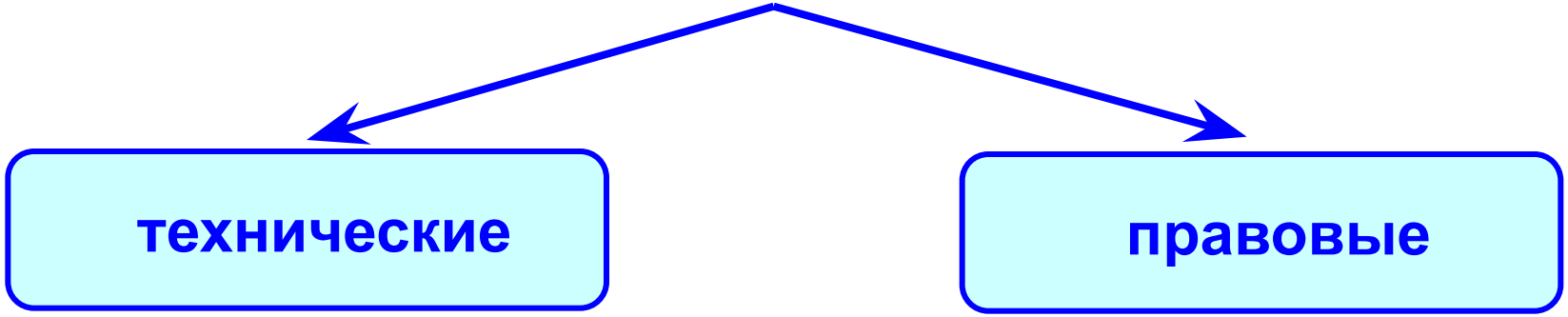
# Правовые основы информационной безопасности

**Вопросы:**

**1. Понятие и правовое обеспечение безопасности ЭИС.**

Доп. литература: Мельников В.В. Безопасность информации в автоматизированных ИС – М:, Финансы и статистика, 2003.- 368 с.

# Меры по обеспечению информационной безопасности




**Аппаратные и программные средства и технологии защиты от вредоносных программ, внешних сетевых атак и пр. (в том числе антивирусные программы)**

**Совокупность нормативных и правовых актов, регулирующих вопросы защиты информации**

# Нормативно-правовые документы по ИБ:

1.Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011) "Об информации, информационных технологиях и о защите информации" (редакция с изменениями не вступившими в силу)

2."Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 03.05.2012) (с изм. и доп., вступающими в силу с 25.05.2012) Статья 13.12. Нарушение правил защиты информации

3."Таможенный кодекс Таможенного союза« (ред. от 16.04.2010) Статья 45. Защита информации и прав субъектов, участвующих в информационных процессах и информатизации

4. Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 08.12.2011) "О Федеральной службе безопасности" Статья 11.2. Обеспечение информационной безопасности

# Нормативно-правовые документы по ИБ:

5. Федеральный закон от 08.12.2003 N 164-ФЗ (ред. от 06.12.2011) "Об основах государственного регулирования внешнеторговой деятельности"
Статья 17. Защита информации

6. Федеральный закон от 07.02.2011 N 7-ФЗ (ред. от 03.12.2011) "О клиринге и клиринговой деятельности" (с изм. и доп., вступающими в силу с 01.01.2012)
Статья 20. Защита информации

7. Федеральный закон от 21.11.2011 N 325-ФЗ "Об организованных торгах"
Статья 23. Защита информации

8. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». (принят и введен в действие Распоряжением Банка России от 21.06.2010 N Р-705)

# *Правовые основы информационной безопасности*

***Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»*** **(принят 27 июля 2006 г.)**

**Статья 1** гласит, что данный закон «регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации».

**Статья 3** формулирует понятия **«безопасность»** и **«защита информации»** в рамках принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
В качестве одного из основных принципов постулируется «обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации».

# *Правовые основы информационной безопасности*

***Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»*** **(принят 27 июля 2006 г.)**

**Статья 10** «Распространение информации или предоставление информации» затрагивает проблему спам-рассылок.

**Статья 16** рассматривает основные понятия и положения, касающиеся защиты информации.

**Статья 17** определяет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

# *Правовые основы информационной безопасности*

***Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»* (принят 27 июля 2006 г.)**

Любые деяния, приводящие к повреждению или уничтожению информации, к ее намеренному искажению, а также стремление получить неправомерный доступ к чужой конфиденциальной информации (то, чем занимаются авторы вирусов, троянов и других вредоносных программ) являются

***преступлением***

# *Правовые основы информационной безопасности*

***Федеральный закон № 152-ФЗ «О персональных данных»*** **(принят 27 июля 2006 г.)**

определяет основные понятия и положения о защите

***персональной***,

т. е. личной информации каждого человека.

**Статья 3** гласит, **что персональные данные** – это «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных),

в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

# *Правовые основы информационной безопасности*

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**
определяет меры наказания за преступления, связанные с компьютерной информацией.

**Глава 28**

**Статья 272.** Неправомерный доступ к компьютерной информации.

**Статья 273.** Создание, использование и распространение вредоносных программ для ЭВМ.

**Статья 274.** Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

## Правовые основы информационной безопасности

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**

**Глава 28. Статья 272**

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается **штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет**.

## Правовые основы информационной безопасности

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**

**Глава 28. Статья 272**

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, — наказывается **штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.**

# 1. Понятие и правовое обеспечение безопасности ЭИС

Безопасность (security) – состояние защищенности субъекта или объекта от воздействия негативных факторов, которые могут причинить ему вред.

Информационная безопасность (ИБ) - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

(Извлечение из документа: Постановление Правления ПФ РФ от 26.01.2001 N 15 "О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи" (вместе с "Регламентом регистрации и подключения юридических и физических лиц к системе электронного документооборота Пенсионного фонда Российской Федерации")

## Правовые основы информационной безопасности

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**

**Глава 28. Статья 273**

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами — наказываются **лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев**.

## Правовые основы информационной безопасности

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**

**Глава 28. Статья 273**

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются **лишением свободы на срок от трех до семи лет**.

## Правовые основы информационной безопасности

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**

**Глава 28. Статья 273**

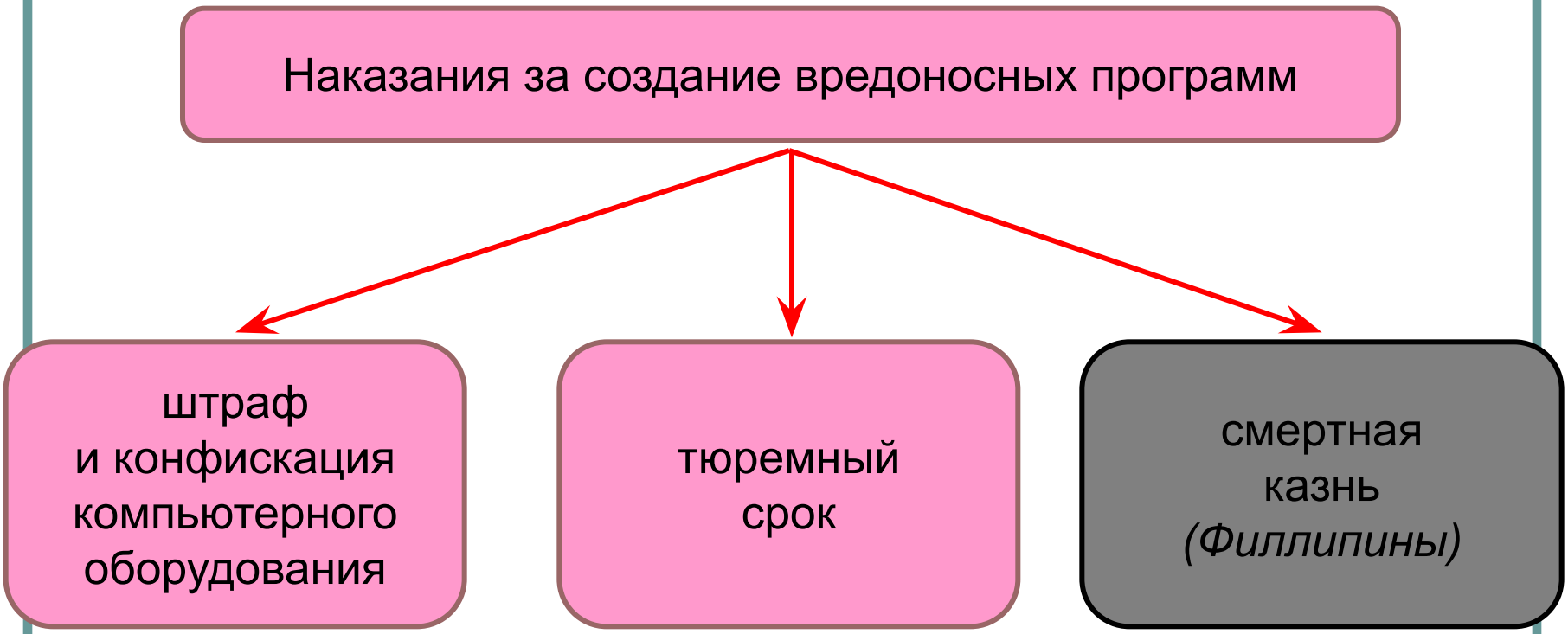
1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами — наказываются **лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев**.

## Правовые основы информационной безопасности

***Уголовный кодекс Российской Федерации (УК РФ) №63-ФЗ***
**(принят 13 июня 1996 г.)**

**Глава 28. Статья 274**

2. То же деяние, повлекшее по неосторожности тяжкие последствия, — наказывается **лишением свободы на срок до четырех лет**.


Наказания за создание вредоносных программ
штраф
и конфискация
компьютерного
оборудования
тюремный
срок
смертная
казнь
(Филлипины)

# Статья 13.12. Нарушение правил защиты информации из Кодекса РФ об административных нарушениях :

1.Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), -влечет наложение административного штрафа на граждан в размере от 300-500 рублей; на должностных лиц - от 500 до 1000 рублей; на юридических лиц - от 5000до 10000 рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации - влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от 1000 до 2000 рублей; на юридических лиц - от 10000 до 20000 рублей с конфискацией несертифицированных средств защиты информации или без таковой.

# Статья 13.12. Нарушение правил защиты информации из Кодекса РФ об административных нарушениях :

3. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от 2000 до 3000 рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от 10000 до 20000 рублей с конфискацией средств защиты информации или без таковой.

# Статья 13.14. Разглашение информации с ограниченным доступом (из Кодекса РФ об административных нарушениях) :

1. Разглашение информации, доступ к которой ограничен ФЗ (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей; на должностных лиц - от 4000 до 5000 рублей.

# Критерии оценки безопасности ИС:

Критерии безопасности компьютерных систем Министерства обороны США (Оранжевая книга) определяют требования к аппаратному, программному и специальному обеспечению и выработки политики безопасности в компьютерных системах военного назначения. В ней приводятся следующие уровни безопасности систем:

- Высший класс- А;
- Промежуточный класс –В;
- Низкий уровень – С;
- Класс систем, не прошедших испытания –Д.

# Критерии оценки безопасности ИС:

- Международная рабочая группа ISO/IES JTC разработала стандарт общих критериев оценки безопасности ИТ ИСО. МЭК 15408-99. Представляет универсальную библиотеку требований безопасности ИС.
- В России установлено 7 классов защищенности СВТ от НСД к информации. Самый низкий класс- седьмой, самый высокий- первый.

  При этом защитные мероприятия охватывают подсистемы:

  -Управления доступом;

  -Регистрации и учета;

  -Криптографическая;

  -Обеспечение целостности;

  -Законодательные меры;

  -Физические меры.

# Требования к критериям оценки безопасности ИС:

Требование 1. *Политика безопасности.* Система должна поддерживать точно определенную политику безопасности.

Требование 2. *Метки.* С объектами должны ассоциироваться метки безопасности, используемые в качестве атрибутов контроля доступа.

Требование 3. *Идентификация и аутентификация*. Все субъекты должны иметь уникальные идентификаторы.

Требование 4. *Регистрация и учет.* Все события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.

Требование 5. *Контроль корректности функционирования средств защиты.*

Требование 6. *Непрерывность защиты.*