ДиалогНаука

Информационная безопасность. Защита персональных данных

Алексей Тесцов

Руководитель отдела управления проектами ЗАО «ДиалогНаука»

ДиалогНаука

О компании «ДиалогНаука»

- ЗАО «ДиалогНаука» создано 31 января 1992 года. Учредители - СП «Диалог» и Вычислительный центр РАН.
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были Aidstest, ADinf, Doctor Web.
- С 2004 года по настоящее время «ДиалогНаука» - системный интегратор, консультант и поставщик комплексных решений в сфере защиты информации.

ДиалогНаука

Членство в ассоциациях

- Межрегиональная общественная организация «Ассоциация защиты информации» (АЗИ)
- Ассоциации документальной электросвязи (АДЭ)
- Сообщество ABISS (Association of Banking Information Security Standards)
- Сертифицированный партнер BSI Management Systems
- Консорциум «Инфорус»

ДиалогНаука

Лицензии компании «ДиалогНаука»

- Лицензия ФСТЭК на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.
- Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации.
- Аттестат аккредитации органа аттестации в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 для проведения аттестации объектов информатизации.
- Лицензия ФСБ на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
- Лицензия ФСБ на осуществление технического обслуживания шифровальных (криптографических) средств.
- Лицензия ФСБ на распространение шифровальных (криптографических) средств.
- Лицензия ФСБ на предоставления услуг в области шифрования информации.
- и другие…

ДиалОгНаука

Основные направления деятельности

- Проведение аудита информационной безопасности
- Разработка системы управления безопасностью в соответствии с ISO 27001
- Разработка Политик информационной безопасности и других нормативных документов, регламентирующих вопросы защиты информации
- Проектирование, разработка и внедрение комплексных систем обеспечения информационной безопасности
- Поставка программного и аппаратного обеспечения в области защиты информации
- Техническое сопровождение поставляемых решений и продуктов

ДиалогНаука

Результаты работы компании в области защиты ПДн

- Выполнено более 100 проектов, связанных с обеспечением безопасности ПДн и выполнения требований законодательства
- Накоплен большой опыт проведения оценки соответствия ИСПДн (добровольной аттестации ИСПДн по требованиям безопасности информации)
- Переработаны проектные документы в соответствии с новой редакцией ФЗ (в том числе комплект типовых организационно-распорядительных документов для Операторов)
- Накоплен большой опыт в применении СЗИ, прошедших оценку соответствия, применяется весь спектр сертифицированных СЗИ, представленных на российском рынке

Опыт «ДиалогНаука» по защите ПДн

- **Страховые компании**: СК «Югория», ВТБ-Страхование, Согаз-Мед
- **Финансовые организации**: УК «КапиталЪ», ВТБ Капитал, ООО «Транснефть Финанс»
- **Банки**: Сити Банк, МосКоммерцбанк, ОТП Банк
- **Нефтегазовый сектор**: ОАО «Черномор-транснефть», ОАО «Северо-западные МН», ОАО «Северные МН»
- **Государственные компании**: ГК «Агентство по страхованию вкладов», ФГУП «Гознак», ФГУ «ЦСМС» РосРыболовства
- **Негосударственные пенсионные фонды**: НПФ «Лукойл Гарант», НПФ «Уголь», НПФ «Промагрофонд», МН «БПФ»
- **Телекоммуникационные компании**: ОАО «РТКОММ», ОАО «МТС», SkyLink

План презентации

- Часть 1. Формирование требований по защите ПДн при их обработке в ИСПДн
- Часть 2. Меры и средства защиты
- Часть 3. Текущая ситуация нормативного регулирования и проверок

Формирование требований по защите ПДн при их обработке в ИСПДН

ДиалОгНаука

ФЗ «О персональных данных»

- Федеральный закон «О персональных данных» № 152-ФЗ был принят Государственной думой 08.07.2006 и одобрен Советом Федерации 14.07.2006
- Федеральный закон полностью вступил в силу с 01.07.2011
- Федеральным законом регулируются отношения, связанные с обработкой персональных данных
- Целью Федерального закона является 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

ДиалОгНаука

ФЗ «О персональных данных»

Действие Федерального закона 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 данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

ДиалОгНаука

Ключевые изменения порядка обработки ПДн

- Изменения терминологии
- Изменения в процедурах получения ПДн и согласий на обработку
- Изменения во взаимодействии с субъектами ПДн
- Дополнения в порядок трансграничной передачи ПДн

ДиалогНаука

Ключевые изменения терминологии

Изменения терминов	Примечания
Персональные данные - любая информация, относящаяся к определенному или определяемому ~~на основании такой информации~~ физическому лицу (субъекту персональных данных)~~, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация~~	Понятие стало более размытым
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	Расширен перечень действий с ПДн
Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники	Новый термин, исключает «неавтоматизированную обработку» ПДн в электронном виде
Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц	Новый термин, фактически означает отнесение ПДн к общедоступным

ДиалогНаука

Ключевые изменения терминологии

Изменения терминов	Примечания
Предоставление персональных данных - действия, направленные на раскрытие персональных данных **определенному лицу** или **определенному кругу** лиц	Понятие стало более конкретным
Блокирование персональных данных - временное прекращение **обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)**	Распространяется на все действия с ПДн, предусматривается возможность уточнения заблокированных ПДн
Уничтожение персональных данных - действия, в результате которых **становится невозможным** восстановить содержание персональных данных в информационной системе персональных данных **и (или)** в результате которых уничтожаются материальные носители персональных данных	Небольшое уточнение
Обезличивание персональных данных - действия, в результате которых **становится невозможным без использования дополнительной информации** определить принадлежность персональных данных конкретному субъекту персональных данных	Важное уточнение, стало больше основания для отнесения к обезличенным ПДн

ДиалОгНаука

Ключевые изменения терминологии

Изменения терминов	Примечания
Информационная система персональных данных - совокупность **содержащихся в базах данных** персональных данных и **обеспечивающих их обработку информационных технологий** и технических средств	Понятие стало более конкретным, исключило обработку ПДн без использования средств автоматизации в ИСПДн
Трансграничная передача персональных данных - передача персональных данных **на территорию иностранного государства** органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу	Исчезло непонятное «через границу РФ», понятие стало более корректным

Удалены понятия	
Использование ПДн	Термин, пересекающийся с обработкой
Конфиденциальность ПДн	Избыточный термин с учетом введения терминов «распространение», «предоставление» и др.
Общедоступные ПДн	Избыточный термин с учетом введения терминов «распространение», «обезличивание» и др.

ДиалОгНаука

Изменения в процедурах получения согласий

- Согласие является лишь одним из случаев законной обработки ПДн
- Наиболее распространенным законным случаем обработки **без согласия субъекта** является «обработка персональных данных необходима для исполнения договора, стороной которого либо **выгодоприобретателем или поручителем** по которому является субъект персональных данных, а также **для заключения договора по инициативе субъекта персональных данных** или договора, по которому субъект персональных данных будет являться **выгодоприобретателем или поручителем**»
- Также обработка **без согласия субъекта** возможна, если «обработка персональных данных необходима для осуществления **прав и законных интересов оператора или третьих лиц** либо для достижения общественно значимых целей при условии, что при этом **не нарушаются права и свободы субъекта** персональных данных»
- Законна обработка ПДн о состоянии здоровья в случае обработки ПДн в соответствии с законодательством об **обязательных видах страхования, со страховым законодательством**

ДиалОгНаука

Изменения в процедурах получения согласий

- Оператор вправе поручить обработку персональных данных **другому лицу с согласия субъекта персональных данных**, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных…
- Лицо, осуществляющее обработку персональных данных **по поручению оператора**, **не обязано получать согласие** субъекта персональных данных на обработку его персональных данных

Изменения в процедурах получения согласий

Если необходимо получать согласие:

- Согласие на обработку персональных данных должно быть **конкретным, информированным и сознательным**. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем **в любой позволяющей подтвердить факт его получения форме**, если иное не установлено федеральным законом
- Обязанность предоставить **доказательство получения согласия** субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований… …**возлагается на оператора**
- В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в **письменной форме субъекта персональных данных**. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом **электронной подписью**.

ДиалОгНаука

Изменения в процедурах получения согласий

Согласие в письменной форме должно содержать (выделены изменения):

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- **фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);**
- наименование **или** фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- **наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;**
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также **способ** его отзыва, **если иное не установлено федеральным законом;**
- подпись субъекта персональных данных.

ДиалогНаука

Изменения во взаимодействии с субъектами ПДн

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) **правовые основания и цели** обработки персональных данных;

3) **цели** и применяемые оператором **способы обработки персональных данных**;

4) **наименование и место нахождения оператора**, сведения о лицах (**за исключением работников оператора**), которые имеют доступ к персональным данным или которым **могут** быть **раскрыты персональные данные на основании договора с оператором или на основании федерального закона;**

5) **обрабатываемые персональные данные, относящиеся к соответствующему субъекту** персональных данных, источник их получения, **если иной порядок представления таких данных не предусмотрен федеральным законом;**

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) **порядок осуществления субъектом** персональных данных **прав, предусмотренных настоящим Федеральным законом;**

8) **информацию об осуществленной или о предполагаемой трансграничной передаче данных;**

9) **наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку** персональных данных **по поручению оператора, если обработка поручена или будет поручена такому лицу;**

10) **иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.**

ДиалОгНаука

Изменения во взаимодействии с субъектами ПДн

Изменения в обязанностях Операторов:

- Добавились исключения в уведомлении субъекта об обработке **при получении Оператором ПДн не от субъекта ПДн** (п.4 ст. 18, в частности, если субъект ПДн уведомлен об осуществлении обработки соответствующим Оператором, если получены на основании договора и т.д.)
- Для получения информации об обработке ПДн необходимо предоставить **сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором** (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором
- Повторный запрос может быть составлен не ранее, чем через 30 дней после предыдущего (если более короткий срок не установлен **федеральным законом**, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, либо если обрабатываемые ПДн **не были предоставлены** ему для ознакомления **в полном объеме**)

ДиалОгНаука

Изменения во взаимодействии с субъектами ПДн

Изменены сроки ответов Оператора на запросу субъектов ПДн и уполномоченного органа по защите прав субъектов:

- Срок рассмотрения возражения субъекта ПДн против решения, порождающего юридические последствия для субъекта ПДн, или иным образом затрагивающее его права и законные интересы, на основании исключительно автоматизированной обработки его ПДн – 30 дней (ч.4 ст.16)
- Срок предоставления субъекту ПДн или его представителю информации о наличии ПДн, относящихся к соответствующему субъекту, а также предоставления возможности ознакомления с этими ПДн – 30 дней (ч.1 ст.20)
- Срок предоставления мотивированного отказа субъекту ПДн или его представителю в предоставлении информации о наличии ПДн, относящихся к соответствующему субъекту, а также предоставления возможности ознакомления с этими ПДн – 30 дней (ч.2 ст.20)
- Срок внесения необходимых изменений в неполные, неточные или неактуальные ПДн – 7 рабочих дней (ч.3 ст.20)
- Срок уничтожения ПДн – 7 рабочих дней со дня предоставления субъектом ПДн или его законным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки (ч.3 ст.20)
- Срок сообщения в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию – 30 дней (ч.4 ст.20)

ДиалОгНаука

Изменения в порядке трансграничной передачи ПДн

❖Трансграничная передача персональных данных на территории иностранных государств, **являющихся сторонами Конвенции Совета Европы** о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом …

❖Уполномоченный орган по защите прав субъектов персональных данных **утверждает перечень иностранных государств**, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных…

❖Оператор **обязан убедиться в том**, что иностранным государством, на территорию которого осуществляется передача персональных данных, **обеспечивается адекватная защита прав субъектов** персональных данных, до начала осуществления трансграничной передачи персональных данных

❖Трансграничная передача персональных данных на территории иностранных государств, **не обеспечивающих адекватной защиты прав субъектов** персональных данных, может осуществляться в случаях:

1)наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных…

...

4)исполнения договора, стороной которого является субъект ПДн

ДиалогНаука

Изменения в части уведомления

Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года (**и отправили уведомление об обработке**), обязаны представить в Роскомнадзор не позднее 1 января 2013 года, следующую дополнительную информацию:

- правовое основание обработки персональных данных
- ФИО физического лица или наименование юридического лица, ответственного за защиту персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты
- сведения о наличии или отсутствии трансграничной передачи персональных данных в процессе их обработки
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ

ДиалОгНаука

Лицо, ответственное за организацию обработки персональных данных

Лицо, ответственное за организацию обработки персональных данных:

- подотчетно исполнительному органу оператора
- осуществляет внутренний контроль за соблюдением требований законодательства
- доводит до сведения работников оператора положения законодательства
- организует прием и обработку обращений и запросов субъектов персональных данных

ДиалОгНаука

Уведомление об обработке ПДн

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:

1) ***обрабатываемых в соответствии с трудовым законодательством***;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных;

4) ***сделанных субъектом персональных данных*** общедоступными;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

ДиалогНаука

Уведомление об обработке ПДн

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, ***предусмотренных статьями 18.1 и 19 настоящего Федерального закона***, ***в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;***

Уведомление об обработке ПДн

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных.

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

ДиалогНаука

Обязанности Оператора по защите

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 выполнения требований Закона, в том числе:

- **назначает лицо, ответственного за организацию обработки** персональных данных
- **принимает внутренние нормативные документы** по вопросам обработки и защиты персональных данных
- принимает **правовые, организационные и технические меры** защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий
- **осуществляет внутренний контроль и (или) аудит** за соответствием обработки персональных данных законодательству
- **осуществляет оценку вреда субъектам, который может быть причинен субъектам** при нарушении законодательства и соотношения вреда и применяемых мер в соответствии с Законом
- **осуществляет ознакомление работников Оператора** с положениями законодательства и внутренними требованиями по вопросам обработки персональных данных
- обеспечивает неограниченный доступ к документам, определяющим политику в области персональных данных

ДиалОгНаука

Правовые, организационные и технические меры по защите ПДн

Оператор при обработке персональных данных **обязан** принимать необходимые 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**

Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности ПДн при их обработке в ИСПДн
- применением организационных и технических мер, обеспечивающих установленные Правительством РФ уровни защищенности персональных данных
- применением СЗИ, прошедших в установленном порядке процедуру оценки соответствия
- оценкой эффективности мер по обеспечению безопасности персональных данных **до ввода в эксплуатацию ИСПДн**
- учетом машинных носителей персональных данных
- обнаружением фактов НСД к персональным данным и принятием мер
- восстановлением персональных данных, модифицированных или уничтоженных вследствие НСД
- установлением правил доступа к персональным данным
- регистрацией и учетом всех действий с персональных данных
- контролем за принимаемыми мерами по обеспечению безопасности ПДн

ДиалогНаука

Нормативные акты по защите ПДн

- Правительство РФ с учетом ущерба субъекту, типа персональных данных, вида деятельности устанавливает:
  - **уровни защищенности** персональных данных
  - **требования, выполнение которых обеспечит достижение заданного уровня защищенности** персональных данных
  - требования к материальным носителям биометрических данных
- **Федеральные органы исполнительной власти**, **Банк России** и иные государственные органы в пределах своих полномочий принимают (по согласованию с ФСТЭК и ФСБ России) нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

ДиалОгНаука

Новые постановления правительства

- **Постановление правительства от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»**

- **Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

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.

4. **Выбор средств** защиты информации для системы защиты персональных данных осуществляется оператором **в соответствии с нормативными правовыми актами**, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

- 5. Информационная система является информационной системой, обрабатывающей **специальные категории** персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
- Информационная система является информационной системой, обрабатывающей **биометрические персональные данные**, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

- 5. Информационная система является информационной системой, обрабатывающей **общедоступные персональные данные**, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».
- Информационная система является информационной системой, обрабатывающей **иные категории персональных данных**, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

❖5. Информационная система является информационной системой, обрабатывающей **общедоступные персональные данные**, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

❖Информационная система является информационной системой, обрабатывающей **иные категории персональных данных**, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

❖Информационная система является информационной системой, обрабатывающей **персональные данные сотрудников** оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей **персональные данные субъектов** персональных данных, **не являющихся сотрудниками оператора.**

ДиалогНаука

Постановление правительства № 1119 от 1.11.2012

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием **недокументированных (недекларированных) возможностей в системном программном обеспечении**, используемом в информационной системе.
- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием **недокументированных (недекларированных) возможностей в прикладном программном обеспечении**, используемом в информационной системе.
- Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, **не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении**, используемом в информационной системе.

ДиалогНаука

Постановление правительства № 1119 от 1.11.2012

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием **недокументированных (недекларированных) возможностей в системном программном обеспечении**, используемом в информационной системе.
- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием **недокументированных (недекларированных) возможностей в прикладном программном обеспечении**, используемом в информационной системе.
- Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, **не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении**, используемом в информационной системе.

Постановление правительства № 1119 от 1.11.2012

❖7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18^1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

Работники	Не работники	Акт НДВ	Уровень
Специальные либо биометрические либо иные	Специальные либо биометрические либо иные	НДВ СПО	1 уровень
	специальные более 100000	НДВ ППО	1 уровень
Общедоступные	Общедоступные ПДн	НДВ СПО	2 уровень
специальные	специальные менее 100000	НДВ ППО	2 уровень
	общедоступные более 100000	НДВ ППО	2 уровень
	иные категории более 100000	НДВ ППО	2 уровень
	специальные более 100000	Нет НДВ	2 уровень
общедоступные	общедоступные менее 100000	НДВ ППО	3 уровень
иные категории	иные категории менее 100000	НДВ ППО	3 уровень
специальные	специальные менее 100000	Нет НДВ	3 уровень
	иные категории более 100000	Нет НДВ	3 уровень
Общедоступные	Общедоступные ПДн	Нет НДВ	4 уровень
иные категории	иные категории менее 100000	Нет НДВ	4 уровень

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

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

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

ДиалОгНаука

Постановление правительства № 1119 от 1.11.2012

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Постановление правительства № 1119 от 1.11.2012

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Постановление правительства № 1119 от 1.11.2012

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).

ДиалогНаука

Документы ФСБ России в дополнение ФЗ «О персональных данных»

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

ДиалогНаука

Документы ФСТЭК России в дополнение ФЗ «О персональных данных»

- «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн».
- «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн».
- ***Проект*** приказа «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

(http://www.fstec.ru/ru/deyatelnost/normotvorcheskaya/proekty/57-deyatelnost/normotvorcheskaya/proekty/prikazy/542-proekt-prikaza-fstek-rossii31)

ДиалОгНаука

Этапы формирования требований к системе защиты

- Моделирование угроз безопасности ПДн и выбор уровня защищенности ПДн
- Формирование требований на основе уровня защищенности в соответствии с нормативными документами, актуальными угрозами безопасности ПДн и уровнем потенциального нарушителя

ДиалогНаука

Как выбрать уровень защищенности?

1. Определить категории ПДн и качественно характеристики возможного ущерба от нарушения свойств безопасности

Например, в результате реализации угроз безопасности информации субъектам ПДн и оператору может быть нанесен ущерб различного характера, в том числе:

- материальный (финансовый) ущерб от разглашения защищаемой информации;
- **моральный, физический или материальный ущерб**, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб, связанный с необходимостью восстановления технических средств и защищаемых информационных ресурсов;
- материальный ущерб (потери), связанный с невозможностью выполнения возложенных функций;
- моральный и материальный ущерб, связанный с дезорганизацией деятельности.

ДиалОгНаука

Как выбрать уровень защищенности?

С точки зрения моделирования угроз безопасности ПДн рассматриваем только **моральный, физический или материальный** ущерб субъекту и оцениваем его качественно:

- Высокий уровень, если в результате нарушения безопасности возможны угроза его жизни и здоровью, значительный материальный ущерб;
- Средний уровень, если в результате нарушения безопасности возможны незначительный материальный ущерб, моральный ущерб;
- Низкий уровень, если в результате нарушения безопасности возможны последствия, не связанные с материальным, моральным ущербом, угрозами его жизни или здоровью

ДиалОгНаука

Как выбрать уровень защищенности?

2. Определить состав и характеристики ПО в компании (состав, производитель, типы лицензий, обновления и т.д.)

Угрозы НДВ в **системном ПО** целесообразно признавать актуальными только в случаях, когда возможен **высокий уровень ущерба** субъекту от нарушения свойств безопасности (то есть производитель системного ПО, а это в большинстве случаев Microsoft, заинтересован во внедрении НДВ или сокрытии уязвимостей ради Ваших ПДн).

Если возможен **средний уровень** ущерба субъекту ПДн, целесообразно признать актуальными угрозы, связанные с НДВ в **прикладном ПО**

ДиалОгНаука

Информационная система персональных данных

- ИСПДн - совокупность содержащихся в базах данных **персональных данных** и обеспечивающих их обработку **информационных технологий** и **технических средств**

Уточненное определение ИСПДн позволяет Операторам самостоятельно объединять/разделять различные информационные системы в ИСПДн с точки зрения их оптимальной защиты.

База данных — представленная в объективной форме совокупность самостоятельных материалов (статей, расчётов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ) (Гражданский кодекс РФ, ст. 1260).

ДиалогНаука

ИСПДн как объект защиты

- персональные данные, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в ИСПДн;
- технические средства, осуществляющие обработку ПДн;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы (технические средства и системы, не предназначенные для обработки ПДн, но размещенные, в помещениях, в которых расположены ИСПДн)

Проект требований ФСТЭК России

3. Настоящий документ предназначен для выбора операторами информационных систем и (или) уполномоченными лицами организационных и технических мер по обеспечению безопасности персональных данных и их реализации в системе защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, в соответствии с установленным уровнем защищенности персональных данных.

Выбранные и реализованные в системе защиты персональных данных организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах должны обеспечивать нейтрализацию актуальных угроз безопасности персональных данных, определенных в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Проект требований ФСТЭК России

5. Для обеспечения безопасности персональных данных при их обработке в информационных системах применяются средства защиты информации, прошедшие в соответствии с законодательством Российской Федерации **оценку соответствия в форме обязательной сертификации** на соответствие требованиям по безопасности информации.

По решению оператора (уполномоченного лица) оценка достаточности выбранных и реализованных в системе защиты персональных данных организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах может осуществляться в рамках **аттестации информационной системы**.

ДиалОгНаука

Подсистемы защиты*

8. В систему защиты персональных данных в зависимости от актуальных угроз безопасности ПДн и структурно-функциональных характеристик ИСПДн включаются следующие меры:

- обеспечение доверенной загрузки;
- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- обеспечение целостности информационной системы и информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств и систем связи и передачи данных.

Проект требований ФСТЭК России

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в системе защиты персональных данных, включает:

- выбор базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных, обрабатываемых в информационной системе, в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении № 1 к настоящему документу;
- адаптацию выбранного базового набора мер по обеспечению безопасности персональных данных применительно к структурно-функциональным характеристикам информационной системы, реализуемым информационным технологиям, особенностям функционирования информационной системы, а также с учетом целей защиты персональных данных (конфиденциальности, целостности, доступности);

Проект требований ФСТЭК России

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в системе защиты персональных данных, включает:

- дополнение адаптированного базового набора мер по обеспечению безопасности персональных данных дополнительными мерами по обеспечению безопасности персональных данных, приведенными в приложении № 1 к настоящему документу, но не определенными в качестве базовых, и определение их содержания для обеспечения блокирования (нейтрализации) актуальных угроз безопасности персональных данных, а также дополнительными мерами, обеспечивающими выполнение требований по обеспечению безопасности персональных данных, установленными иными нормативными правовыми актами в области защиты информации.

Проект требований ФСТЭК России

- 12. Для обеспечения 4 уровня защищенности персональных данных в информационных системах персональных данных должны применяться средства защиты информации 6 класса защиты (6 класса защищенности средств вычислительной техники).
- Для обеспечения 3 уровня защищенности персональных данных в информационных системах, в которых не определены в качестве актуальных угрозы 2-го типа и которые не подключены к информационно-телекоммуникационным сетям международного информационного обмена, должны применяться средства защиты информации не ниже 5 класса защиты (5 класса защищенности средств вычислительной техники).

Проект требований ФСТЭК России

- Для обеспечения 1 и 2 уровня защищенности персональных данных в информационных системах персональных данных, а также 3 уровня защищенности персональных данных в информационных системах, в которых определены в качестве актуальных угрозы 2-го типа или которые подключены к информационно-телекоммуникационным сетям международного информационного обмена, должны применяться средства защиты информации не ниже 4 класса защиты (5 класса защищенности средств вычислительной техники).
- 13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых в настоящем документе не определены меры по обеспечению безопасности персональных данных, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

Реализация требований.
Меры и средства защиты

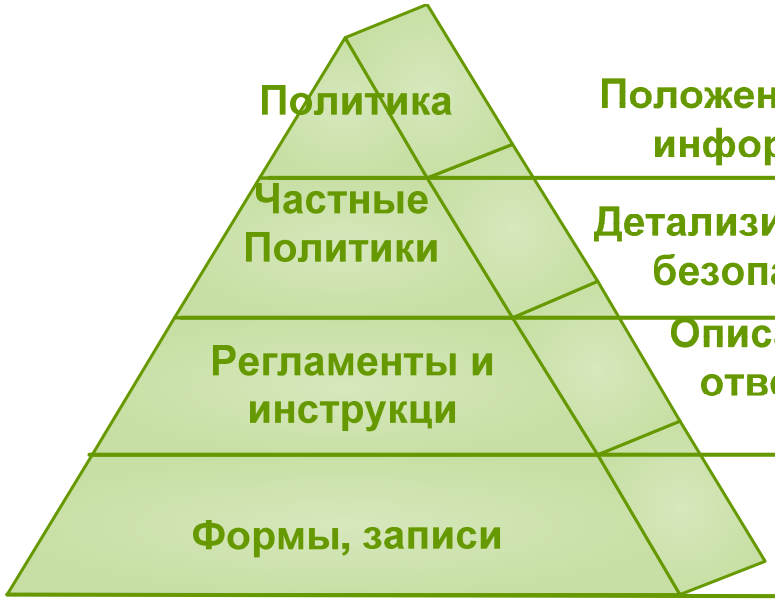
ДиалогНаука

Порядок проведения работ по приведению в соответствие

- подготовительный этап выполнения работ;
- стадия обследования (обследование ИСПДн, процессов обработки ПДн, разработка модели угроз и нарушителя, выбор уровня защищенности);
- этап разработки организационно-распорядительных документов;
- стадия проектирования СЗПДн, включающая в себя разработку технического проекта;
- этап ввода в действие СЗПДн;
- оценка эффективности реализованных мер защиты ПДн;
- поддержка реализованных процессов и мер защиты

ДиалогНаука

Идеальная иерархия внутренних нормативных актов



Положения корпоративной Политики информационной безопасности

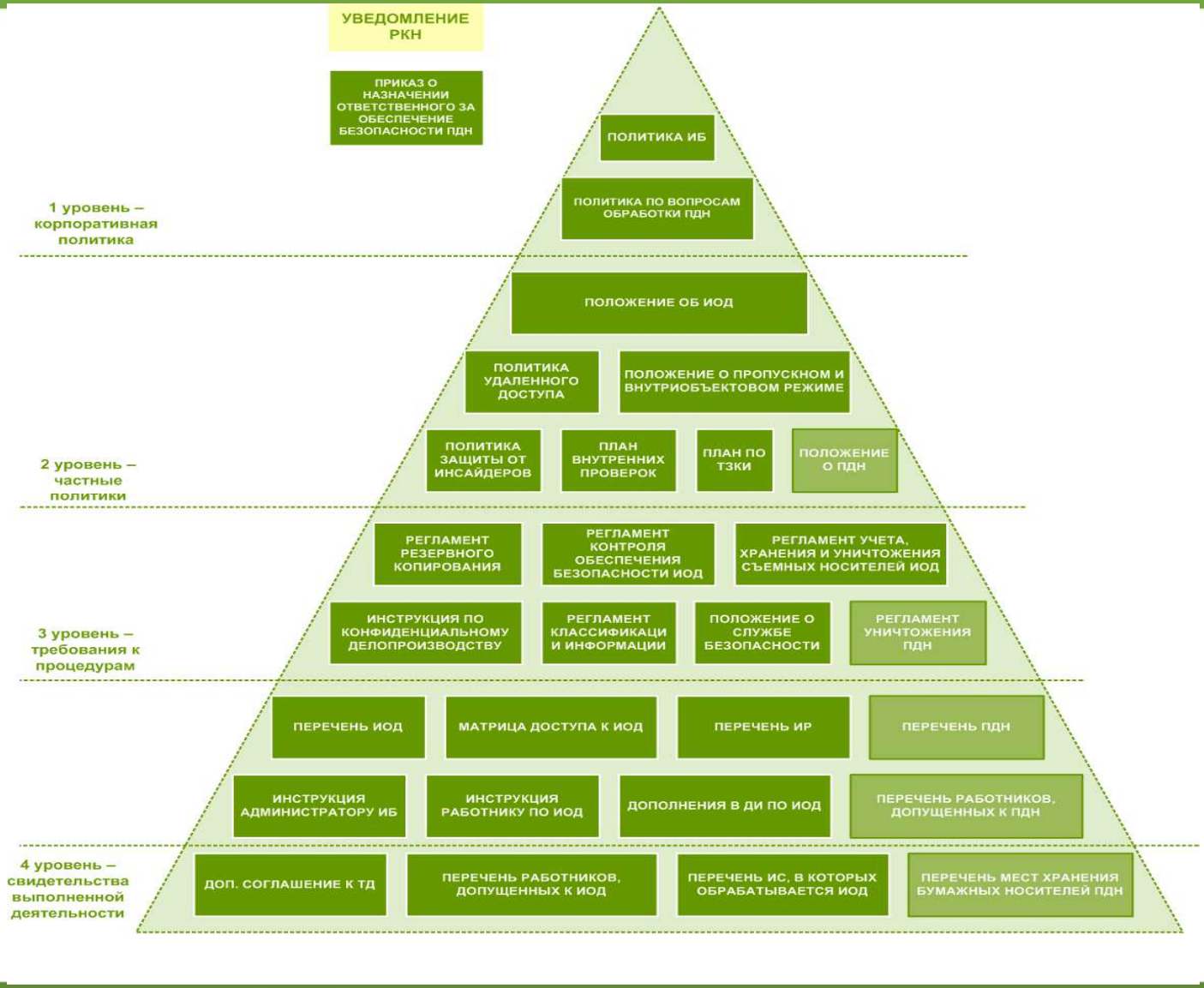
Детализированные положения Политики информационной безопасности, применительно к отдельным областям

Описание содержания, последовательности действий и ответственности должностных лиц применительно к отдельным процедурам

Свидетельства выполненной деятельности

ДиалогНаука

Структура документов по ИОД (включая ПДн)



ДиалогНаука

Организационно-распорядительная документация

№	Название	Содержание
1.	Приказ «О создании рабочей группы по организации работ по обеспечению безопасности персональных данных в соответствие с требованиями Федерального Закона «О персональных данных»	Назначает рабочую группу по организации работ по обеспечению безопасности персональных данных, ее обязанности, полномочия, сроки.
		Приложение 1. Состав рабочей группы
		Приложение 2. План мероприятий по защите персональных данных
2.	Приказ «Об утверждении частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных и выборе уровня защищенности ПДн»	Утверждает и вводит в действие «Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных и модель нарушителя безопасности».
		Приложение 1. «Частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
		Приложение 2. «Модель нарушителя».
3.	Приказ «О введении в действие перечня обрабатываемых персональных данных, перечня информационных систем персональных данных и перечня подразделений и сотрудников, допущенных к работе с персональными данными».	Утверждает и вводит в действие Перечень обрабатываемых персональных данных, Перечень информационных систем персональных, Перечень подразделений и должностей, допущенных к работе с персональными данными
		Приложение 1. Перечень обрабатываемых персональных данных.
		Приложение 2. Перечень информационных систем персональных.
		Приложение 3. Перечень подразделений и должностных лиц, допущенных к работе с персональными данными.

ДиалогНаука

Организационно-распорядительная документация

№	Название	Содержание
4.	Приказ «Об организации работ по обеспечению безопасности персональных данных»	Утверждает ответственных лиц за обработку и защиту персональных данных и вводит в действие внутренние документы по организации работ и обеспечению безопасности персональных данных.
		Приложение 1. Положение об обработке персональных данных.
		Приложение 2. Положение об организации и обеспечении защиты персональных данных.
		Приложение 3. Положение о подразделении, осуществляющем функции по организации и обеспечению защиты персональных данных
		Приложение 4. Типовая форма дополнительного соглашения по изменению трудового договора с сотрудниками.
		Приложение 5. Дополнения в должностные инструкции лиц участвующих в обработке персональных данных.
		Приложение 6. Инструкция работнику по обеспечению безопасности при работе с персональными данными
		Приложение 7. Инструкция администраторам безопасности информационных систем персональных данных.
		Приложение 8. Инструкция по действиям в случае компрометации ключевой информации.
		Приложение 9. План внутренних проверок состояния защиты персональных данных.
		Приложение 10. Перечень мест хранения материальных носителей персональных данных, обрабатываемых без использования средств автоматизации.
5.	Форма Политики в отношении обработки и защиты персональных данных	Содержит описание политики Оператора в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных

ДиалОгНаука

Техническое задание

Техническое задание на создание системы защиты персональных данных должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- предполагаемые к использованию СЗИ;
- этапность и сроки реализации системы защиты

ДиалОгНаука

Проектирование системы защиты персональных данных

- Макетирование и стендовые испытания средств защиты информации

- Разработка технического проекта на создание системы защиты персональных данных, включая:
  - Пояснительную записку с описанием программно-технических решений по защите персональных данных
  - Ведомость покупных изделий

ДиалОгНаука

Ввод в действие системы защиты персональных данных

- установка пакета прикладных программ в комплексе с программными средствами защиты информации;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации

ДиалОгНаука

Оценка эффективности реализованных мер по защите

Возможные варианты оценки эффективности:

- Внутренняя оценка эффективности (декларирование)
- Аттестация информационной системы персональных данных

Порядок оценки эффективности:

- Разработка программы и методики
- Проведение испытаний в соответствии с программой и методикой
- Оформление материалов испытаний
- Утверждение акта (протокола, заключения) проведения оценки/выдача аттестата соответствия

ДиалОгНаука

Аттестация ИСПДн

- Для специальных и биометрических ПДн, а также когда обрабатывается более 100 000 ПДн – рекомендуем проведение аттестации по требованиям безопасности информации

Преимущества аттестации:

- Делегирование рисков несоответствия действующему законодательства органу по аттестации, выдавшему аттестат соответствия
- Упрощение процедуры проверки со стороны регуляторов

ДиалОгНаука

Как устранить недостатки аттестации (внутренней оценки)?

- Четко обозначить: границы системы, требования к системе, критерии соответствия. Оформить это в виде Программы и методики испытаний
- Разработать корректные документы на ИСПДн: технический паспорт, матрицу доступа, описание технологических процессов обработки и защиты ПДн. В документах должны быть отражены характеристики, ВЛИЯЮЩИЕ на защищенность ПДн.
- Разработать и согласовать регламент внесения изменений в ИСПДн. Уведомление органа по аттестации обязательно только при изменении характеристик, влияющих на защищенность, и в результате которых ИСПДн не будет соответствовать требованиям
- Зафиксировать в материалах испытаний полученные свидетельства о соответствии с целью повторения аттестационных испытаний и оперативной оценки соответствия при внесении изменений

ДиалогНаука

Реализация системы защиты

Подсистема	Меры защиты в соответствии с проектом ФСТЭК России
Управления доступом	Обеспечение доверенной загрузки, идентификация и аутентификация, управление доступом субъектов к объектам
Регистрации и учета	Регистрация событий безопасности
Обеспечения целостности	Ограничение программной среды
Антивирусной защиты	Обеспечение целостности ИС и информации
Межсетевого экранирования	Защита ИС, ее средств и систем связи и передачи данных
Анализа защищенности	Обеспечение целостности ИС и информации
Обнаружения вторжений	Обеспечение целостности ИС и информации
Криптографической защиты информации	Защита ИС, ее средств и систем связи и передачи данных
	Защита среды виртуализации

ДиалОгНаука

Состав предлагаемых средств защиты

Подсистема	Специальные, биометрические ПДн	Общедоступные, иные
Подсистема управления доступом	Панцирь-К, SecretNet, Aladdin eToken	Пакет сертификации для ОС Microsoft, сертифицированные прикладные системы
Подсистема регистрации и учета	Панцирь-К, SecretNet	Пакет сертификации для ОС Microsoft, сертифицированные прикладные системы
Подсистема обеспечения целостности	Панцирь-К, SecretNet	Пакет сертификации для ОС Microsoft
Подсистема антивирусной защиты	Dr.Web, Антивирус Касперского, NOD 32, Symantec Endpoint Protection, TrendMicro	
Подсистема межсетевого экранирования	Континент, VipNet, С-Терра СиЭсПи, StoneGate	МЭ ISA, Check Point, Cisco

ДиалогНаука

Состав предлагаемых средств защиты

Подсистема	Специальные, биометрические ПДн	Общедоступные, иные
Подсистема анализа защищенности	MaxPatrol, Xspider, Ревизор Сети	MaxPatrol, Xspider, Ревизор Сети
Подсистема обнаружения вторжений	Proventia Network IPS, StoneGate IPS	Proventia Network IPS, StoneGate IPS, Cisco IPS, Check Point IPS
Подсистема криптографической защиты информации	КриптоПро CSP (в составе С-Терра, StoneGate, Континент), ViPNet CSP, Secret Disc	КриптоПро CSP (в составе С-Терра, StoneGate, Континент), ViPNet CSP, Secret Disc
Защита среды виртуализации	VMware (пакет сертификации), vGate (для VMware), TrendMicro Deep Security	

ДиалОгНаука

ТЕХНИЧЕСКОЕ И КОНСУЛЬТАЦИОННОЕ СОПРОВОЖДЕНИЕ

№ п/п	Работы	Разрабатываемые документы
1.	Актуализация состава и содержания ОРД по вопросам обработки и защиты ПДн	▪ Справка с обоснованием необходимости корректировки ОРД. ▪ Проекты доработанных ОРД
2.	Контроль соблюдения требований законодательства и оценка рисков несоблюдения законодательства	▪ Актуальный реестр требований законодательства. ▪ Актуальный реестр рисков невыполнения законодательства. ▪ Актуальный план контрольных мероприятий. ▪ Отчет о контрольных мероприятиях. ▪ Предложения по снижению рисков невыполнения законодательства
3.	Информационное сопровождение	▪ Справка об изменении законодательства с комментариями ▪ Ответы с разъяснениями законодательства в случае поступления запросов
4.	Проведение тренингов работников и аудитов выполнения требований по обработке и обеспечению безопасности ПДн	▪ Презентации для проведения тренингов. ▪ Методики аудита. ▪ Протоколы и свидетельства проведенных аудитов
5.	Сопровождение при проверках процессов обработки ПДн контролирующими организациями	▪ Проекты ответов на запросы контролирующих органов

ДиалОгНаука

Часть 3

Текущая ситуация нормативного регулирования и проверок

Изменения в наказаниях

Новая (2-я!!!) редакция изменений в КоАП.

http://www.rsoc.ru/docstore/doc1353.htm

«Статья 13.11. Невыполнение оператором обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных

Невыполнение оператором обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных, -

влечет наложение административного штрафа на граждан в размере от пятисот рублей до двух тысяч рублей; на должностных лиц – от четырех тысяч до пяти тысяч рублей; на индивидуальных предпринимателей – от пяти тысяч до семи тысяч рублей; на юридических лиц – от **двадцати тысяч до тридцати тысяч** рублей.».

ДиалОгНаука

Изменения в наказаниях

- «Статья 13.11.1. Обработка персональных данных без согласия субъекта (субъектов) персональных данных

Обработка персональных данных **без согласия** субъекта (субъектов) персональных данных в случаях, когда такое согласие обязательно, а равно обработка персональных данных **с нарушением** установленной законом **формы согласия** субъекта (субъектов) персональных данных -

влечет наложение административного штрафа на граждан от одной тысячи до двух тысяч рублей; на должностных лиц – от пяти тысяч до семи тысяч рублей; на индивидуальных предпринимателей – от пятнадцати до двадцати тысяч рублей; на юридических лиц – от **тридцати тысяч до пятидесяти тысяч** рублей.

ДиалОгНаука

Изменения в наказаниях

Обработка персональных данных **без согласия** субъекта (субъектов) персональных данных в случаях, когда такое согласие обязательно, а равно обработка персональных данных **с нарушением установленной законом формы согласия** субъекта (субъектов) персональных данных, если такая обработка повлекла **причинение вреда жизни и (или) здоровью** гражданина, -

- влечет наложение административного штрафа на граждан – от четырех тысяч до пяти тысяч рублей; на должностных лиц – от десяти тысяч до пятнадцати тысяч рублей; на индивидуальных предпринимателей – в размере **1,5 % совокупного дохода за** прошедший отчетный **год**, но не менее **трехсот тысяч** рублей; на юридических лиц – в размере **1,5 % совокупного дохода за прошедший отчетный год, но не менее пятисот тысяч** рублей.

ДиалОгНаука

Изменения в наказаниях

Обработка персональных данных **без согласия** субъекта (субъектов) персональных данных в случаях, когда такое согласие обязательно, а равно обработка персональных данных с нарушением установленной законом формы согласия субъекта (субъектов) персональных данных, **с целью извлечения дохода**, -

- влечет наложение административного штрафа на граждан – пять тысяч рублей; на должностных лиц – от пятнадцати до двадцати тысяч рублей; на индивидуальных предпринимателей – в размере 2 % совокупного дохода за прошедший отчетный год, но не менее четырехсот тысяч рублей; на юридических лиц – в размере **2 % совокупного дохода за прошедший отчетный год, но не менее шестисот тысяч** рублей.

ДиалОгНаука

Изменения в наказаниях

Обработка персональных данных **без согласия** субъекта (субъектов) персональных данных в случаях, когда такое согласие обязательно, а равно обработка персональных данных с нарушением установленной законом формы согласия субъекта (субъектов) персональных данных лицом, **ранее подвергнутым административному наказанию** за аналогичное административное правонарушение, -

- влечет наложение административного штрафа на граждан – пять тысяч рублей; на должностных лиц – от тридцати тысяч до сорока тысяч рублей; на индивидуальных предпринимателей – в размере 2 % совокупного дохода за прошедший отчетный год, но не менее пятисот тысяч рублей; на юридических лиц – в размере **2 % совокупного дохода за прошедший отчетный год, но не менее семисот тысяч** рублей.».

ДиалОгНаука

Изменения в наказаниях

«Статья 13.11.2. Незаконная обработка специальных категорий персональных данных

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также персональных данных о судимости в случаях, не предусмотренных законом,

– в размере 1,5 % совокупного дохода за прошедший отчетный год, но не менее четырехсот тысяч рублей **(просто обработка).**

– в размере 2 % совокупного дохода за прошедший отчетный год, но не менее пятисот тысяч рублей **(причинение ущерба)**.

– в размере 2 % совокупного дохода за прошедший отчетный год, но не менее семисот тысяч рублей **(повторное)**.

ДиалОгНаука

Изменения в наказаниях

«Статья 13.11.3. Несоблюдение условий трансграничной передачи персональных данных

1. Несоблюдение условий трансграничной передачи персональных данных, -

– от двадцати тысяч до тридцати тысяч рублей.

2. Несоблюдение условий трансграничной передачи персональных данных, повлекшие неправомерный или случайный доступ к ним, уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия в отношении персональных данных, -

– в размере 1,5 % совокупного дохода за прошедший отчетный год, но не менее пятисот тысяч рублей.

3. – в размере 2 % совокупного дохода за прошедший отчетный год, но не менее 700 тысяч рублей.» (**повторное**).

ДиалОгНаука

Разъяснения регуляторов на публичных мероприятиях

- Обработчики – такие же операторы (Роскомнадзор)
- Для передачи ПДн сторонним организациям (СК, НПФ и пр.) согласие необходимо. Если компании меняются, необходимо сотрудника уведомить
- Законными правами и интересами Оператора являются права и интересы, прописанные в федеральном законодательстве
- Необходимо получать согласия родственников при их передаче в сторонние организации (например, для заключения договоров ДМС)

Разъяснения по поводу проверок

- ФСБ проверяет только государственные ИС, в которых используются СКЗИ (остальные – по указанию Правительства)
- 2011, 2012– проверки осуществляет Роскомнадзор (частично совместно с ФСТЭК России)
- Проверки в соответствии с регламентами, утвержденными регуляторами
- Цель проверок – выполнение ПП 781 и 687
- В части СКЗИ – проверки использования СКЗИ, режимов доступа в помещения СКЗИ, работу с ключевыми носителями

ДиалОгНаука

Типовые замечания по проверкам

- Уведомление не отправлено или не соответствует действительности
- До сотрудников не доведены под роспись локальные правовые акты, перечни и т.д. (низкий уровень знаний работников в целом)
- СКЗИ: несоответствие класса СКЗИ и модели нарушителя, истечение сроков сертификатов, отличие версий СКЗИ

ДиалогНаука

Выводы: что делать?

ДиалОгНаука

Что делать

- Откладывать выполнение требований законодательства уже нельзя
- Первоочередная задача – привести процессы обработки ПДн в соответствие законодательству (сбор согласий, учет, доведение до работников и т.д.)
- Если корректно написать ОРД, привести процессы в соответствие, то изменение законодательства не потребует серьезных корректировок процессов
- Законодательство меняется – требования остаются неизменными (и набор СЗИ также)
- Необходимо стараться объективно оценивать ущерб от нарушения безопасности ПДн и выбирать меры защиты в соответствии с данным ущербом

ДиалогНаука

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: pdn@DialogNauka.ru