



Семинар  
«Организация защиты  
информационных систем в  
образовательном учреждении»  
14 февраля 2013 г.

**Павлов Александр Владиславович,**  
заместитель директора по информационной  
безопасности



## ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

### ПОСТАНОВЛЕНИЕ

от 1 ноября 2012 г. №1119

МОСКВА

#### Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

В соответствии со статьей 19 Федерального закона «О персональных данных» Правительство Российской Федерации **п о с т а н о в л я е т**:

1. Утвердить прилагаемые требования к защите персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

Председатель Правительства  
Российской Федерации

Д.Медведев

УТВЕРЖДЕНЫ  
постановлением Правительства  
Российской Федерации  
от 1 ноября 2012 г. № 1119

### ТРЕБОВАНИЯ

#### к защите персональных данных при их обработке в информационных системах персональных данных

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровню защищенности таких данных.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным

# Обязанности оператора ПДн

- Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".
- Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

- Безопасность персональных данных при их обработке в информационной системе **обеспечивает оператор** этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

# Основные этапы работ по обеспечению безопасности персональных данных в испдн



# Основные этапы работ

- Определение ответственных за обеспечение безопасности ПДн
- Подготовка (обучение) должностных лиц
- Анализ ИС, формирование перечня ПДн
- Классификация ИСПДн
- Построение частной модели угроз и модели нарушителя
- Разработка системы защиты ПДн
- Разработка документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн
- Развертывание, настройка и ввод в эксплуатацию СЗПДн
- Уведомление уполномоченного органа по защите прав субъектов ПДн
- Организация контроля за соблюдением условий использования СЗПДн
- Аттестация (декларация соответствия)

# 1. Определение ответственных

- Создание (назначение) структурного подразделения и/или должностного лица (работника), ответственного за обеспечение безопасности ПДн в ИСПДн.

## **Документ – Приказ(ы) о назначении ответственных**

- Выделение необходимых финансовых, людских и материальных средств (с учетом возможного привлечения специализированных организаций к работам)
  - *17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом). ППРФ от 1.11.2012 г. №1119*

- Принятие решения на защиту ПДн и планирование всех видов обеспечения работ
  - Мероприятия по видам обеспечения проводятся в соответствии с решением руководителя организации на организацию защиты ПДн и утвержденной концепцией.
  - Обеспечение организации защиты – это комплекс мероприятий, связанных с назначением и подготовкой кадров, выделением финансовых средств, закупкой технических средств защиты, оценок и т.п.

**Документ – раздел в Плане работ по защите...**



- **Виды обеспечения работ по защите ПДн:**
  - **Финансовое.** Осуществляется по результатам проведенного обоснования необходимых затрат на организацию защиты
    - Зарплата сотрудников
    - Подготовка кадров
    - Привлечение сторонних организаций
    - Закупка технических средств защиты
  - **Кадровое**
    - Повышение квалификации
    - Привлечение специалистов
  - **Программно-аппаратное**
    - Закупка и испытание средств защиты
  - **Информационное**
    - Информирование всех заинтересованных лиц
    - Доведение требований и нормативных документов
    - Обеспечение справочной и иной информацией в ходе работ
  - **Материальное**
    - Шкафы, кондиционеры, мебель, канцтовары...

## 2. Обучение должностных лиц

- Подготовка (обучение) должностных лиц, ответственных за обеспечение безопасности ПДн с целью:
  - Компетентного планирования, руководства и исполнения работ по защите ПДн
  - Получение лицензий ФСТЭК и ФСБ
- Ответственные лица должны быть обязательно обучены:
  - В сертифицированном учебном центре
  - Обучение, предусмотренное в договоре поставки средств защиты информации
  - Обученным специалистом (Приказ об обучении и ведомость сдачи зачета)
- Система повышение осведомленности

## 3. Анализ исходных данных

- Инвентаризация и анализ информационных ресурсов на предмет наличия в ИС ПДн и процессов их обработки
- Описание технологии обработки ПДн, форм представления (формы фиксации) ПДн
- Формирование перечня ПДн и выявление сегментов ИСПДн
- Сбор и анализ исходных данных по особенностям построения ИСПДн...

### **Документы:**

- Перечень персональных данных
- Описание технологического процесса (технологии) обработки информации в ИСПДн
- Список лиц, допущенных к обработке ПДн
- ...

## 4. Классификация

- Постановление Правительства РФ от 1.11.2012 г. №1119
  - Определение вида информационной системы
  - Определение типа угроз безопасности ПДн
  - Присвоение ИСПДн соответствующего уровня защищенности
    - С 4 по 1 уровень

**Документ – Акт классификации ИСПДн**

## 5. Построение модели угроз

- *2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей **актуальные угрозы**, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".  
(ППРФ от 1.11.2012 г. №1119)*
- Мероприятия по построению модели угроз и модели нарушителя в ИСПДн
  - Определение исходной защищенности ИСПДн
  - Анализ уязвимостей и возможных угроз безопасности ПДн
  - Определение модели нарушителя
  - Оценка ущерба от реализации угроз
  - Определение актуальности угроз

**Документ – Частная модель угроз**

## 6. Разработка системы защиты

- Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. (ППРФ от 1.11.2012 г. №1119)
- Этапы разработки (проектирования) СЗПДн:
  - Определение требований к СЗПДн исходя из уровня защищенности ИСПДн
  - Определение основных функций, структуры, состава СЗПДн и перечня предполагаемых к использованию сертифицированных средств защиты
  - Планирование организационных мероприятий по защите ПДн в ИСПДн (по администрированию, по разрешительной системе и др.)

### **Документы:**

- Техническое задание на СЗПДн
- Описание СЗПДн

## 7. Разработка документации

- Разработка организационно-распорядительной документации, регламентирующей вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн
  - Должностных инструкций персоналу ИСПДн в части обеспечения безопасности ПДн
  - Разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации
  - По организации учета лиц, допущенных к работе с ПДн
  - Инструкций по использованию программных и аппаратных средств защиты
  - По организации учета средств защиты и носителей персональных данных
  - По организации охраны и физической защите ресурсов ИСПДн
  - ...

**Документы – Пакет орг.расп. документов**

## 8. Развертывание СЗПДн

- Организация и проведение работ по развертыванию СЗПДн (ее элементов в ИСПДн) включает:
  - Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией
  - Обучение лиц, использующих средства защиты информации, правилам работы с ними
  - Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных
  - Учет лиц, допущенных к работе с персональными данными в ИС
  - ...

### **Документы:**

- **Приказы, Акты, Свидетельства и Удостоверения об обучении**



## 9. Испытания СЗПДн

- Проведение приемо-сдаточных испытаний СЗПДн по результатам опытной эксплуатации
- Анализ защищенности системного и прикладного программного обеспечения
- Доработка СЗПДн и дополнительная настройка СЗИ по результатам опытной эксплуатации
- Сертификация СЗПДн

**Документы – Приказы, Акты, Заключение**

# 10. Уведомление

- Ст. 22 ФЗ «О персональных данных» от 27.07.2006 г. №152-ФЗ
  - 1. Оператор **до начала обработки** персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

# 11. Организация контроля

- 17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом)

*ППРФ от 1.11.2012 г. №1119*



А есть ли у нас ИСПДн?

# ИСПДн

- Автоматизированная обработка – обработка персональных данных с помощью средств вычислительной техники
- ИСПДн – информационная система персональных данных:
  - **Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств**

# Основные элементы ИСПДн

- Персональные данные, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в ИСПДн
- Информационные технологии, как совокупность приемов, способов и методов применения СВТ при обработке ПДн
- Технические средства, осуществляющие обработку ПДн (СВТ, сети, средства передачи, приема и обработки ПДн)
- Программные средства (ОС, СУБД и т.п.)
- Средства защиты информации
- Вспомогательные технические средства и системы (средства и системы, их коммуникации не предназначенные для обработки ПДн, но размещенные в помещениях ИСПДн)

- **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)
- **Персональные данные работника** – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника

# ПДн подлежащие защите

- Сведения о работниках и кандидатах на вакансии (отдел кадров)
- Сведения о работниках (бухгалтерия)
- Сведения о посетителях (вахта)
- Сведения о телефонных абонентах (телефонный справочник)
- Сведения о контактных лицах организаций (клиентская база)
- Сведения о контактах переписки (электронная почта)
- Сведения о внешних участниках деловых встреч (визитные карточки)
- Сведения о работниках и внешних лицах в технологических документах – планах, графиках и т.п. (расписание занятий, списки обучающихся)
- Сведения о лицах в договорной документации



# АИС в ОУ

- **Автоматизированные информационные системы в образовательном учреждении:**
  - Системы кадрового учета персонала
  - Системы бухгалтерского учета
  - «Электронный журнал»
  - Базы данных контактов юридических лиц-контрагентов
  - Контактные списки почтовой системы

- **Автоматизированная информационная система включает в себя:**

- Обслуживающий персонал
- Конечные пользователи
- Технические средства:
  - Аппаратное обеспечение
  - Программное обеспечение
  - Данные (информация)

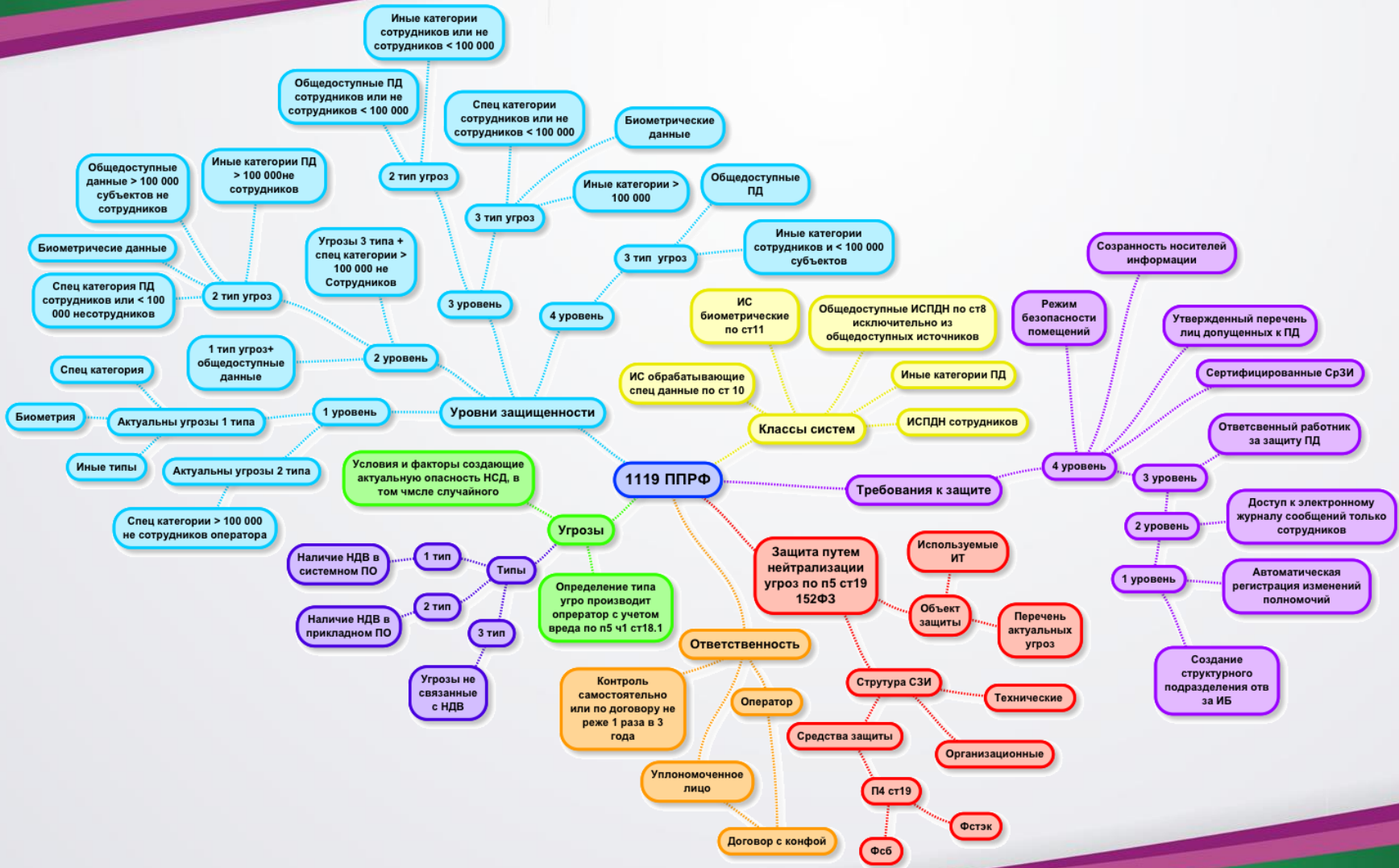


# Обязанности

- Оператор **самостоятельно определяет состав и перечень мер**, необходимых и достаточных для выполнения обязанностей, предусмотренных ФЗ-152 и принятыми в соответствии с ним нормативно-правовыми актами, если иное не предусмотрено федеральными законами.



# Классификация ИСПДн



# Классификация

Категория ПДн + кол-во	АУ 1 типа	АУ 2 типа	АУ 3 типа
<b>Спец.категории ПДн</b> более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	1	1	2
<b>Спец.категории ПДн</b> сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	1	2	3
<b>Биометрические ПДн</b>	1	2	3
<b>Иные категории ПДн</b> более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	1	2	3
<b>Иные категории ПДн</b> данных сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора	1	3	4
<b>Общедоступные ПДн</b> более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	2	2	4
<b>Общедоступные ПДн</b> сотрудников оператора или общедоступные ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	2	3	4

# Требования

- **Регулярный контроль за выполнением требований**
  - Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

# Требования

- **Физическая безопасность и контроль доступа**
  - Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения





# Требования

- **Безопасность носителей**
  - Обеспечение сохранности носителей персональных данных



# Требования

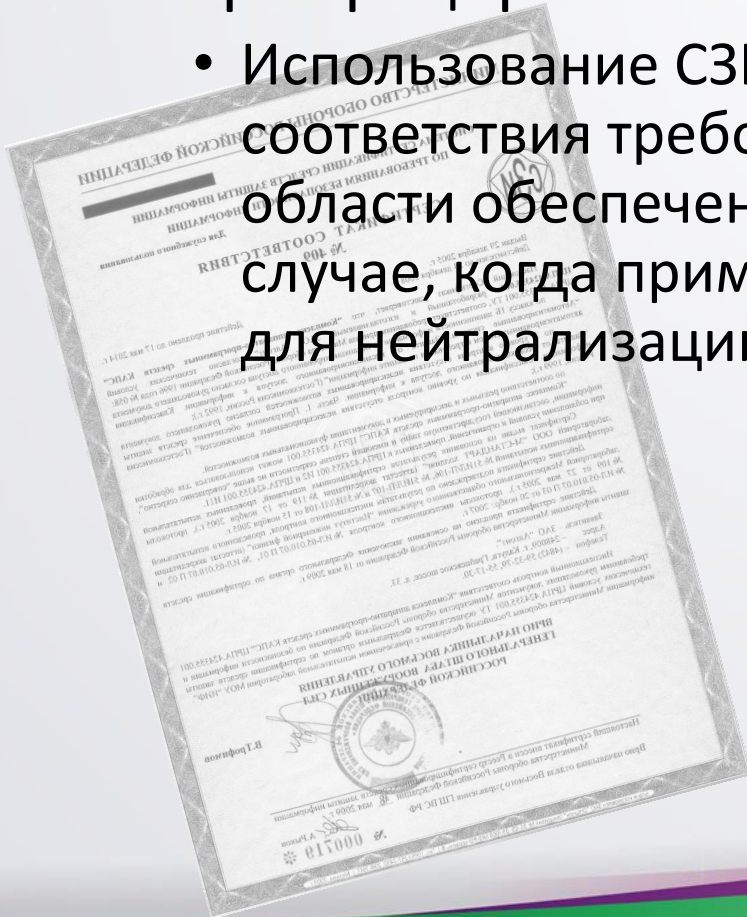
- **Перечень допущенных лиц**

- Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

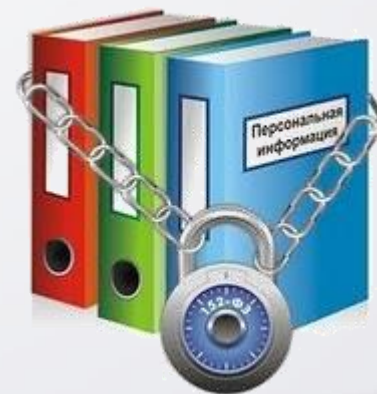


# Требования

- Сертифицированные СЗИ
  - Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

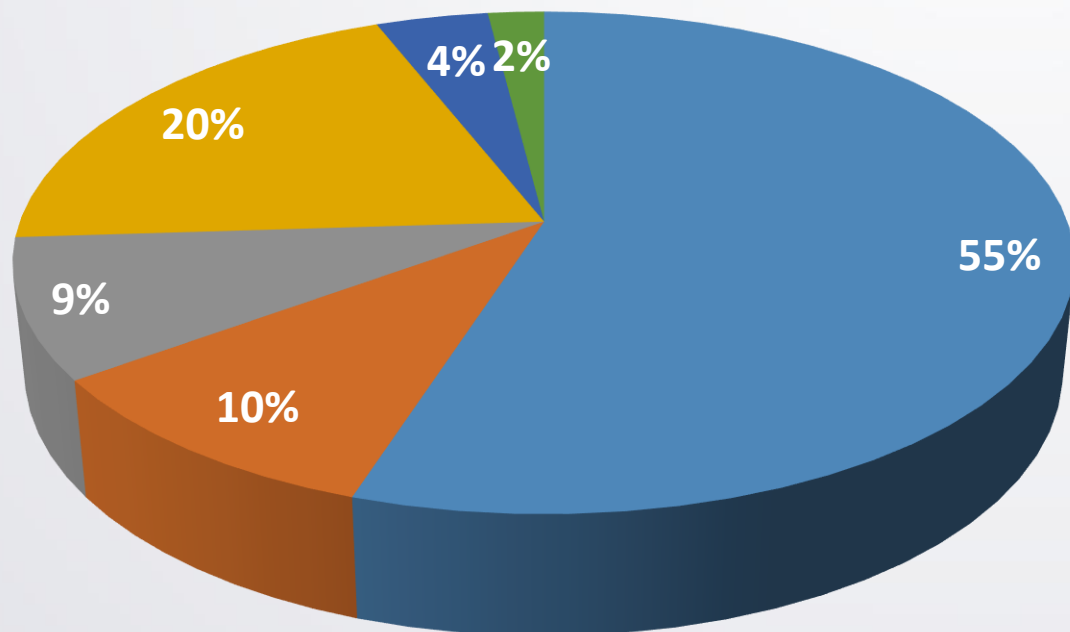


# Система безопасности информационных технологий



# Основная угроза - персонал

Анализ нарушений и проблем с АИС  
(Computer Security Institute)



- Ошибки персонала
- Нечестные сотрудники
- Обиженные сотрудники
- Отказы и сбои в работе АИС
- Вирусы

# Система обеспечения БИТ

- Цель – достижения заданного (приемлемого) уровня ИБ организации
- Распределение функций между исполнителями и организация процессов их взаимодействия
- Основной вопрос:  
**Кто и что в этой системе должен делать?**

# Необходимые условия БИТ

- Наличие в организации полной и непротиворечивой правовой базы по вопросам БИТ
- Распределение функций всех подразделений и должностных лиц на всех этапах жизненного цикла АИС (полномочия, ответственность)
- Наличие подразделения защиты информации наделенного необходимыми полномочиями и непосредственно отвечающего за формирование и реализацию единой политики БИТ в организации

# Технология обеспечения БИТ

- Назначение должностных лиц
- Строгий учет всех подлежащих защите ресурсов
- Разработка орг.распорядительных документов
- Реализация (реорганизация) технологических процессов АИС с учетом требований по безопасности
- Принятие эффективных мер сохранности и физической целостности технических средств
- Применение физических и технических (программно-аппаратных) средств защиты



# Технология обеспечения БИТ

- Регламентация процессов обработки информации
- Четкое знание и строгое соблюдение всеми сотрудниками требования по БИТ
- Персональная ответственность сотрудников за свои действия (бездействие) в рамках своих функциональных обязанностей
- Эффективный контроль за соблюдением требований по обеспечению безопасности информации
- Проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации

# Некоторые выводы

- К обеспечению БИТ должны привлекаться практически все сотрудники, в том числе и обслуживающий персонал
- Институт ответственных за обеспечение безопасности – руководители структурных подразделений, руководители проектов
- Необходима система повышения компетентности сотрудников в области БИТ
- Необходима «Концепция обеспечения информационной безопасности»



# Надзорные органы

- Уполномоченный орган по защите прав субъектов персональных данных - **РОСКОМНАДЗОР**
- ФОИВ, уполномоченный в области обеспечения безопасности – **ФСБ**
- ФОИВ, уполномоченный в области противодействия техническим разведкам и технической защите информации - **ФСТЭК**



# Контакты

- Павлов Александр Владиславович
  - [pavlov.av@ciur.ru](mailto:pavlov.av@ciur.ru), [pavlov.av@obr18.ru](mailto:pavlov.av@obr18.ru)
  - 334-373
- АУ УР «региональный центр информатизации и оценки качества образования»
  - г.Ижевск, ул.Ленина, д.16
- Образовательный портал УР
  - [www.ciur.ru](http://www.ciur.ru)
  - Файловый архив
  - [ftp.obr18.ru](ftp://obr18.ru)

