Аладдин РД

Защита персональных данных на предприятии.
Проблемы и решения

Руководитель направления
по работе с государственными заказчиками
Чугунов Владимир

27 июня 2012 г.

Защита персональных данных на предприятии.

- ✓Где прячутся персональные данные на предприятии?
- ✓Что делать с персональными данными?
- ✓Кто виноват? Что делать?

  Кто со всем этим будет разбираться?
- ✓Что предлагает Аладдин Р.Д.?

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 3.
Основные понятия, используемые в настоящем Федеральном законе

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 3.
Основные понятия, используемые в настоящем Федеральном законе

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 3.
Основные понятия, используемые в настоящем Федеральном законе

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 18.1
Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 18.1
Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 18.1
Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 18.1
Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 18.1
Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 18.1
Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 19
Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые *правовые, организационные* и *технические* меры или обеспечивать их принятие для защиты персональных данных

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 19
Меры по обеспечению безопасности персональных данных при их обработке

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 19
Меры по обеспечению безопасности персональных данных при их обработке

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 19
Меры по обеспечению безопасности персональных данных при их обработке

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, **а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными** в информационной системе персональных данных;

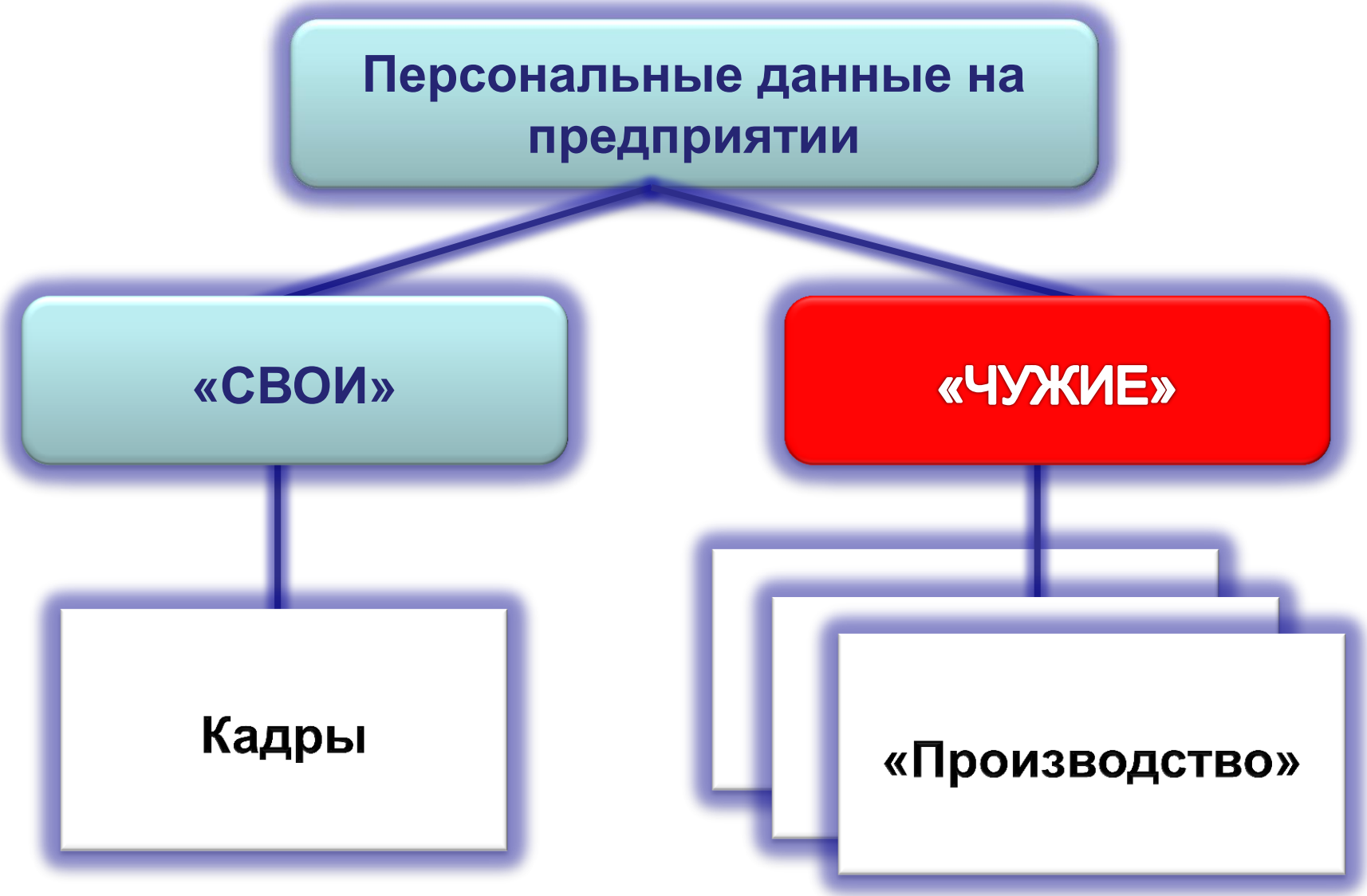
Требования законодательства

Федеральный закон № 152-ФЗ «О персональных данных»

Статья 19
Меры по обеспечению безопасности персональных данных при их обработке

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Персональные данные. Где они?

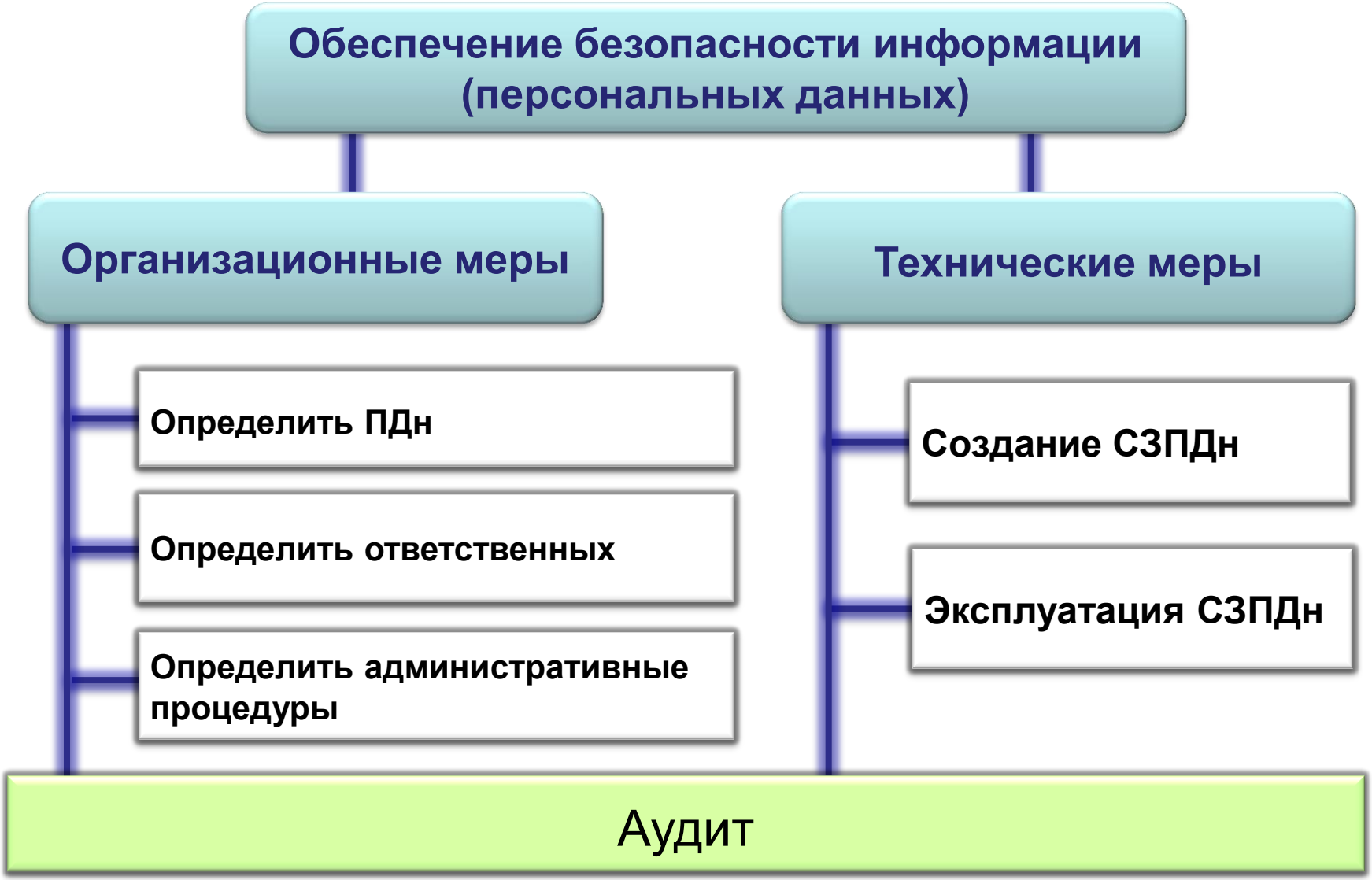


Что делать с персональными данными?

Персональные данные – это информация!

Информацию нужно защищать!

Что делать?


Обеспечение безопасности информации (персональных данных)
Организационные меры
Технические меры
Определить ПДн
Определить ответственных
Определить административные процедуры
Создание СЗПДн
Эксплуатация СЗПДн
Аудит

Что делать?

Определить состав обрабатываемых ПДн, цели и условия обработки, срок хранения ПДн

- **Составление перечня ПДн.**
- **Категоризация ПДн.**
- **Разработка Положения об обработке персональных данных.**
- **Разработка и оформление процедур получения согласия на обработку ПДн, обработки ПДн без согласия субъекта ПДН, доступа субъекта ПДн к ПДн, внесения изменений, блокировки и удаления ПДн, уведомление субъекта ПДн об изменениях и принятых мерах, отказа в предоставлении доступа субъекту к ПДн.**
- **Обучение и информирование персонала, оценка его квалификации.**

Кто будет отвечать?

- За защиту ПДн?
- За эксплуатацию СЗИ, СКЗИ?
- За администрирование ИБ?

Определить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн

- **Организация –**

  Руководство по защите ПДн (информации).

- **Подразделение –**

  Положение о структурном (производственном) подразделении.

- **Должностное лицо –**

  Должностная инструкция (специальный раздел).

  Руководств администратора ИБ.

Что делать?

Технические меры

Информационные системы

- Определение уровня защищённости
  - Модель угроз
  - Модель нарушителя
  - Классификация ИСПДн
- Создание (совершенствование) СЗПДн
- Оценка соответствия
- Организация процессов
- Постоянный контроль защищённости

Меры общережимного характера

- Организация КЗ
- Охрана помещений с ИСПДн
- Организация режима и контроля доступа в КЗ

Что делать?

Разработать модель угроз для ИСПДн

- Определение общего перечня угроз безопасности ПДн.
- Определение исходного уровня защищённости ИСПДн.
- Определение актуальности полученных угроз безопасности ПДн для ИСПДн.
- Разработка Модели

Разработать модель нарушителя для ИСПДн

Что делать?

Выделить и классифицировать ИСПДн

- Обследовать инфраструктуру информационной системы.
- Составить перечень ИСПДн.
- Описать топологию, конфигурацию и условия работы ИСПДн.
- Классифицировать ИСПДн.
- Разработать план мероприятий по приведению инфраструктуры и организационно-распределительной документации заказчика в соответствие с требованиями законодательства
- Учесть носители информации, содержащие ПДн.

Что делать?

Спроектировать и реализовать систему защиты ПДн

- Формирование требований к комплексу средств защиты информации в ИСПДн.
- Разработка Технического задания на внедрение комплекса средств защиты информации.
- Выбор средств защиты информации.
- Разработка Технического проекта на внедрение комплекса средств защиты информации.
- Внедрение комплекса средств защиты информации.
- Разработка инструкции Ответственному за эксплуатацию, инструкции Администратора системы, инструкции Администратора безопасности.
- Разработка программы и методики испытания комплекса средств защиты информации.
- Проведение опытной эксплуатации.
- Проведение приёмосдаточных испытаний.
- Разработка организационно-распределительной документации.
- Доработка должностных инструкций для персонала.
- Формирование технического паспорта системы защиты ИСПДн и заключение о готовности к эксплуатации.

Что делать?

Провести оценку соответствия системы защиты ПДн требованиям нормативных документов

Обеспечить постоянный контроль защищённости ПДн

- ❑ Регламент контроля защищённости ПДн
- ❑ Проведение регулярного контроля защищённости ПДн (подготовка, проведение, анализ результатов, подготовка отчёта)
- ❑ Проведение мероприятий по результатам контроля.

Что предлагает Аладдин Р.Д.?

Аутентификация пользователей

Разграничение доступа к информации

Защищённое хранение информации

Почтовый адрес: 129226, Москва, ул. Докукина, д. 16, корп. 1
Телефон: +7 (495) 223-0001
Факс: +7 (495) 646-0882
E-mail: aladdin@aladdin-rd.ru
Сайт: www.aladdin-rd.ru

Благодарю за внимание!

Руководитель направления
по работе с государственными
заказчиками
Чугунов В.С.