

Информационная безопасность



Сергей Халяпин
ведущий инженер ЛИВС

Защита персональных данных

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Перечни ПДн определяют:

- 75** Международных правовых актов
- 13** Кодексов РФ
- 100** Федеральных законов
- 250** Актов Правительства РФ



152-ФЗ от 27 июля 2006

Структура законодательства России по персональным данным

Конвенции и иные
международные
договора



Европейская конвенция

Законы

152-ФЗ от 27.07.2006

Постановления
правительства

№ 211 от
21.03.2012

**№ 1119 от
01.11.2012**

№ 512 от
06.07.2008

№ 687 от
15.09.2008

№ 940 от
18.09.2012

Приказы
и иные документы

**Роскомнадзор
№ 274 от 15.03.2013**

**3 НМД
ФСТЭК**

**2 НМД
ФСБ**

Закон N 149-ФЗ

«Об информации, ИТ и о защите информации»

Общедоступная информация

Свободно распространяемая

Предоставляемая по соглашению

Подлежит предоставлению

Информация ограниченного доступа

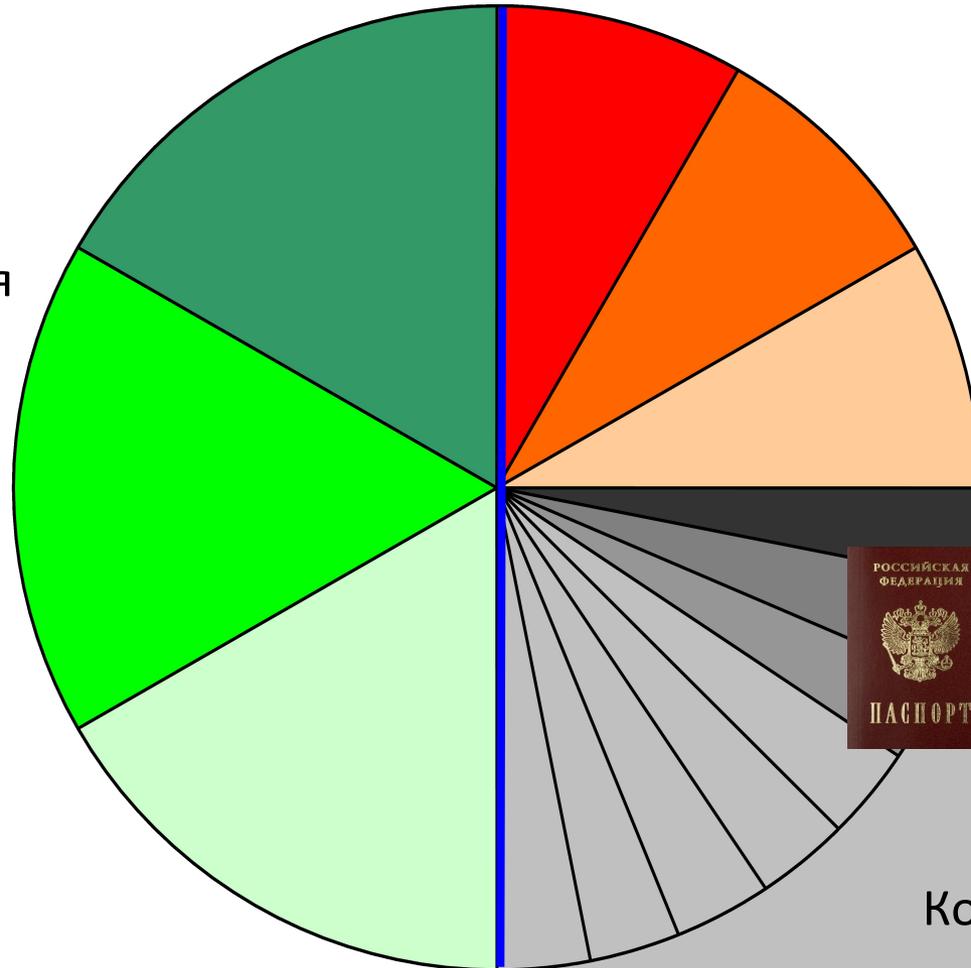
Государственная тайна

Служебная тайна

Персональные данные

Коммерческая тайна

Конфиденциальная



149-ФЗ от 27 июля 2006

Защита персональных данных

Необходимые меры



- Ответственный за организацию обработки ПДн
 - Разработать и утвердить около 60 требуемых документов
 - Правовые, организационные и технические меры по обеспечению безопасности ПДн
 - Периодические проверки условий обработки ПДн
-
- Знакомить сотрудников, осуществляющих обработку ПДн, с положениями законодательства РФ о персональных данных
 - Уведомить Роскомнадзор об обработке ПДн
 - Осуществить обезличивание ПДн
 - Опубликовать документы, определяющие политику в отношении обработки ПДн

Концепция информационной безопасности



Информационная безопасность –

защищенность информационных систем (данных и обрабатывающей их инфраструктуры) от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре.

Обеспечивает:

- Конфиденциальность
- Целостность информации
- Доступность информации



Концепция информационной безопасности



Концепция - официальный документ

- В самом общем виде сформулированы цели и приоритеты в области ИБ
- Намечены пути достижения этих целей

Меры защиты информации:

- законодательные (правовые)
- организационные (административные)
- физические
- технические (аппаратные и программные)



Нарушители и угрозы безопасности



Нарушители:

- Внешние
- Внутренние

Угрозы:

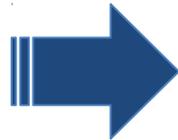
- Утечка, уничтожение, модификация, блокирование данных
- Программные
- Технические неисправности
- Стихийные (форс-мажор)
- НСД (случайно и преднамеренно)
- Недостатки организационных мер
- Ошибки пользователей



Правовые меры защиты данных

Государство:

- Законы
- Стандарты
- Указы
- Нормативные акты
- Распоряжения
- Регламенты



Институт:



Организационные меры

На основании Политики:

- Административные контрмеры
- Процедурные контрмеры
- Правила доступа в помещения ИС Института
- Правила доступа к ресурсам ИС Института
- Описания процессов работы в ИС
- Инструкции пользователей при работе в ИС
- Инструкции действий в чрезвычайных ситуациях



Физические меры защиты данных



- Защита зданий, помещений, объектов и средств информатизации
- Средства визуального наблюдения, связи и охранной сигнализации



Аппаратно-программные меры



- Уменьшение уязвимости коммуникаций
- Идентификация и аутентификация пользователей
- Разграничение прав доступа
- Контроль целостности программных и информационных ресурсов
- Контроль и регистрация событий безопасности
- Криптографические средства защиты данных



Важнейшие шаги



Политика информационной безопасности



- Инвентаризация ИС
- Отчет об инвентаризации
- На основании Отчета:
 - Перечень ИС Института
 - Перечень мер защиты
 - Топология сети
 - Прочие документы



Ответственность



Законодательство РФ

- Нарушение порядка сбора, хранения, использования или распространения информации
- Нарушение правил защиты информации
- Административное и уголовное наказание

Все пользователи ИС

- Персональная ответственность за безопасность данных
- Простота применения средств защиты
- Минимизация полномочий
- Обязательность контроля

Состояние дел. Важные вопросы.

Организационные

Принять временные Положения:

- о защите от вредоносных программ
- о парольной защите

Проблемы:

- Нет центра принятия оперативных решений по ИТ
- Нет общего подразделения по ИТ с утвержденными полномочиями
- Множественные точки доступа в интернет
- Слабые пароли
- Нелицензионное ПО
- Административные права пользователей
- Антивирусное ПО





Спасибо

за внимание!

