителей:

1) *Нарушитель обладает высоким уровнем знаний в области программирования, проектирования и эксплуатации МИС, технико-программного обеспечения в целом;*
2) *Нарушитель знает структуру, функции и механизм действия средств защиты, их место в МИС;*
3) *Нарушитель правильно представляет функциональные особенности работы МИС, основные закономерности формирования в ней информационных массивов и потоков запросов к ним;*
4) *Нарушитель может использовать непреднамеренные действия других пользователей МИС (эти действия могут быть как случайными, так и обусловленными необходимостью выполнения пользователями своих служебных обязанностей).штатных программно-технических средств МИС.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## А4.Возможности внутренних нарушителей:

1) *Использование штатных программно-технических средств, входящих в состав МИС (при получении к ним доступа);*
2) *Использование штатных носителей информации (флэш-накопитель информации, переносной жесткий диск и т.п.) и технических средств (например, ноутбук) , которые разрешается легально проносить через посты охраны ЛПУ;*
3) *Использование компактных носителей информации и технических средств (например, сотовый телефон, беспроводные средства передачи информации и т.п.), непосредственно не относящиеся к сетевыс средствам и средствам ВТ.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## В1.Внешние нарушители:

1) *Разработчики и поставщики ПО для МИС:*
   - *сотрудники фирм-разработчиков,*
   - *сотрудники фирм-поставщиков ПО.*
2) *Разработчики и поставщики оборудования для МИС:*
   - *сотрудники фирм-разработчиков оборудования,*
   - *сотрудники фирм-поставщиков технических средств.*
3) *Злоумышленники, хакеры:*
   - *бывшие технические работники ЛПУ,*
   - *«любители-исследователи»,*
   - *«крутые профессионалы»,*
   - *лица, преследующие корыстные цели..*
4) *Нелегальные специалисты ИТ:*
   - *нарушитель высшего класса.*
   - *нарушитель-классный специалист,*
   - *продвинутый нарушитель, знающий основы работы компьютера и сети,*
   - *нарушитель-дилетант.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## В2.Ограничения внешних нарушителей :

1) *Доступ посторонних лиц к информационным и вычислительным ресурсам МИС с территории ЛПУ и из помещений, где расположены технические средства МИС, исключается мерами по охране территории и организации пропускного режима ЛПУ;*
2) *Внешний нарушитель не может реализовывать угрозы, зная, что подобные попытки будут обнаружены сотрудниками, эксплуатирующими МИС ЛПУ, а также администраторами безопасности МИС;*
3) *Возможность установки и использования нарушителем технических средств съема и передачи информации, в т.ч. замаскированных под штатные технические средства (путем подмены), исключается режимными мерами ограничения доступа лиц на территорию ЛПУ и в помещения, где расположено оборудование МИС.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## В3.Знания внешних нарушителей:

1) *Нарушитель обладает высоким уровнем знаний в области программирования, проектирования и эксплуатации МИС, технико-программного обеспечения в целом;*
2) *Нарушитель знает структуру, функции и механизм действия средств защиты, их место в МИС;*
3) *Нарушитель правильно представляет функциональные особенности работы МИС, основные закономерности формирования в ней информационных массивов и потоков запросов к ним;*
4) *Нарушитель может использовать непреднамеренные действия других пользователей МИС (эти действия могут быть как случайными, так и обусловленными необходимостью выполнения пользователями своих служебных обязанностей).штатных программно-технических средств МИС.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## В4.1.Возможности внешних нарушителей:

1) ***Атаки на систему защиты МИС:***
   - ***на политику безопасности и процедуры администрирования средств обеспечения безопасности;***
   - ***на постоянные компоненты системы защиты МИС (алгоритмы криптозащиты, механизмы подтверждения подлинности, средства защиты целостности и проч.);***
   - ***на сменные компоненты системы защиты МИС (профили и пароли легальных субъектов, служебные БД, ключи шифрования, параметры конфигурирования МИС и системы защиты и т.п.);***
   - ***на протоколы взаимодействия и обмена данными (внутрисистемные, внешние открытые и закрытые и пр.);***
   - ***на функциональные элементы МИС (вычислительные ресурсы, средства управления вычислительными процессами, носители информации и проч.).***

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

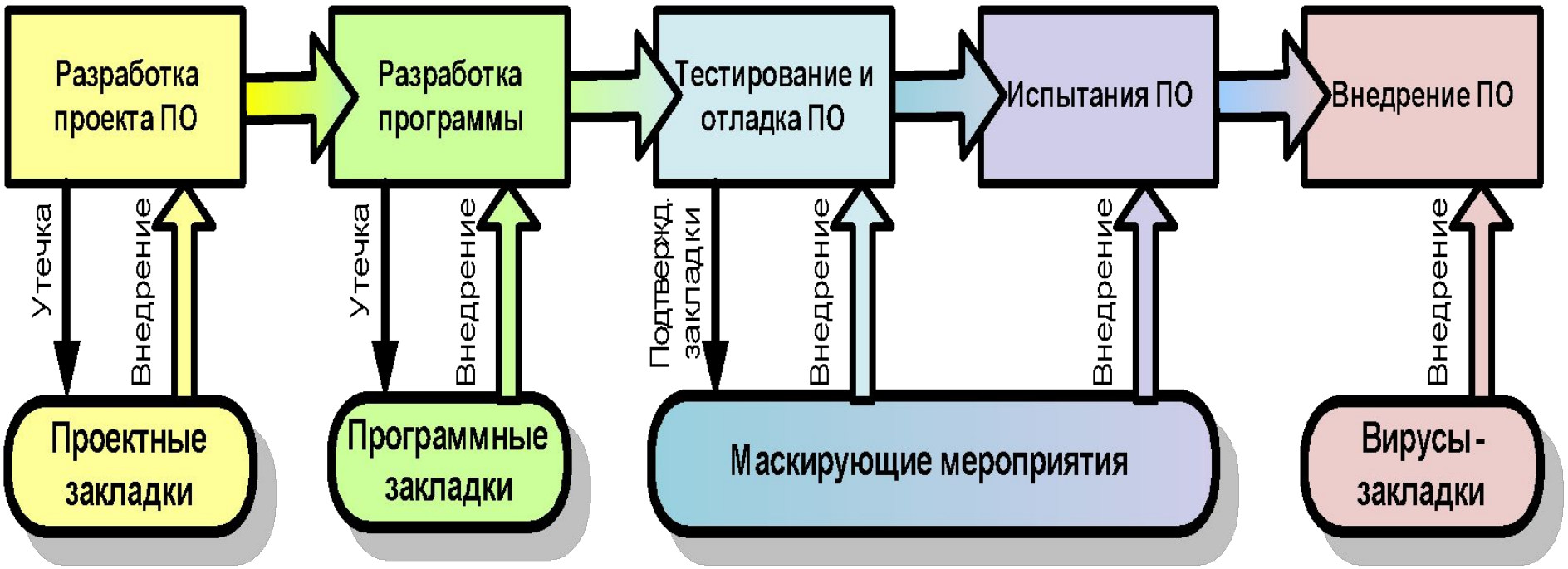
## В4.2.Возможности внешних нарушителей:

2) ***Атаки на объекты тракта обработки данных:***

- ***на носители информации и информационные объекты, на них находящиеся (информационные хранилища, базы и банки данных, информационные файлы);***
- ***на каналы связи и взаимодействия (внутрисистемные, открытые и закрытые внешние), а также информацию, по ним циркулирующую;***
- ***на средства управления информационными, операционными, вычислительными, программными, техническими, коммуникационными ресурсами МИС;***
- ***на область обработки информации – процессоры, сверхоперативную, оперативную и буферную память, операционную среду, средства управления вычислительными процессами, системные и прикладные средства обработки данных и пр.***

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## B5.1.Угрозы разработчиков и поставщиков ПО - Жизненный цикл ПО и этапы внедрения угроз:



# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## B5.2.Угрозы разработчиков и поставщиков ПО:

1. ***Программные проектные решения:***
   - ***Выбор нерациональных алгоритмов работы,***
   - ***Облегчение внесения закладок и затруднение их обнаружения.***
2. ***Использование готовых информационных технологий:***
   - ***Внедрение информационных технологий или их элементов, содержащих программные закладки,***
   - ***Внедрение неоптимальных информационных технологий.***
4. ***Архитектура программной системы:***
   - ***Внедрение «чужих» подпрограмм и системных данных,***
   - ***Нерациональная организация вычислительного процесса,***
   - ***Неправильная организация динамически формируемых команд,***
   - ***Неправильная организация переадресации команд,***
   - ***запись злоумышленной информации в используемые программной системой или другими программами ячейки памяти.***

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## B5.3.Угрозы разработчиков и поставщиков ПО:

4. ***Компоненты программной системы:***
   - *Формирование программной закладки, воздействующей на другие части программной системы,*
   - *Встраивание программной закладки, как в подпрограммы и в управляющую структуру программной системы,*
   - *Организация замаскированного спускового механизма программной закладки,*
   - *Формирование программной закладки, изменяющей структуру программной системы.*
5. ***Формирование дистрибутива программной системы:***
   - *Формирование дистрибутива ПО со встроенными дефектами или внедренными программными закладками.*
6. ***Тестирование и отладка программной системы:***
   - *Формирование и внедрение маскирующего набора тестовых данных, не позволяющих выявить программную закладку,*
   - *Формирование программной закладки, не обнаруживаемой в силу ее неадекватности объекту тестирования.*

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## B5.4.Угрозы разработчиков и поставщиков ПО:

7. ***Испытания ПО:***
   - ***Формирование спускового механизма программной закладки, не включающего ее при испытаниях на безопасность,***
   - ***Маскировка программной закладки путем внесения в ПО ложных «непреднамеренных» дефектов,***
   - ***Формирование программных закладок в ветвях программной системы, не проверяемых при испытаниях,***
   - ***Формирование программных закладок, не позволяющих выявить их в ПО путем контрольного суммирования,***
   - ***Поставка программного обеспечения и вычислительной техники для организации контроля или испытаний, содержащих программные, аппаратные и программно-аппаратные закладки.***
8. ***Анализ результатов тестирования и испытаний ПО:***
   - ***Искажение сведений об обнаруженных дефектах и программных закладках в процессе испытаний,***
   - ***Маскировка выявленных программных закладок,***
   - ***Внедрение новых программных закладов вместо выявленных при доработке ПАО по итогам испытаний.***

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## B5.5.Угрозы разработчиков и поставщиков ПО:

9. ***Внедрение и опытная эксплуатация ПО:***
   - ***Формирование спускового механизма программной закладки, не включающего ее при испытаниях на безопасность,***
   - ***Сбор сведений о дефектах и закладках, обнаруженных при внедрении и опытной эксплуатации.***
   - ***Искажение сведений о дефектах и закладках, обнаруженных при внедрении и опытной эксплуатации.***
   - ***Сбор сведений о рекламациях и подмена их ложными с целью сокрытия истинных сведений об обнаружении закладок,***
   - ***Разработка новых программных закладок и их внедрения при доработке программной системы,***
   - ***Внедрение закладок и компьютерных вирусов любыми способами.***

# Информационная безопасность в медицинской информатике - 11.Нарушители безопасности МИС:

## B5.6.Угрозы разработчиков и поставщиков оборудования для МИС:

1. ***Оборудование для тестирования и отладки ПО:***
   - ***Поставка вычислительных средств для организации контрольно-испытательных процедур, содержащих программные, аппаратные или программно-аппаратные закладки, в т.ч. рапдиозакладки.***
2. ***Аппаратные компоненты и сетевое оборудование:***
   - ***Поставка технических средств и сетевого оборудования для МИС со встроенными дефектами и сбойными драйверами,***
   - ***Поставка технических средств и сетевого оборудования для МИС с внедренными программными закладками,***

# Информационная безопасность в медицинской информатике

## Лк.3: ВЫВОДЫ

1. Модель нарушителя включает:
✔ Категории лиц,
✔ Ограничения,
✔ Уровень подготовки (знания),
✔ И его возможности.

Модель нарушителя безопасности


Установить личность нарушителя ...необходимо подумать

2. Выделяются две категории нарушителей безопасности
✔ Внутренние нарушители:
- ❑ Пользователи МИС,
- ❑ Мед.персонал,
- ❑ Пациенты,
- ❑ Вспомогат. персонал

✔ Внешние нарушители:
- ❑ Хакеры,злоумышленники
- ❑ Разрабочики ПО,
- ❑ Разработчики тех.средств

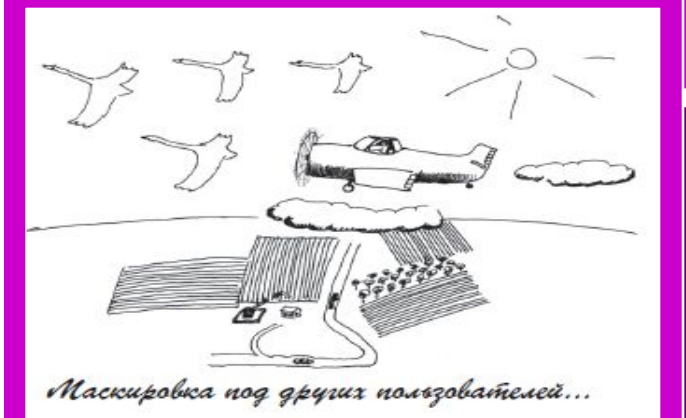

А это типичный внутренний нарушитель безопасности


Любимые действия внешних нарушителей

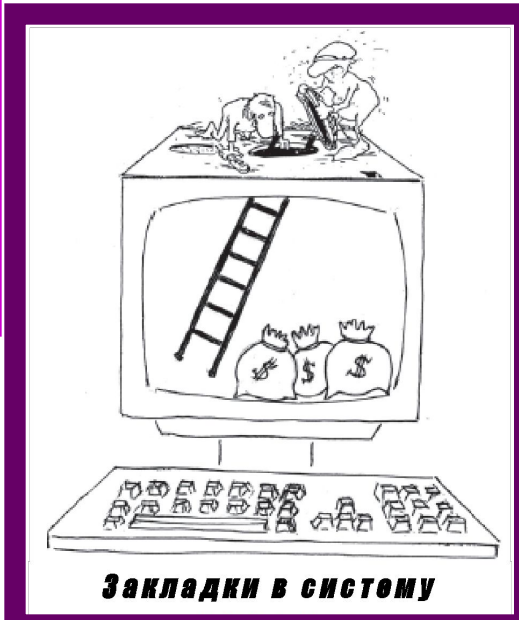
# Информационная безопасность в медицинской информатике

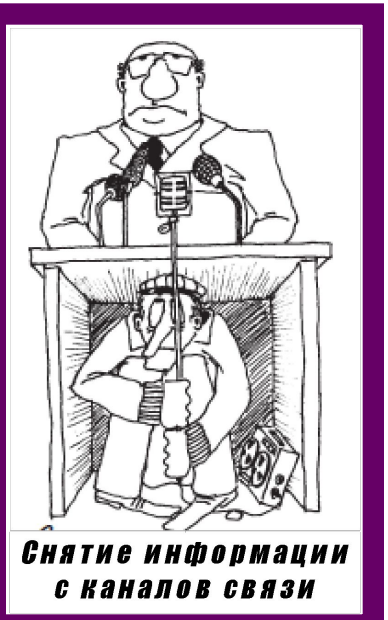
3. Наиболее опасными угрозами внутренних нарушителей являются:
   - ✔ Разглашение
   - ✔ Копирование данных на сменные носители
   - ✔ Маскировка под другого пользователя






4. Наиболее опасными угрозами внешних нарушителей являются:
   - ✔ Внедрение закладок,
   - ✔ Перехват информации в каналах связи



# Информационная безопасность в медицинской информатике

## Лекция 3 закончена.

## БЛАГОДАРЮ ЗА ВНИМАНИЕ!