



**Уральский Центр Систем Безопасности**

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

# **Защита персональных данных. Практический алгоритм проведения работ в организациях, учреждениях, на предприятиях**

Истомин Дмитрий  
[distomin@ussc.ru](mailto:distomin@ussc.ru)

[www.USSC.ru](http://www.USSC.ru)



# Содержание

- Обследование ИСПДн
- Оптимизация ИСПДн
- Разработка внутренней документации
- Создание проекта СЗПДн
- Внедрение СЗПДн
- Аттестация СЗПДн
- Сопровождение СЗПДн



# Этап 1. Обследование ИСПДн

- Анализ процессов обработки ПДн
- Определение категорий обрабатываемых ПДн
- Определение подразделений и сотрудников, допущенных к обработке ПДн
- Идентификация ИСПДн





## Этап 2. Оптимизация ИСПДн

**Сегментирование** – разделение одной ИСПДн на несколько с целью уменьшения числа субъектов, чьи данные обрабатываются в каждой ИСПДн

**Уточнение** объема ПДн, необходимого к обработке (список необходимых данных)



**Уральский Центр Систем Безопасности**

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

## Этап 2. Оптимизация ИСПДн

### **Обезличивание персональных данных**

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

*152-ФЗ «О персональных данных»<sub>5</sub>*



## Этап 2. Оптимизация ИСПДн

### Неавтоматизированная обработка

Обработка ПДн **не может быть признана** осуществляемой с использованием средств автоматизации **только на том основании, что ПДн содержатся в информационной системе либо были извлечены из нее.**

*ПП № 687 от 15.09.2008 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»*



Уральский Центр Систем Безопасности

Технологии защиты бизнеса.  
Аудит. Проектирование.  
Внедрение. Сопровождение.

## Этап 3. Разработка внутренней документации. Модель угроз

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) **определение угроз безопасности** персональных данных при их обработке, **формирование** на их основе **модели угроз**;

*ПП № 781 от 17.11.2007 г.*

*«Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»*



## Этап 3. Разработка внутренней документации. Модель угроз

Заместителем директора ФСТЭК России  
14.02.2008г. утверждены документы:

- Базовая модель угроз безопасности ПДн при их обработке в ИСПДн
- Порядок проведения классификации информационных систем персональных данных





## Этап 3. Разработка внутренней документации. Акт классификации

**категория 1** - касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

**категория 2** - позволяющие идентифицировать субъекта и получить о нем дополнительную информацию;

**категория 3** - ПДн, позволяющие идентифицировать субъекта;

$X_{\text{ПД}}$ \ $X_{\text{НПД}}$	3	2	1
4	К4	К4	К4
3	К3	К3	К2
2	К3	К2	К1
1	К1	К1	К1

*«Порядок проведения классификации информационных систем персональных данных» от 13.02.2008г.*



## Этап 3. Разработка внутренней документации. ОРД

- Положение о защите персональных данных
- Приказ о назначении администратора безопасности ИСПДн
- Приказ об утверждении списка лиц, которым необходим доступ к ПДн, обрабатываемым в ИСПДн, для выполнения служебных (трудовых) обязанностей
- Журнал учета средств защиты информации
- ...



## Этап 3. Разработка внутренней документации. ОРД

В общем виде **положение** должно содержать:

- организационную структуру системы обеспечения безопасности ПДн
- обязанности должностных лиц, в части обеспечения безопасности ПДн
- порядок обучения администраторов средств (систем) защиты информации, и первичного инструктажа пользователей
- правила антивирусной защиты



## Этап 3. Разработка внутренней документации. ОРД

В общем виде **положение** должно содержать:

- порядок организации ведения и периодической проверки электронного журнала обращений пользователей информационной системы к ПДн
- порядок контроля за соблюдением условий использования средств защиты информации

*«Методические рекомендации по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,  
утвержденные УФСТЭК по УрФО<sup>12</sup>*



## Этап 4. Проектирование СЗПДн

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных **обязан** принимать необходимые организационные и **технические** меры, в том числе использовать шифровальные (криптографические) средства, для защиты ПДн от **неправомерного** или случайного **доступа** к ним, **уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.**

*152-ФЗ «О персональных данных»*



## Этап 4. Проектирование СЗПДн

- Защита информации от утечки по техническим каналам
- Защита информации от несанкционированного доступа, обеспечивающая функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевое взаимодействия



## Этап 4. Проектирование СЗПДн

- ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
- ГОСТ Р 51.583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.



## Этап 5. Внедрение СЗПДн

- Подготовка персонала
- Пусконаладочные работы
- Проведение предварительных испытаний
- Проведение опытной эксплуатации
- Проведение приёмочных испытаний

*ГОСТ 34.601-90. Информационная технология.  
Комплекс стандартов на автоматизированные  
системы. Стадии создания*





Уральский Центр Систем Безопасности

Технологии защиты бизнеса.

Аудит. Проектирование.

Внедрение. Сопровождение.

## Этап 6. Аттестация СЗПДн

Оценка соответствия ИСПДн по требованиям безопасности ПДн проводится:

**для ИСПДн 1 и 2 классов** - обязательная сертификация (**аттестация**) по требованиям безопасности информации;

**для ИСПДн 3 класса** - декларирование соответствия требованиям безопасности информации;

*«Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн»*



## Этап 7. Сопровождение СЗПДн

12. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя:

- з) **контроль** за соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;
- и) **разбирательство** и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн...

*ПП № 781 от 17.11.2007 г.*



# Проблемные вопросы

- Отсутствие ответственных лиц
- Отсутствие специалистов по ИБ
- Отсутствие средств СЗИ для ПДн
- Неконкретность требований законодательства
- Противоречия при выполнении некоторых требований



**Уральский Центр Систем Безопасности**

Технологии защиты бизнеса.  
Аудит. Проектирование.  
Внедрение. Сопровождение.

**ООО «УЦСБ»**

**620026, Екатеринбург, ул.  
Красноармейская, д.78Б, оф.902  
Тел.: +7 (343) 379-98-34  
Факс: +7 (343) 264-19-53**

**[info@ussc.ru](mailto:info@ussc.ru)**

**[www.USSC.ru](http://www.USSC.ru)**