Организация работы по защите персональных данных

Цель Федерального закона «О персональных данных»

Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 2

Распространенные заблуждения о том на кого распространяется ФЗ-152:

1. Мы обрабатываем / храним ПДн по поручению, мы «обработчики», а не Операторы ПДн.
2. Мы обрабатываем ПДн на основании заключенных трудовых и иных договоров, поэтому не являемся Оператором ПДн.
3. Мы не госорган, поэтому не является Оператором ПДн.

Приведенные суждения ОШИБОЧНЫ!

Основные понятия

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Представление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Пункты 1, 5 и 6 статьи 3

Конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 7

Каких данных достаточно для определения физ. лица?

- ФИО, дата рождения, серия и номер паспорта
- ФИО, дата рождения, адрес регистрации
- ФИО, телефон
- должность, место работы
- ...

Каких данных достаточно для определения физ. лица?

...если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными, даже если они не включают в себя данные документов, удостоверяющих личность.

Но!
(о формальной определенности)

Роскомнадзор:

…отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких — нет.

Перечень обрабатываемых ПДн

Субъекты ПДн

- Работники
- Кандидаты
- Клиенты
- Контрагенты и их представители
- . . . . . .

Категории ПДн

- Специальные
- Биометрические
- Общедоступные
- Иные

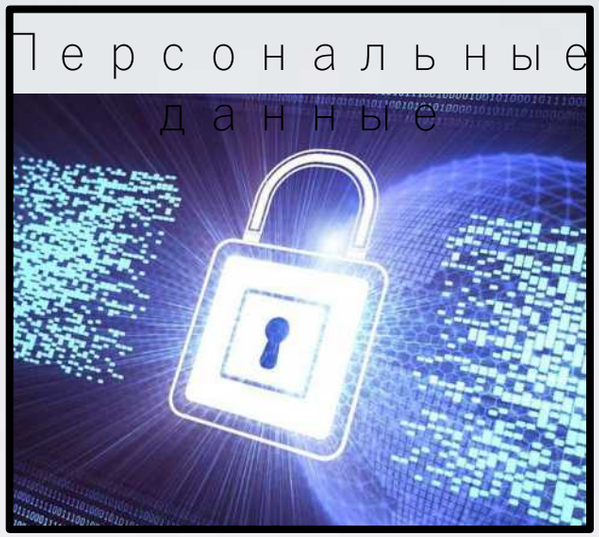
Состав обрабатываемых ПДн

Цели обработки

Кто вовлечен в обработку ПДн?

Отдел бухгалтерского учета

Финансовый отдел



Отдел персонала

Бизнес отделы

Отдел информационных технологий

Администрация

Юридический отдел

Сторонние организации

Основные понятия

Угрозы безопасности персональных данных – это совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать:

- уничтожение;
- изменение;
- блокирование;
- копирование;
- предоставление;
- распространение;
- иные неправомерные действия при обработке персональных данных в информационной системе персональных данных.

Часть 11 статьи 19

Основные понятия

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Часть 11 статьи 19

Участники взаимодействия при обработке персональных данных

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.

Пункт 2 статьи 3

Лицо, осуществляющее обработку персональных данных по поручению оператора.

Части 3, 4 и 5 статьи 6

Роскомнадзор:

…операторами могут быть как российские, так и иностранные граждане…

Участники взаимодействия при обработке персональных данных

Субъект персональных данных – физическое лицо.

Пункт 1 статьи 3

Представитель субъекта персональных данных.

Часть 1 статьи 9

Уполномоченный орган по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям 152-ФЗ – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи Роскомнадзор.

Статья 23

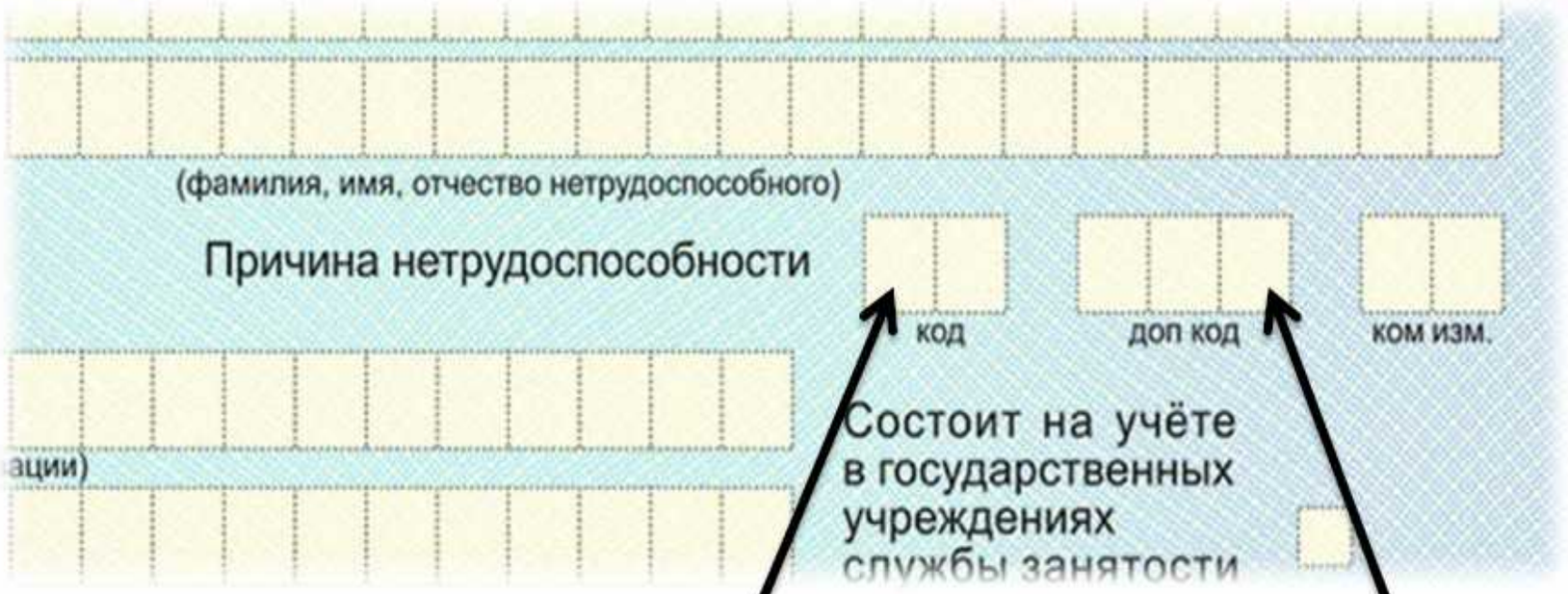
Сложности в обработке специальных категорий ПДн

<u>Обработка специальных категорий персональных данных :</u>

обеспечение наличия правовых оснований для обработки
повышенные требования по защите ИСПДн

Какие ПДн касаются состояния здоровья?

Листок нетрудоспособности – сведения о здоровье, или… о нетрудоспособности?



- ❑ Заболевание
- ❑ Травма
- ❑ Беременность и роды
- ❑ Уход за членом семьи
- ❑ …

- ❑ Лечение в санатории
- ❑ Лечение в НИИ
- ❑ …

Сведения о судимости

Обработка ПДн о судимости допустима в случаях и в порядке, определенными законодательством:

- категория социальной принадлежности, в которую входят сведения о профессии (сотрудники правоохранительных органов, судьи и проч.), ином социальном статусе лиц (малообеспеченные семьи, безработные);
- простое сообщение о наличии (отсутствии) судимости без дополнительной информации о факте осуждения и назначения судом наказания не может характеризоваться в качестве специальных ПДн.

Биометрические ПДн

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности, на основании которых можно установить личность и которые используются для установления личности.

Биометрические ПДн могут обрабатываться только при наличии согласия в письменной форме!

Эволюция подходов к понятию «биометрические ПДн»

Актуальный подход (комментарии Роскомнадзора):

…отсутствует единообразное толкование данного термина, а соответственно, и понимание…

…используются для идентификации, подтверждения личности по физиологическим параметрам, что предполагает применение биометрических методов аутентификации личности…

Понятие общедоступности ПДн

Не требует согласия обработка ПДн, сделанных общедоступными субъектом.

С письменного согласия субъекта ПДн могут включаться в общедоступные источники.

...согласие на размещение ПДн в определенном общедоступном источнике не дает основания оператору размещать ПДн в других общедоступных источниках...

Процедура получения согласия на обработку ПДн

Согласие должно быть:

- конкретным,
- информированным,
- сознательным,
- в любой форме, позволяющей подтвердить факт его получения.

Обязанность предоставить доказательство получения согласия (или доказательство наличия оснований обработки ПДн без согласия) возлагается на оператора. В отдельных случаях обработка персональных данных осуществляется только с согласия в письменной форме.

Согласие в письменной форме на обработку ПДн

Согласие в письменной форме должно содержать:

- ФИО, адрес, сведения об основном документе;
- сведения об операторе (наименование, адрес);
- перечень персональных данных;
- цель обработки;
- сведения о лицах, которым поручается обработка ПДн;
- перечень действий с ПДн, общее описание способов обработки;
- срок действия согласия и способ его отзыва;
- подпись субъекта персональных данных.

Согласие, подписанное ЭП

Виды электронных подписей

Простая

Усиленная

неквалифицированная

квалифицированная

…регистрация пользователя на сайте, подтвержденная логином и паролем, означает согласие субъекта на обработку его ПДн.

Согласие, подписанное ЭП

Согласие
в письменной форме

=

Согласие, подписанное в соответствии с № 63-ФЗ «Об электронной подписи»

Сфера действия 152-ФЗ и принципы обработки ПНд

Отношения, связанные с обработкой персональных данных, осуществляемой операторами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Часть 1 статьи 1

Сфера действия 152-ФЗ и принципы обработки ПНд

Действие 152-ФЗ не распространяется на отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- организации хранения, комплектования, учета и использования содержащих персональные данных документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

Сфера действия 152-ФЗ и принципы обработки ПНд

- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

- предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Часть 2 статьи 1

Установленные сроки

После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу осуществляется в соответствии с настоящим Федеральным законом. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны не позднее 1 января 2013 года представить в уполномоченный орган по защите прав субъектов персональных данных следующие сведения, указанные в части 3 статьи 22 № 152-ФЗ:

- пункт 5 - правовое основание обработки персональных данных;
- пункт 7.1 - ФИО физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- пункт 10 - сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- пункт 11 - сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

Статья 25

Риски неисполнения требований Федерального закона

- гражданско-правовые иски со стороны клиентов или работников;
- репутационные риски;
- принудительное приостановление или прекращение обработки персональных данных в компании;
- привлечение компании и (или) ее руководителя к административной или иным видам ответственности;
- приостановление действия или аннулирование лицензий (при определенных условиях);
- прочие риски.

Статья 24: лица, виновные в нарушении требований Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Изменения в 149-ФЗ «Об информации…»

Создается «Реестр нарушителей прав субъектов персональных данных»:

- Основание включения в Реестр – судебный акт;
- Если хостинг-провайдер не добивается устранения нарушения – блокировка ресурса.

Постановления правительства:

- ПП № 675 от 06.07.2015 «О порядке осуществления контроля за соблюдением требований, предусмотренных 149-ФЗ…»
- ПП № 857 от 19.08.2015 «Об автоматизированной информационной системе «Реестр нарушителей прав субъектов персональных данных»

Ответственность за нарушения 152-ФЗ

Статьи КоАП РФ:

- 5, 39 – отказ в предоставлении информации (гражданину).
- 13.11 – нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).
- 13.14 – разглашение информации с ограниченным доступом.
- 19.7 – непредставление сведений (информации) госоргану.

Ответственность за нарушения 152-ФЗ

Статьи КоАП РФ:

13.12 (п.2)

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключение средств защиты информации, составляющей государственную тайну).

13.12 (п.1, 5)

Нарушение (в т.ч. грубое) условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

Ответственность за нарушения 152-ФЗ

Статьи КоАП РФ:

13.13

Занятие видами деятельности в области защиты информации (за исключением информации, составлющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии).

13.13

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Ответственность за нарушения 152-ФЗ

Статьи УК РФ:

137 – Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

140 – Отказ должностного лица предоставить документы, затрагивающие права и свободы субъекта.

272 - 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.

Обязанности по защите

Статья 19 п.1.
Оператор при обработке персональных данных обязан принимать необходимы правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Постановление Правительства РФ от 19 ноября 2007 года № 781.
Утверждает «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Обязанности по защите

Федеральный закон № 152-ФЗ от 27 июля 2006 года
«О персональных данных».

П.10.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных.

П.17.

Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

Действия оператора по выполнению требований Федерального законодательства

Необходимо начать с определения:

- типа обрабатываемых персональных данных;
- состава персональных данных;
- количества субъектов персональных данных;
- цели их обработки.

После этого - направить уведомление в Уполномоченный орган.

И в продолжение:

- разработать систему защиты персональных данных;
- разработать документы, регламентирующие обработку персональных данных в организации;
- реализовать требования по инженерно-технической защите помещений;
- Провести аттестацию по требованиям безопасности информации.

Обеспечение законности обработки ПДн

Для всех обрабатываемых персональных данных всех категорий субъектов персональных данных необходимо определить:

- если ли законные основания для обработки персональных данных?
- требуется ли согласие субъекта на обработку персональных данных?

Направления работ с персональными данными

Организационно-правовое направление:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Техническое направление:

- руководящие и методические документы ФСТЭК России и ФСБ России

Направления работ с персональными данными

Организационно-правовое направление работ:

1. Выявление наличия/отсутствия признаков организации работы с персональными данными
2. Формирование перечня информации, относимой к персональным данным
3. Формирование перечня информационных систем персональных данных
4. Разработка или совершенствование существующей нормативной правовой базы, регламентирующей обработку персональных данных

Организационно-правовое направление работ

1. Выявление наличия/отсутствия признаков организации работы с персональными данными:

- анализ нормативной правовой базы, регламентирующей деятельность оператора;
- анализ функциональной структуры предприятия и схемы взаимодействия его подразделений;
- анализ взаимодействия предприятия с внешними организациями;
- анализ бизнес-процессов предприятия с целью выявления наличия/отсутствия признаков организации работы с персональными данными.

2. Формирование перечня информации, относимой к персональным данным:

- определение правовых оснований для обработки персональных данных оператором;
- категорирование персональных данных, обрабатываемых оператором;
- определение владельца персональных данных, обрабатываемых оператором;
- выявление способов обработки персональных данных и действий с персональными данными, производимых оператором:
  - без использования средств автоматизации
  - с использованием средств автоматизации
- выявление особенностей обработки персональных данных оператором:
  - внутри одного подразделения
  - в разных подразделениях
  - в подразделениях с учетом филиальной сети
  - при взаимодействии с внешними организациями
- исследование возможности снижения категории и объема персональных данных на основании оптимизации бизнес-процессов и правовых оснований для обработки персональных данных оператором.

3. Формирование перечня информационных систем персональных данных:

- определение правовых оснований для создания и использования оператором информационных систем персональных данных;
- определение состава и структуры каждой информационной системы персональных данных и технических особенностей ее построения и функционирования:
  - состав и структура программного обеспечения
  - технические средства обработки персональных данных
  - топология информационной системы персональных данных
- определение состава и структуры информационного взаимодействия с внешними системами.

4. Разработка или совершенствование существующей нормативной правовой базы, регламентирующей обработку персональных данных:

- административно-распорядительные документы оператора, направленные на организацию работы с персональными данными;
- положение об обработке персональных данных;
- инструкция о порядке обработки персональных данных без использования средств автоматизации;
- инструкция о порядке обработки персональных данных с использованием средств автоматизации;
- должностные инструкции специалистов, непосредственно осуществляющих обработку персональных данных;
- соглашение о неразглашении сведений, относимых к персональным данным;
- регламенты взаимодействия с внешними организациями при обработке персональных данных;
- и др.

Направление работ с ПДн

Техническое направление работ:

1. Выявление уязвимых звеньев и возможных угроз безопасности персональным данным в информационной системе персональных данных.

2. Разработка концептуальных документов оператора по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

3. Разработка новой или совершенствование существующей нормативной правовой базы, регламентирующей обеспечение безопасности персональных данных, обрабатываемых в информационной системе персональных данных оператора.

4. Организация работы с персональными данными в рамках разработки (модернизации) информационной системы персональных данных оператора в соответствии с утвержденными концептуальными документами обеспечения безопасности персональных данных.

Техническое направление работ

1. Выявление уязвимых звеньев и возможных угроз безопасности персональным данным в информационной системе персональных данных:

- анализ информационных систем персональных данных оператора, в т.ч.:
  - оценка возможности физического доступа к персональным данным;
  - выявление возможных каналов утечки информации, в т.ч. с использованием программно-математического воздействия на информационную систему персональных данных;
  - анализ возможностей программно-математического воздействия на информационную систему персональных данных;
  - анализ возможностей электромагнитного воздействия на информационную систему персональных данных;
- оценка ущерба от реализации угроз безопасности персональным данным;
- анализ имеющихся в распоряжении оператора мер и средств защиты персональных данных.

2. Разработка концептуальных документов по обеспечению безопасности персональных данных:

- формирование требований по обеспечению безопасности персональных данных при организации работы с ними:
  - составление перечня и проведение оценки актуальных угроз безопасности персональных данных;
  - разработка модели угроз безопасности ПНд с учетом конкретных условий функционирования информационных систем ПНд;
  - разработка модели нарушителя безопасности ПНд с учетом конкретных условий функционирования информационных систем ПНд, функциональных групп пользователей данных информационных систем ПНд;
- обоснование требований по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации (в случае необходимости):
  - определение целесообразности использования СКЗИ в информационных системах ПНд;
  - разработка модели угроз безопасности ПНд, обрабатываемых с использованием СКЗИ;
  - разработка модели нарушителя безопасности ПНд, обрабатываемых с использованием СКЗИ;
  - определение требуемого уровня криптографической защиты ПНд;
  - определение требуемого уровня специальной защиты от утечки по каналам ПЭМИН при защите ПНд с использованием СКЗИ;

- обоснование требований по обеспечению безопасности персональных данных при взаимодействии с внешними организациями и их информационными системами:
  - **проводится с учетом** требований 152-ФЗ, категорий внешних информационных систем ПНд, способов взаимодействия с ними;
  - **и в соответствии** с требованиями руководящих документов федеральных органов исполнительной власти, уполномоченных в области противодействия техническим разведкам и технической защиты информации и в области обеспечения безопасности (ФТЭК России и ФСБ России);
- разработка концептуальных документов по обеспечению безопасности персональных данных:
  - разработка концепции обеспечения безопасности ПНд оператора;
  - разработка моделей угроз и нарушителя безопасности ПНд оператора;
  - разработка технического задания на создание системы защиты ПНд в рамках разработки (модернизации) информационной системы ПНд;
  - обоснование выбора оптимальные мер и средств защиты ПНд в соответствии с целями защиты;
  - разработка финансово-экономического обоснования создания системы защиты ПНд в рамках разработки (модернизации) информационной системы ПНд.

3. Разработка (совершенствование) нормативной правовой базы, регламентирующей вопросы обеспечения безопасности персональных данных:

- положение о режиме защиты персональных данных;
- положение по организации и проведению работ по обеспечению безопасности ПНд при их обработке в информационных системах ПНд;
- требования по обеспечению безопасности ПНд при их обработке в информационных системах персональных данных;
- должностные инструкции специалистов оператора, обслуживающих информационные системы персональных данных, в части обеспечения безопасности персональных данных;
- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации;
- регламент взаимодействия с внешними организациями.

4. Организация работы с персональными данными в рамках разработки (модернизации) информационной системы персональных данных:

- проведение работ по созданию подсистемы защиты персональных данных в соответствии с утвержденными концептуальными документами;
- разработка эксплуатационной документации на подсистему защиты персональных данных в информационной системе персональных данных;
- проведение развертывания и ввода в опытную эксплуатацию подсистемы защиты персональных данных;
- осуществление доработки подсистемы защиты персональных данных по результатам опытной эксплуатации;
- аттестация информационной системы персональных данных.

Основы построения ИСПДн в защищенном исполнении

Жизненный цикл ИСПДн в защищенном исполнении

Создание модели защиты ИСПДн	Обеспечение защиты ИСПДн	Проведение специальных работ	Подготовка объекта информатизации	Обеспечение эксплуатации ИСПДн
Разработка документального описания модели защиты ИСПДн	**Реализация функций защиты ПДн**	**Исследования и проверки в интересах ИСПДн**	**Реализация функций защиты на объектах ИСПДн**	**Организация эксплуатации ИСПДн**
Определение объекта защиты (архитектура, процессы, ПДн)	Идентификация и аутентификация	Тематические исследования СЗИ:	Инженерно-техническая защита	Положение о режиме защиты ПДн
Модель нарушителя	Разграничение доступа к функциям и данным	❑ функции защиты от НСД;	Защита технических каналов:	Должностные инструкции
Модель угроз	Регистрация событий безопасности	❑ анализ наличия НДВ.	❑ ПЭМИН;	Конструкторская и эксплуатационная документация
Политика информационной безопасности	Контроль целостности	Проведение спецпроверок и специсследований	❑ акустический и виброакустический;	Аттестат соответствия
Требования по реализации	Криптографическая защита	Проведение сертификационных (аттестацио	❑ визуально-;	Обучение специалисто в
	Антивирусная		❑ прочие	Аудити

Соответствие требованиям по защите ИСПДн

Основы построения ИСПДн в защищенном исполнении

Иерархия моделей угроз

Базовая модель / модель угроз верхнего уровня

Типовая отраслевая модель угроз

Частная / детализированная модель угроз информационной системы персональных данных

- Состав и категории персональных данных
- Предметные риски
- Классы специальных информационных систем
- Отраслевая специфика
- Легитимность
- Снижение ресурсных затрат
- Унификация технических решений

Основы построения ИСПДн в защищенном исполнении

Классификация информационных систем персональных данных

Классификация информационных систем персональных данных в соответствии с «Порядком классификации информационных систем персональных данных», утвержденным совместным Приказом ФСТЭК/ФСБ/Мининформсвязи от 13 февраля 2008 года № 55/86/20, на основе анализа исходных данных о системе и обрабатываемых в ней персональных данных с учетом:

- типа обрабатываемых персональных данных,
- объема обрабатываемых персональных данных,
- заданных оператором характеристик безопасности персональных данных.

Определение актуальных угроз

Разработка модели нарушителя и угроз

Угрозы безопасности информации определяются по результатам анализа и оценки:

- возможностей нарушителей,
- уязвимостей системы,
- возможных способов реализации угроз,
- последствий от нарушения свойств безопасности.

Перечень актуальных угроз формируется на основе:

- вероятности реализации угрозы,
- опасности угрозы.

Вероятность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Основы построения ИСПДн в защищенном исполнении

Определение типа системы обработки персональных данных

Типовая информационная система обработки персональных данных по требованиям ФСТЭК России

Специальная информационная система обработки персональных данных по требованиям ФСТЭК России

Информационная система обработки персональных данных по требованиям ФСБ России

Основы построения ИСПДн в защищенном исполнении

Специальная система:

- Конфиденциальность + необходимость обеспечения хотя бы одной из характеристик безопасности персональных данных, отличной от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий)
- Информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных
- Информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы

Характеристики безопасности

Основные:

- **Конфиденциальность** – операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
- **Целостность** – способность средства вычислительно техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).
- **Доступность** – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мене необходимости.

Дополнительные:

- **Неотказуемость** – способность доказать, что действие или событие произошло таки образом, что факт действия или события не может быть опровергнут.
- **Учетность** – обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены уникально по отношению к субъекту.
- **Аутентичность** – идентичность объекта тому, что заявлено.
- **Адекватность** – свойство соответствия преднамеренному поведению и результатам.

Защита персональных данных

Оптимизация защиты персональных данных

- снижение количества субъектов персональных данных, обрабатываемых в ИСПДн;
- обезличивание персональных данных;
- сегментирование ИСПДн (объектовое, функциональное)
- объединение различных подсистем ИСПДн;
- типизация ИСПДн;
- разделение баз данных;
- минимизация мест хранения ПДн в ИТ-инфраструктуре предприятия;
- сокращение числа АРМ, необходимых для обработки персональных данных;
- перевод обработки персональных данных с автоматизированной на неавтоматизированную.

Определение уровня защищенности (ПП РФ № 1119)

- ✓ 4 уровня защищенности ПДн.
- ✓ Требования для достижения соответствующего УЗ.

Категория ПДн		Объем ПДн	Угрозы		
			1 типа	2 типа	3 типа
Спец. категория	НЕ сотрудники оператора	Более 100 000	1 уровень	1 уровень	2 уровень
		Менее 100 000	1 уровень	2 уровень	3 уровень
	Сотрудники оператора		1 уровень	2 уровень	3 уровень
Биометрические ПДн			1 уровень	2 уровень	3 уровень
Иные ПДн	НЕ сотрудники оператора	Более 100 000	1 уровень	2 уровень	3 уровень
		Менее 100 000	1 уровень	3 уровень	4 уровень
	Сотрудники оператора		1 уровень	3 уровень	4 уровень
Общедоступные	НЕ сотрудники оператора	Более 100 000	2 уровень	2 уровень	4 уровень
		Менее 100 000	2 уровень	3 уровень	4 уровень
	Сотрудники оператора		2 уровень	3 уровень	4 уровень

Правила отнесения угрозы безопасности ПДн к актуальной

Таблица для оценки актуальности угроз

	Возможность реализации угрозы (Y)	Показатель опасности угрозы		
		Низкая	Средняя	Высокая
0 ≤ **Y** ≤ 0,3	**Низкая**	неактуальная	неактуальная	актуальная
0,3 < **Y** ≤ 0,6	**Средняя**	неактуальная	актуальная	актуальная
0,6 < **Y** ≤ 0,8	**Высокая**	актуальная	актуальная	актуальная
Y > 0,8	**Очень высокая**	актуальная	актуальная	актуальная
		если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	если реализация угрозы может привести к негативным последствиям для субъектов персональных данных	если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

Защита персональных данных

Наличие системы организации работы с персональными данными и их защиты позволит:

- оптимизировать бизнес-процессы оператора, связанные с обработкой персональных данных
- снизить трудозатраты сотрудников оператора, связанные с обработкой персональных данных и взаимодействием с субъектами персональных данных;
- нормативно закрепить основы обработки персональных данных у оператора;
- сократить возможные жалобы и обращения граждан в уполномоченные органы на действия оператора;
- успешно проходить проверки контрольно-надзорных органов.

Меры реагирования РКН в 2015 г. в отношении интернет-ресурсов

Результат реагирования	Кол-во
Деятельность доменного имени приостановлена по решению суда	26
Деятельность доменного имени приостановлена по решению РКН	155
Информация, содержащая персональные данные субъектов, удалена	68
Хостинг приостановлен провайдером	7
Интернет-ссылка заблокирована	4
ВСЕГО:	260

Почему в России достаточно часто происходят утечки ПДн?

Потому что российские компании, в отличие от зарубежных, не несут расходы на:

- уведомление граждан о фактах утечки;
- ликвидацию последствий утечки;
- оказание содействия жертвам утечки;
- рекламу и маркетинг для восстановления размеров оборота вследствие оттока клиентов и падения имиджа компании;
- выплату штрафов за нарушение нормативных и законодательных требований.

Система нормативных правовых актов по защите ПДн

Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1982 / с изменениями от 15.06.1999) ETS №. 108

Федеральный закон от 19.12.2005 №. 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

Конституция Российской Федерации

Федеральный закон от 27.07.2006 №. 152-ФЗ «О персональных данных»

Постановление Правительства Российской Федерации от 01.11.2012 г. №. 1119

Постановление Правительства Российской Федерации от 06.07.2008 №. 512

Постановление Правительства Российской Федерации от 15.09.2008 №. 687

Приказа ФСБ России №. 378

Приказа ФСТЭК России №. 21

Постановление Правительства Российской Федерации от 21.03.2012 №. 211

Приказ Роскомнадзора от 22.07.2015 № 85

Форма заявления субъекта персональных данных о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных

1. Субъект персональных данных (представитель субъекта персональных данных)

(Ф.И.О., данные документа, удостоверяющего личность)

(наименование, реквизиты документа, подтверждающего полномочия)

2. СНИЛС