CLOUD4Y

#1 КОРПОРАТИВНЫЙ ОБЛАЧНЫЙ ПРОВАЙДЕР

Об обработке персональных данных «с чистого листа»

WHITE PAPER

Оглавление

Введение

Данный документ является руководством, описывающим действия организаций, которые необходимо предпринять ответственным лицам для соответствия законодательству, регулирующему отношения, связанные с обработкой персональных данных.

При подготовке были использованы факты и логические заключения, сделанные на основе действующих нормативных правовых актов Российской Федерации, формирующих «границы» правового поля, в которых необходимо находится при совершении любых операций со сведениями о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющих прямо или косвенно идентифицировать его личность.

Каждый из нас одновременно является субъектом персональных данных и оператором, самостоятельно или совместно с другими лицами осуществляющим обработку персональных данных. По этой причине, хотя этот документ в формате *white paper* имеет бизнес-направленность, он будет полезен и актуален также государственным органам, органам местного самоуправления, муниципальным органам и физическим лицам.

Действие *Федерального Закона № 152-ФЗ «О персональных данных»*, регулирующего деятельность по обработке (использованию) персональных данных *(далее ПДн)* 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.

Однако, знание этого закона может помочь каждому избежать подобного нарушения чужих прав и обеспечить защиту своих прав и свобод человека и гражданина при обработке ПДн, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Именно защита прав субъектов ПДн – является основной целью закона *152-ФЗ* и функцией уполномоченного органа, которым является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи и массовых коммуникаций (Роскомнадзор)[1].

[1] В соответствии с п. 1 ст. 23 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» и п.1 Положения о Федеральной службе по надзору в сфере связи и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16.03.2009 года № 228

Возможно, если ранее вы не были хорошо знакомы с законодательством, регулирующим отношения, связанные с обработкой персональных данных, то после прочтения первых нескольких абзацев, у вас уже появились вопросы.

Одна из главных целей этой книги – устранить путаницу и обеспечить понимание законодательства в области персональных данных, ясно описать процесс приведения информационной системы персональных данных в соответствие с требованиями закона.

Надеюсь, что эта книга приблизит вас к достижению этих целей и поможет минимизировать риски возможных штрафов со стороны регулирующих органов и избежать других негативных последствий, связанных с нарушением прав субъектов персональных данных.

Эта книга будет интересна как читателям, начинающим изучение этого вопроса «с чистого листа», так и имеющим базовые знания.

Особенно актуальна она для:

- менеджмента организаций - для всех, кто принимает решения;
- руководителей и сотрудников IT-служб - для всех, кто строит и поддерживает работу IT-инфраструктуры;
- специалистов кадровой службы - для тех, кто не может не работать с личными данными сотрудников;
- новичков в профессии и тех, кто только готовится посвятить себя карьере в области защиты информации.

Глава 1. Краткая история вопроса

В далёком 1981 году Совет Европы опубликовал конвенцию о защите личности при обращении с персональными данными. Цель Конвенции – «гарантировать на территории каждой страны каждому частному лицу, независимо от его национальности и места проживания, соблюдение его прав и основных свобод, и особенно его права на личную жизнь в аспекте автоматизированной обработки данных личного характера (статья 1).

Согласно части 1 статьи 3 «Стороны обязуются применять настоящую Конвенцию в отношении автоматизированных картотек и для автоматизированной обработки данных личного характера в общественном и частном секторах».

Стоит отметить, что мнение Совета Европы о персональных данных не являлось и не является единственным в мире. На примере Китая и США можно видеть несколько иной подход.

Для СССР в то время вопрос обработки с помощью средств автоматизации не был актуален по причине слабого проникновения компьютерных технологий в экономику. Позднее по причинам экономических проблем сфера защиты конфиденциальной информации в России имела значительное отставание в развитие законодательной базы и осведомленности населения.

Как необходимый шаг для вступления в ВТО, Россия подписала Конвенцию в ноябре 2001 года. Таким образом только спустя 20 лет со дня публикации Конвенции в России началось движение в сторону создания правовых основ обработки персональных данных. Конвенция была принята формально, но по факту не действовала из-за отсутствия российских нормативных актов.

Вновь законодатели вернулись к этому вопросу в 2005 году, когда был принят Федеральный закон от 19 декабря 2005 года №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

Знаковым стал 2006 год, когда в целях наведения порядка в сфере интеллектуальной собственности и защиты персональных данных, в том числе как выполнение одного из условий вступления России в ВТО, были приняты два Федеральных закона.

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

Авторы научно-практического комментария[2] к Федеральному закону «О персональных данных» высказывают следующее мнение о целях принятия 152-ФЗ:

«В целях защиты прав граждан в области персональных данных Российская Федерация с учетом трансграничности потоков персональных данных в первую очередь обеспечила имплементацию в российское законодательство требований общеевропейского права, создала систему защиты прав субъектов персональных данных, соответствующую основным принципам, заложенным в межгосударственных нормативных правовых актах в области персональных данных.»

В Законе были перечислены общие положения, принципы и условия обработки персональных данных, права субъекта персональных данных, обязанности оператора и ответственность за нарушение требований.

Многие эксперты считают, что закон «О персональных данных» (далее Закон) является слишком общим, требует доработки с упором на международную практику и чёткой сегментации.

Так, Статья 3. «Основные понятия, используемые в настоящем Федеральном законе» позволяет усомниться в формальной определенности этих понятий. Само слово «понятие» использовано вместо слов «термин» или «определение», которые зачастую можно встретить в формулировках других законов. 152-ФЗ не даёт однозначного понимания при толковании. В дальнейшем мы попытаемся устранить эту неоднозначность в меру возможностей активного участника IT-отрасли, не претендуя «на истину в последней инстанции».

Впрочем, наиболее серьёзные проблемы были связаны с выполнением требований подзаконных актов, которые подготовили регуляторы в области защиты персональных данных. Подробнее об этом мы расскажем в следующих главах.

[2] Под редакцией заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой

Государственные Регуляторы в области защиты персональных данных

Ответственными ведомствами за соблюдение Закона являются

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - контроль и надзор за соответствием обработки ПДн требованиям законодательства.
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) устанавливает методы и способы защиты информации в информационных системах некриптографическими методами.
- Федеральная служба безопасности (ФСБ России) устанавливает методы и способы защиты информации в информационных системах криптографическими методами.



Существует разделение ответственности и полномочий между ведомствами. Роскомнадзор не проверяет наличие и состояние технической защиты информационных систем персональных данных. Регуляторами в части технических мер защиты являются ФСТЭК и ФСБ, при этом ФСБ - только при использовании криптографии.

Главная задача Роскомнадзора — проверка правовых оснований обработки персональных данных. Вопреки расхожему мнению, положения, инструкции, приказы и прочие документы не являются самым главным объектом проверок. Конечно, локальные документы организации также будут проверены, но Уполномоченный орган больше интересуют сами персональные данные и соответствие объема и состава этих данных целям обработки.

Что же такое персональные данные и их обработка?

В соответствии с Законом, персональные данные – **любая информация**, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Данное определение практически идентично определению, установленному пп. «а» ст. 2 Конвенции 1981 года, согласно которому персональные данные означают **любую**

информацию об определенном или поддающемся определению физическом лице («субъекте данных»).

Таким образом, Закон даёт чёткое понимание того, что субъектами ПДн являются только физические лица.

В то же время при буквальном толковании Закона к понятию **«персональные данные»** можно отнести широкий круг информации, в том числе выходящий за рамки разумно ожидаемого в данном контексте. В частности, в нем нет указания на связь между информацией и прямой или косвенной определенностью или «определяемостью» физического лица. Соответственно, отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких – нет[3].

В целом члены рабочей группы по определению матрицы персональных данных[4] в рамках Консультативного совета при Роскомнадзоре согласны в том, что, **если совокупность данных необходима и достаточна для идентификации лица**, такие данные следует **считать персональными данными этого субъекта**, даже если они не включают в себя данные документов, удостоверяющих личность. При этом данные нельзя считать персональными в том случае, если без использования дополнительной информации они не позволяют идентифицировать физическое лицо. Изложенный подход допустимо рассматривать как учитывающий баланс интересов всех участников отношений.

С точки зрения правоприменительной практики, предпринимать какие-либо попытки доказать, что информация не является персональными данными, так как не строго однозначно указывает на конкретного человека и в отношении этих данных остается некоторый аспект вероятного совпадения с другим человеком, мы не рекомендуем, так как вероятность такого совпадения должна быть достаточно велика и очевидна.

Перечень совокупностей или наборов сведений о субъекте, который позволял бы говорить с уверенностью, что это персональные данные законодательно никак не закреплён. Из этого следует, что любая совокупность данных, прямо или косвенно с достаточной вероятностью указавшая на физическое лицо, может быть признана его персональными данными.

---

[3] Федеральный закон «О персональных данных»: научно-практический комментарий под редакцией заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой

[4] Материалы, используемые в комментарии к настоящей статье, предоставили члены рабочей группы под председательством В.В. Архипова (А.Э. Адилова, Е.А. Войниканис, А.Г. Бодров, М.С. Овешников, К.Т. Сумманен).

Например, для идентификации достаточно дополнения сведений о фамилии, имени и отчестве любой иной персональной информацией: датой рождения, адресом, номером телефона, местом работы и многим другим, например, адресом электронной почты.

Ответ на вопрос о достаточной вероятности совпадения с другими лицами при идентификации по определенному набору данных также не имеет чёткого числового критерия. Так при обработке Ф.И.О + страна проживания, набор не является персональными данными, но набор Ф.И.О + название населённого пункта с менее чем 1000 жителями, уже может быть достаточным для идентификации конкретного физического лица, а значит являться ПДн.

Таким образом, вопрос «Обрабатываются ли персональные данные в вашей организации?» для регуляторов не стоит. **Да, персональные данные в вашей организации есть**, хотя бы по причине того, что вы обрабатываете персональные данные сотрудников.

С точки зрения Закона, 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.

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.

Если в вашей организации накапливаются, просто хранятся или каким-то образом используются в работе персональные данные, хотите вы этого или нет, с точки зрения закона **вы признаетесь оператором персональных данных** и **обязаны соблюдать требования законодательства** при обработке любых персональных данных, позволяющих идентифицировать лицо, которому принадлежат эти данные.

С правовой точки зрения персональные данные разделены на 4 категории, для которых различны требования к организации обработки и обеспечению безопасности:

- **специальные категории** персональных данных (с самыми строгими требованиями к защите прав их субъектов) - персональные данные, касающиеся
    - расовой,
    - национальной принадлежности,
    - политических взглядов,

- религиозных или философских убеждений,
- состояния здоровья,
- интимной жизни субъектов персональных данных.

- биометрические персональные данные сведения, которые
  - характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые
  - используются оператором [5] для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных (если особые биометрические методы идентификации личности не используются - это не биометрические ПДн).
- общедоступные персональные данные - персональные данные субъектов персональных данных, полученные только из общедоступных источников [6] персональных данных
- иные категории персональных данных - персональные данные, не отнесенные Законом к специальной категории, биометрическим и общедоступным.

Важными вопросами при этом являются «что» и «как» необходимо сделать, чтобы защитить персональные данные, обрабатываемые в вашей организации, в соответствии с законом. Требования для физических лиц самые мягкие, для муниципальных и государственных органов — самые строгие. Для бизнеса строгость требований во многом зависит от того, какие категории ПДн и в каком объёме обрабатываются в организации.

Именно об этом в следующих главах, но прежде нам необходимо познакомиться со структурой и иерархией соответствующих нормативных правовых актов.

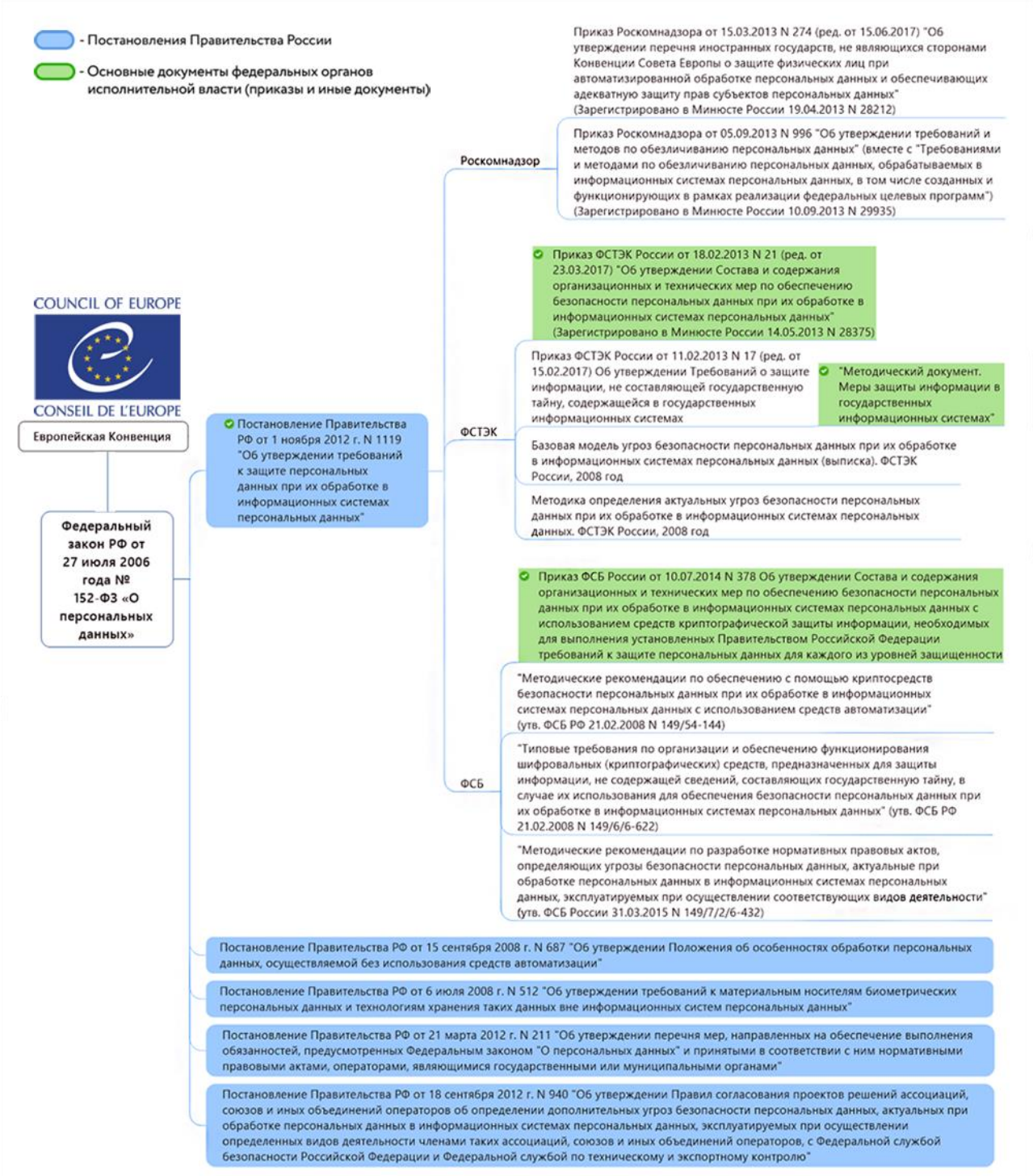
[5] Таким образом, законодательное понятие биометрических данных предполагает не только наличие определенных сведений, содержащих информацию о физиологических и биологических особенностях человека, но также обязательно использование особых биометрических методов идентификации личности для подтверждения личности по физиологическим параметрам.

[6] В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Глава 2. Структура законодательства России в области защиты прав субъектов ПДн

Схема ниже описывает структуру и иерархию актуального на момент публикации книги законодательства России, обеспечивающего защиту прав субъектов персональных данных.

Данная схема может быть дополнена уровнем локальных нормативных правовых актов, которые должны быть разработаны в вашей организации.



Далее мы попытаемся описать значение и место каждого документа в процессе «правильной» с точки зрения регуляторов обработки персональных данных.

Для начала вернёмся к основному в этой области закону «О персональных данных». Он задаёт некоторую структуру и основы правовой системы в вопросах обработки персональных данных, объединяя разные элементы права.

Кроме ранее описанных особенностей 152-ФЗ, стоит обратить внимание ещё на ряд закреплённых им правовых норм.

Статья 5. Принципы обработки персональных данных

…

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

…

Действующее законодательство не содержит критериев избыточности обрабатываемых персональных данных. Однако, если продавец одежды будет собирать и хранить сведения об именах, возрасте и поле детей покупателя, с точки зрения закона, такие данные будут избыточными, несмотря на «благое» желание продавца предоставить скидку на подарок ребёнку в его день рождения. По той же причине нельзя требовать у соискателя на вакантную должность размер одежды (имело место быть нарушение в одной организации, где работа связана с ношением униформы). Эти данные мы можем требовать, уже нанимая человека на работу, но для того, чтобы рассмотреть его как кандидата – они излишни.

Далее, Статья 6. Условия обработки персональных данных

Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

…

5) 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;

…

Из приведенной выше выписки Закона следует, что физическое лицо (например, клиент), персональные данные которого обрабатываются, должен быть уведомлен о целях обработки, и это должно быть отражено в форме его письменного согласия.

Получается также, что обработка может осуществляться и без согласия физического лица, а в каких именно случаях описано в пунктах со 2 по 11. При этом с согласия физического лица можно обрабатывать его ПДн и в других неописанных в законе целях, которые при этом должны быть обозначены в письменном согласии субъекта ПДн.

На практике встречаются случаи, когда оператор, ссылаясь на 5 пункт этой статьи комментируемого закона, заключая договор с физическим лицом, использует данные физического лица (номер телефона) для рекламной рассылки в целях продвижения товаров без получения согласия физического лица.

Однако, исходя из положений этой статьи Закона, получение согласия субъекта на обработку персональных данных не требуется, если это непосредственно связано с исполнением и (или) заключением договора. Последующее использование персональных данных в маркетинговых целях никак не связано с исполнением договора, стороной или выгодоприобретателем которого является физическое лицо. Таким образом, оператору персональных данных требуется получение согласия на использование данных в целях продвижения своих товаров. При нарушении указанного требования оператор персональных данных подлежит привлечению к ответственности на основании ст. 13.11 КоАП РФ.

Законодатель ограничил возможность обработки персональных данных в целях продвижения товаров, работ, услуг на рынке путем прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации, установив, что обработка информации в таких целях допускается только при условии предварительного согласия субъекта.

На практике же случаи запрашивания предварительного согласия субъекта персональных данных на рассылку рекламной или иной подобной корреспонденции крайне редки[7].

Об изменениях, внесенных 242-ФЗ

21 июля 2014 года вступил в силу Федеральный закон №242 от «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

242-м законом были внесены, в том числе, и изменения по интересующим нас вопросам.

ФЗ №242 в статье 1 дополнил Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации» новой статьёй 15.5 «Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных».

В соответствии с частью 1 статьи 1 была создана автоматизированная информационная система «Реестр нарушителей прав субъектов персональных данных», целью которой является ограничение доступа к информации в «Интернет», обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных. Основанием для внесения в "Реестр нарушителей" доменного имени, URL-адреса интернет-страницы, законодателем установлено вступившее в законную силу решение суда о признании деятельности по распространению информации, содержащей персональные данные, нарушающей требования ФЗ №152, а также права субъекта персональных данных на неприкосновенность частной жизни, личную и семейную тайну.

Второй же статьей вносятся изменения в две статьи (ст. 18, 22) главы 4 «Обязанности оператора» и одну статью (ст. 23) главы 5 «Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего федерального закона» (ФЗ № 152).

Частью 1 второй статьи внесены изменения в статью 18 «Обязанности оператора при сборе персональных данных» ФЗ № 152, согласно которым для оператора устанавливается **обязанность осуществлять при сборе персональных данных определенные виды обработки персональных данных в базах данных, которые находятся на территории России.**

[7] Федеральный закон «О персональных данных»: научно-практический комментарий под редакцией заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой

Определенные виды обработки это: запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Таким образом с 1 сентября 2015 года действует положение о локализации хранения и отдельных процессов обработки персональных данных граждан России на территории нашей страны и фактически любые действия с ПДн, оператор обязан осуществлять с использованием баз данных, находящихся на территории Российской Федерации.

Закон, с определенными оговорками[8], допускает трансграничную передачу[9]. Но, главное при этом помнить, что **результаты этой обработки должны сначала попасть в базу на нашей территории**, которая всегда должна быть "полнее".

О неавтоматизированной обработке и применении средств вычислительной техники

152-ФЗ регулирует отношения, связанные как с автоматизированной обработкой персональных данных, так и обработку без использования средств автоматизации.

Согласно Закону, **автоматизированная обработка** персональных данных - обработка ПДн **с помощью средств вычислительной техники**.

Впервые закон был принят в 2006 году, а это определение появилось позднее в 2011 году, когда в 152-ФЗ были внесены соответствующие изменения.

Особенности неавтоматизированной обработки ПДн были определены в 2008 году в Постановлении Правительства РФ N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", при этом позже никаких изменений в документ не вносилось. В ПП N 687 для неавтоматизированной обработки даётся следующее определение:

---

[8] См. ФЗ «О персональных данных» статья 12. Трансграничная передача персональных данных и Приказ Роскомнадзора от 15.03.2013 N 274 (ред. от 15.06.2017) "Об утверждении перечня 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"

[9] Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Сложилась ситуация, когда постановление Правительства РФ противоречит Федеральному закону. Причем эта ситуация актуальна и по сей день (правки в постановление так и не внесли). Роскомнадзор в своих разъяснениях напоминает о верховенстве Федерального закона над всеми его подзаконными актами (в данном случае, 152-ФЗ главнее Постановления Правительства). Следовательно, о противоречивых определениях неавтоматизированной обработки персональных данных в ПП-687 можно забыть. А выводы сделать следующие:

- Если вы обрабатываете всю информацию, позволяющую идентифицировать хотя бы одного человека или более, только в бумажном виде, например, у вас хранятся личные дела сотрудников в отделе кадров, то вы осуществляете обработку персональных данных в своей специфической информационной системе персональных данных (далее ИСПДн) без использования средств автоматизации. Такая ИСПДн позволяет осуществлять в соответствии с заданным алгоритмом поиск и доступ к персональным данным, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных. Поэтому вам необходимо при работе с ПДн соблюдать ФЗ-152, а что именно необходимо сделать для обеспечения безопасности данных в вашей специфической ИСПДн описано в ПП РФ N 687. Краткое содержание документа мы приводим здесь:

    I. Общие положения
    II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации
    III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Меры, которые необходимо предпринять оператору при неавтоматизированной обработке, описаны последними тремя пунктами достаточно полно. В рамках данной книги мы больше не будем возвращаться к особенностям неавтоматизированной обработки. Если это именно ваш случай, то продолжить чтение мы рекомендуем вам только в том случае, если вы начнёте использовать в своём бизнесе средства вычислительной техники при работе с ПДн[10].

ПП 1119, Приказ ФСТЭК №21 и "Методический документ"

Однако, на сегодняшний день ситуация, при которой организация осуществляет обработку персональных данных только в «бумажном» виде становится всё менее вероятной.

Использование при работе с информацией, содержащей ПДн, средств вычислительной техники (компьютеров, локальных и облачных серверов, сетей передачи данных) гораздо более частое явление в современной экономике. Обработка в таких ИСПДн будет считаться автоматизированной, несмотря на участие в этом процессе человека.

[10] Также, возможно, вам будет полезно ознакомиться с главой посвященной процессу организации обработки ПДН в организации в части разработки локальных документов организации, а также с главой об ответственности оператора.

При этом, если наряду с обработкой на компьютерах используются бумажные носители, обработка будет считаться смешанной. Это не отменяет потребности обеспечивать безопасность персональных данных и соблюдать требования закона как к автоматизированной обработке, так и к обработке без использования средств автоматизации.

Основным документом для операторов с любой формой собственности, осуществляющих автоматизированную или смешанную обработку персональных данных является Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

В части 3 статьи 19 152-ФЗ сказано, что Правительство РФ устанавливает уровни защищенности персональных данных при их обработке в информационных системах персональных данных (далее — ИСПДн) и требования к защите персональных данных в ИСПДн. Таким образом, у нас появилось Постановление Правительства №1119 от 01.11.2012, определяющее эти требования.

Именно в ПП-1119 описаны правила определения уровня защищённости (далее УЗ) персональных данных в ИСПДн и требования, выполнение которых необходимо выполнить.

Данное постановление отменило Постановление Правительства №781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", а значит руководящие документы, которые разработаны во исполнение постановления №781 теряют силу. Такими документами являются:

- Приказ ФСТЭК России №55, ФСБ России №86, Мининформсвязи Российской Федерации №20 от 13.02.2008 «Об утверждении Порядка классификации информационных систем персональных данных» (больше известен как приказ трёх *№ 55/86/20*).
- Приказ ФСТЭК России от 05.02.2010 №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

В своё время наиболее серьёзные проблемы возникли у операторов именно с исполнением требований этих подзаконных актов. Наиболее сложными из них оказались обязательная сертификация средств защиты для базы персональных данных и аттестация объектов.

Также сложно реализуемыми оказались требования по защите так называемых специальных типов персональных данных. Повышенная степень защиты для сведений о здоровье, политических и религиозных взглядах, а также сексуальной ориентации была прописана ещё в конвенции, поэтому ФСБ предложила использовать для защиты таких данных методы, разработанные ей для сохранения государственной тайны. Сам документ, описывающий требования к защите, был с грифом ДСП, якобы потому, что он давал представление и методах защиты государственной тайны. В частности, в этих требованиях указывалось, что нужно предусмотреть защиту от утечек по нетехническим каналам, таким как звуковая и визуальная информация, а также с помощью побочного электромагнитного излучения.

В результате, все медицинские учреждения и пенсионные фонды потребовалось защищать по этим завышенным требованиям с аттестацией помещения и проверкой на правильное расположение мониторов и телефонов, а также на наличие ПЭМИН.

В новой на 2011 год редакции закона "О персональных данных" появились совсем другие нормы, которые фактически закрепляли на законодательном уровне часть технических требований из подзаконных актов. Часть излишнего обременения была снята с операторов персональных данных. Выпуск ПП-1119 являлся прямым требованием пунктов 1 и 2 части 3 ст.19 новой редакции 152-ФЗ «О персональных данных» и фактически определил требования к системе построения безопасности обработки персональных данных в информационных системах по-новому.

Нет смысла руководствоваться в работе документами, утратившими силу, поэтому важно запомнить, что ПП 781, приказ трёх № 55/86/20 и Приказ ФСТЭК №58 утратили силу. Большое количество авторских статей в Интернете, которые ссылаются на требования этих актов более не актуальны с практической точки зрения.

Во исполнение Постановления №1119 Регуляторами были разработаны и утверждены необходимые для работы по защите персональных данных документы:

вместо Приказа №58 от 05.02.2010г., вступили в действие 2 Приказа ФСТЭК России

- Приказ №21 от 18.02.2013г. "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и
- Приказ №17 от 11.02.2013г. "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

Приказы определяют состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн. Документы являются ключевыми для обеспечения безопасности ПДн, что является одной из основных обязанностей оператора. Приказ №21 применяется юридическими лицами с частной формой собственности, а 17 приказ разработан для государственных органов и муниципалитетов.

Подведём промежуточный итог обзора законодательства в этой сфере.

Итак, 152-ФЗ определил обязанность каждого Оператора при обработке персональных данных 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.

Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает в ПП-1119:

- необходимый для вашей ИСПДн уровень защищенности персональных данных при их обработке в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных в ИСПДн, исполнение которых обеспечивает необходимый уровень защищенности;

Состав и содержание требований организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн устанавливает уполномоченный в области технической защиты информации ФСТЭК в Приказе №21.

Если же речь идёт о реализации требований для Государственных или Муниципальных Информационных Систем (далее ГИС/МИС) необходимо применять Приказ ФСТЭК №17.

Таким образом после прочтения этих нормативных правовых документов у каждого оператора может сложится относительно полное понимание того, что необходимо сделать, чтобы обрабатывать ПДн «правильно».

Однако для полноценной работы по защите персональных данных Операторам ПДн требовалась «инструкция» о том, как необходимо реализовывать перечень мер защиты персональных данных, утвержденных Приказом ФСТЭК №21. Регулятором такой документ в соответствии с требованиями Приказа №21 разработан и утвержден не был.

Выйти из этой ситуации можно, использовав **"Методический документ. Меры защиты информации в государственных информационных системах"** (утвержден ФСТЭК России 11 февраля 2014 г. и доступен на сайте Регулятора). Данный «Методический документ», как следует из названия, был разработан в целях детализации организационных и технических мер защиты информации, применяемые в государственных информационных системах в соответствии с Требованиями, утвержденными в 17-ом Приказе ФСТЭК.

Но, так как подобного документа для ИСПДн выпущено не было, в тексте этого Документа закреплено:

«По решению оператора персональных данных настоящий методический документ применяется для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, защита которых обеспечивается **в соответствии с** Составом и содержанием организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, утвержденных **приказом ФСТЭК России от 18 февраля 2013 г. № 21**».

При использовании этого Методического документа оператору необходимо учесть специфику ГИС. Основным отличием является определение уровня защищенности ПДн для ИСПДн вместо класса защищённости для ГИС/МИС. Сами по себе детализируемый состав и содержание мер по обеспечению безопасности ПДн соответствуют Приказу ФСТЭК №21 (например, *ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора* необходима как для обеспечения каждого из уровней защищенности персональных данных по Приказу №21, так и для всех классов защищенности ГИС).

Таким образом, используя ФЗ-152 *(для понимания основ)*, ПП-1119 *(для определения УЗ)*, Приказ ФСТЭК № 21 *(для выбора мер обеспечения безопасности)* и "Методический документ. Меры защиты информации в государственных информационных системах" *(для детализации содержания и правил реализации мер)* оператор ПДн может получить ответы на основные вопросы, связанные с обеспечением безопасности ПДн при автоматизированной обработке.

Федеральными органами исполнительной власти в пределах своих полномочий и в своей сфере деятельности приняты и другие нормативные правовые акты, которые должны быть применены с учётом специфики организации или носят рекомендательных характер.

Наиболее вероятные частные случаи при организации обработки и защиты ПДн могут быть связаны с передачей биометрических персональных данных[11], обезличиванием ПДн[12] и применением криптографических средств защиты.

Приказ ФСБ России N 378

Как уже было сказано ранее вопрос применения криптографических средств защиты регулирует ФСБ. По аналогии с Приказом ФСТЭК №21, **состав и содержания организационных и технических мер**[13] по обеспечению безопасности персональных данных при их обработке в ИСПДн **с использованием средств криптографической** защиты информации, необходимых для каждого из уровней защищенности, определен в **Приказе ФСБ России от 10.07.2014 N 378.**

Требования этого приказа понятны и выполнимы, однако, открытым остается вопрос **«когда необходимо применять средства криптографической защиты информации?»**. Ответ можно найти в документе "**Методические рекомендации по разработке нормативных правовых актов**, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности" (утв. ФСБ России 31.03.2015 N 149/7/2/6-432).

Эти методические рекомендации разработаны для госорганов, но также указано, что ими **целесообразно руководствоваться** при разработке частных моделей угроз **операторам информационных систем персональных данных, принявшим решение об использовании средств криптографической защиты информации** (далее – СКЗИ) для обеспечения безопасности персональных данных.

---

[11] Постановление Правительства РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"

[12] Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ") (Зарегистрировано в Минюсте России 10.09.2013 N 29935)

[13] Приказ ФСБ России от 10.07.2014 N 378 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности

Забегая немного вперёд, ФСБ в этих рекомендация выделяет только две ситуации, когда использование СКЗИ для обеспечения безопасности персональных данных необходимо:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);
- хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Таким образом, использование средств криптографической защиты в ИСПДн необходимо только в двух типах случаев при условии актуальности вышеописанных угроз. Однако, до самостоятельного принятия положительного или отрицательного решения об использовании средств криптографической защиты любой организации необходимо пройти путь по организации обработки и обеспечения безопасности ПДн с самого начала. Именно описанию этих процессов и посвящена следующая глава.

Глава 3. Пошаговая инструкция по организации обработки и обеспечению безопасности ПДн для оператора

Согласно 152-ФЗ, **Статья 18.1. п 1.** «**Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей**, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. **Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами**, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами».

Таким образом, несмотря на самостоятельность определения состава и перечня мер, оператор не может решить, что защищать персональные данные он не будет, только потому что определенный им самостоятельно перечень мер не включает и не должен ничего включать, исходя из его личного мнения. **Оператор обязан предпринять необходимые и достаточные меры, а какие именно являются такими следует самостоятельно определить** из ФЗ-152 и принятых в соответствии с ним нормативных правовых актов (основные были описаны в предыдущей главе).

Далее мы вкратце опишем каждую из мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных 152-ФЗ и закрепленных в статье 18.1. этого Закона.

Операторам, которые являются государственными или муниципальными органами при этом следует руководствоваться также **Постановлением Правительства РФ от 21 марта 2012 г. N 211** "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" (далее **ПП-211**) и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

Перечень мер для операторов частного и государственного сектора схожи, однако, в некоторых случаях в нормативных правовых документах для ГИС/МИС можно найти более подробную детализацию, которой нигде нет в документах, разработанных для организаций с частной формой собственности.

Первый этап

Первым шагом в процессе приведения процесса обработки персональных данных в организации в соответствии с требованиями закона должно стать **назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных.**

Кого следует назначить ответственным за организацию обработки персональных данных? Того, кто сможет эффективно выполнять обязанности лица, ответственного за организацию обработки персональных данных, а именно:

- **осуществлять внутренний контроль** за соблюдением оператором и его работниками законодательства РФ о ПДн, в том числе требований к защите ПДн;
- **доводить до сведения работников** оператора положения законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- **организовывать прием и обработку обращений и запросов** субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Из этого следует, что этот ответственный сотрудник занимается **управлением процессом обработки ПДн** и **осуществляет функции менеджмента**, а не обязанности специалиста, который работает больше всех напрямую с субъектами ПДн (клиентами или сотрудниками). Для эффективного выполнения возложенных на него обязанностей он должен **обладать достаточным административным ресурсом** в рамках компании, чтобы процесс организации обработки ПДн на начинал «пробуксовывать» по причине недостаточной мотивации других сотрудников. Исходя из вышесказанного, наибольшая ожидаемая **эффективность** может быть получена **при назначении ответственным кого-либо из руководства компании**.

В дальнейшем при подаче уведомления о намерении осуществлять обработку персональных данных в Роскомнадзор необходимо будет указать контактные данные ответственного за обработку. Поэтому в будущем взаимодействие Регулятора с вашей компанией, например, при проведении проверки, будет начинаться именно через этого сотрудника.

Должен ли ответственный за организацию обработку ПДн обладать компетенциями в вопросах технических мер защиты информации? Для ответа на этот вопрос важно помнить, что

- специалист ответственный за организацию обработки НЕ РАВНО ответственный за обеспечение безопасности ПДн, а процесс обеспечения безопасности ПДн является составляющей частью процесса организации обработки.

При этом только согласно Приказу ФСБ №378, который определяет требования по обеспечению безопасности с использованием средства криптозащиты, для выполнения требования, указанного в пункте 16 этого Приказа, необходимо назначение должностного лица (работника) оператора, обладающего достаточными навыками, ответственным за обеспечение безопасности персональных данных в информационной системе.

Таким образом, для ответственного за организацию обработки необходимые компетенции законодательно не закреплены. Требования предъявляются только к ответственному за обеспечение безопасности ПДн и только в Приказе ФСБ №378, сферу действия которого мы описали ранее (применение средств криптографической защиты).

Назначать ответственных необходимо приказами. При этом относительно всех принимаемых локальных документов, в том числе регламентирующих порядок и условия обработки персональных данных, необходимо помнить о Статье 22 ТК РФ, согласно которой «… Работодатель обязан: … знакомить работников под роспись с принимаемыми локальными нормативными актами, непосредственно связанными с их трудовой деятельностью;»

Второй этап - основной

Результатами второго этапа должно стать

- издание оператором, являющимся юридическим лицом,
  - документов, определяющих политику оператора в отношении обработки персональных данных,
  - локальных актов по вопросам обработки персональных данных, а также
  - локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение
  - правовых,
  - организационных и
  - технических мер по обеспечению безопасности персональных данных в соответствии законом;

Таким образом второй этап можно разбить на две составляющие:

1) организацию обработки и 2) обеспечение безопасности.

Организация обработки

Для того, чтобы эффективно достичь затратных по времени и труду результатов организации обработки, следует **составить план мероприятий**. Для реализации этого плана потребуется **собрать комиссию**, состав которой нужно определить исходя из понимания того, какие сотрудники наиболее хорошо знакомы с работой информационных систем организации, содержащих какие-либо персональные данные. О назначении комиссии следует издать указ и ознакомить членов комиссии с нормативными и методическими документами, которыми нужно руководствоваться.

Комиссия должна провести **«инвентаризацию» персональных данных**, обрабатываемых организацией и **описать процессы их обработки**. Каждый процесс должен иметь цель обработки на правовых основаниях (с письменным согласием субъекта ПДн или без него в соответствии с законом). Для каждого процесса необходимо определить перечень ответственных за обработку и допущенных к ней лиц, состав обрабатываемых ПДн и сроки обработки.

Имея карту процессов обработки ПДн организации, необходимо **выделить все** «изолированные друг от друга» **информационные системы персональных данных (ИСПДн)**. При этом следует помнить, что не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Для каждой ИСПДн необходимо определить перечень, категории и объём обрабатываемых ПДн, перечень действий, правовые основания, даты начала обработки, сроки и условия прекращения обработки, сведения о трансграничной передаче[14], если таковая имеется.

Для обследования ИСПДн рекомендуется разработать анкеты, которые помогут комиссии получить необходимые сведения от работников организации.

Итогом работы комиссии должно стать издание оператором необходимых документов и актов с приказом о вводе документов в действие. **Какой перечень документом необходимо утвердить руководителю организации?**

[14] Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Законодательно подробный перечень документов (как и их формы, шаблоны) для организаций с частной формой собственности не закреплен. Однако, такой перечень можно найти в Постановлении Правительства ПП-211 и, адаптировав, убрав лишнее, применить в своей организации.

Приведём этот список здесь:

- *Политика оператора в отношении обработки персональных данных* или правила обработки персональных данных, устанавливающие *процедуры, направленные на выявление и предотвращение нарушений* законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных
    - *содержание обрабатываемых персональных данных,*
    - *категории субъектов, персональные данные которых обрабатываются,*
    - *сроки их обработки и хранения,*
    - *порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;*
- правила рассмотрения запросов субъектов персональных данных или их представителей;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- правила работы с обезличенными данными в случае обезличивания персональных данных;
- перечень информационных систем персональных данных;
- перечни персональных данных, обрабатываемых в организации;
- перечень должностей ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;
- перечень должностей замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных;
- типовое обязательство сотрудника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку

персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

- типовая форма согласия на обработку персональных данных сотрудника, иных субъектов персональных данных,
- а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;

При разработке документов можно воспользоваться рекомендациями Регуляторов (например, Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»), шаблонами документов, разработанных компаниями интеграторами и образовательными учреждениями, пользоваться для ориентира чужими опубликованными документами. Однако, строго обязательно адаптировать эти документы под специфику своей организации, так как неправильно оформленные документы, например, с указанием неверных целей обработки ПДн, могут быть причиной наложения штрафа на организацию.

Часть документов должны находится в публичном доступе. **Оператор обязан опубликовать** или иным образом обеспечить неограниченный доступ к документу, определяющему его **политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных**. При этом стоит помнить, что политика описывает лишь общий характер действий, направленных на обеспечение безопасности ПДн в организации, поэтому детально раскрывать особенности организации обработки ПДн, которые не требуются по закону, не нужно.

Все **владельцы сайтов**[15], независимо от того сама организация осуществляет его администрирование или это отдано на аутсорсинг другому лицу, **обязаны опубликовать** в соответствующей информационно-телекоммуникационной сети документ, определяющий его **политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных**, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Закончив краткий обзор деятельности оператора по разработке документов и локальных актов, перейдем к мерам по обеспечению безопасности персональных

[15] Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей.

данных. Оба этих процесса, как применение мер, так и разработка и издание документов, связаны с друг другом и происходят одновременно.

Обеспечение безопасности - организационные и технические меры

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, необходимых для выполнения требований, исполнение которых обеспечивает установленные в ПП-1119 уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- и рядом других мер.

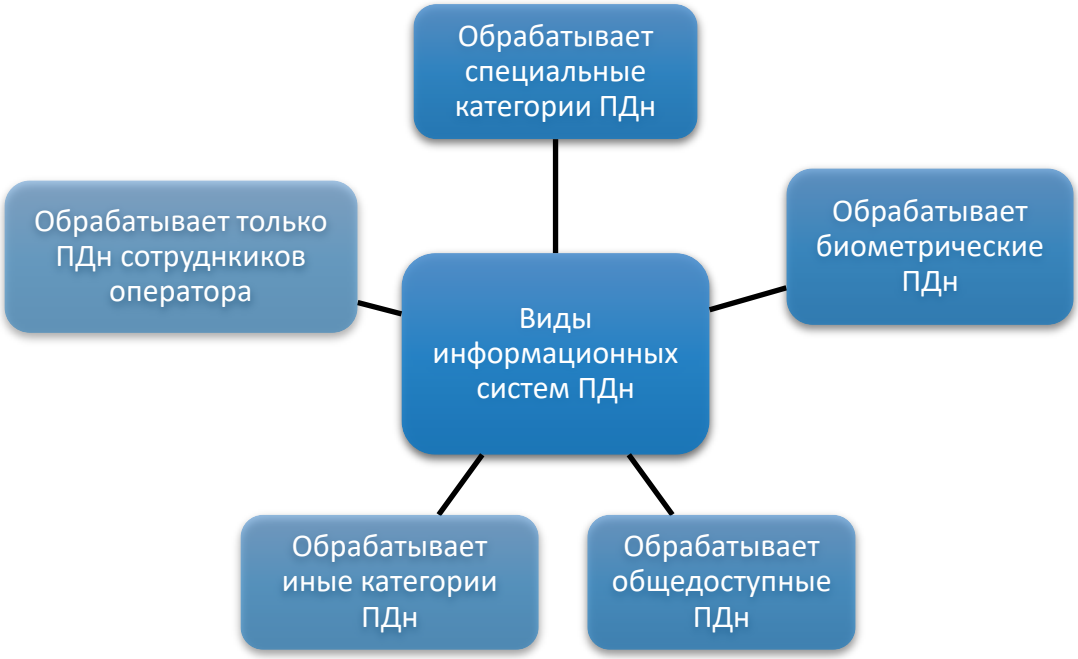
Таким образом организации нужно создать систему обеспечения безопасности ПДн, которая должна:

- Нейтрализовать актуальные угрозы;
- Включать в себя организационные и/или технические меры;
- Применять средства защиты информации, выбранные оператором в соответствии с нормативными правовыми актами ФСТЭК и ФСБ.

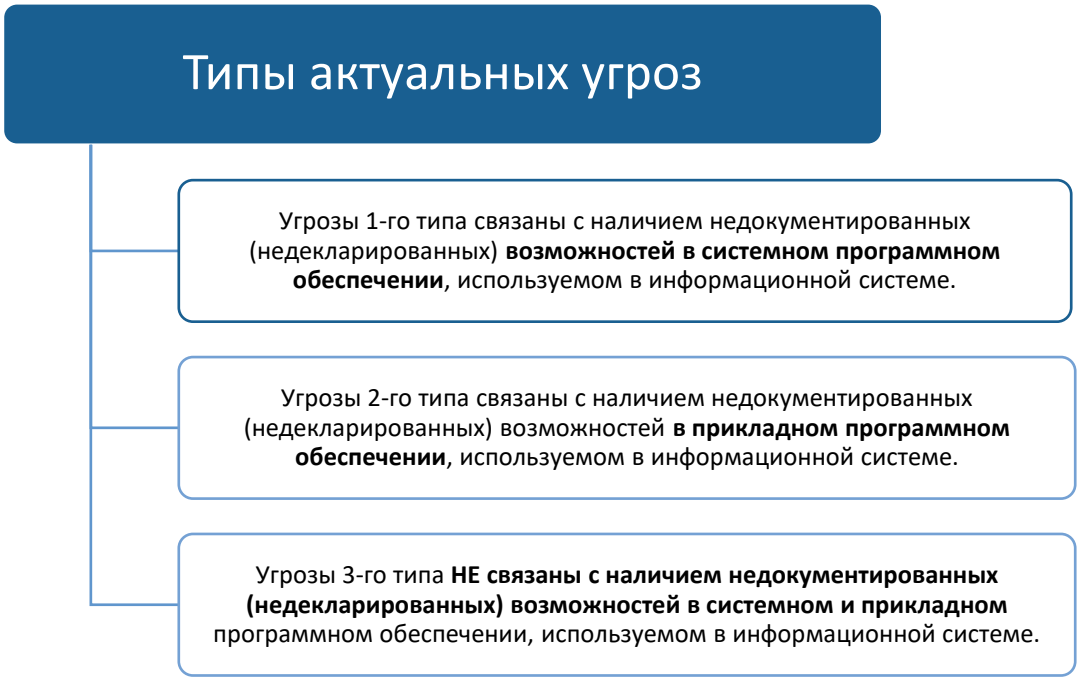
При принятии мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора, оператор обязан оценивать вред, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ и соотносить уровень возможного вреда и принимаемые им меры, направленные на обеспечение выполнения обязанностей. Вред должен определяться исходя из оценки всех неблагоприятных

последствий, которые может повлечь несоблюдение требования Закона: от размера штрафных санкций до репутационных рисков и судебных издержек.

Для этого берём Постановление Правительства №1119 и определяем для каждой ИСПДн уровень защищённости. Для этого для сначала определяем вид ИСПДн.



Далее в соответствии с этим Постановлением нужно понять какие угрозы актуальны для ИСПДн. В ПП-1119 выделяется три типа угроз.



Как понять, что такое угрозы каждого из типов? Технические детали операторы ожидали получить от ФСТЭК. Однако, в «Информационном сообщении по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России № 17 и № 21», Регулятор одновременно сообщил, что ФСТЭК России не наделена полномочиями по разъяснению Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в том числе в части определения типов угроз персональных данных и порядка определения уровней защищенности персональных данных.

Таким образом, ФСТЭК обозначили свою позицию. Из неё следует, что **Правительство России, выпустившее ПП-1119 должны сами разъяснить, что Правительство имело ввиду, говоря об угрозах 1-ого, 2-ого и 3-го типов. Однако, таких разъяснений с их стороны не было опубликовано.** По этой причине возможность решить вопрос об актуальности угроз 1 и 2-ого типов оператору предоставляется **на основе собственных суждений**. Это приводит к тому, что большинство операторов при определении угроз считают актуальными только угрозы 3-го типа.

Теперь, зная тип ИСПДн, в соответствии с ПП-1119 мы можем определить уровень защищенности ПДн при их обработке в этой ИСПДн. Ниже приведена таблица, описывающая необходимость обеспечения каждого из уровней защищенности, установленных ПП-1119 в удобной для работы табличной форме.

Тип ИСПДн	ПДн только сотрудников оператора	Количество субъектов ПДн	Требуемый уровень защищенности		
			если актуальны угрозы		
			1 типа	2 типа	3 типа
ИСПДн-С Специальные	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да	Любое			
ИСПДн-Б Биометрические	Да/Нет	Любое	УЗ-1	УЗ-2	УЗ-3
ИСПДн-И Иные	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да	Любое			
ИСПДн-О Общедоступные	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да	Любое			

Для обеспечения каждого из уровней защищенности персональных данных при их обработке в информационных системах необходимо выполнение набора требований. При этом помимо выполнения требований предыдущего уровня (например, УЗ-4), для каждого последующего (например, УЗ-3) добавляются дополнительные требования.

Требования, выполнение которых необходимо для обеспечения			
УЗ-4	**УЗ-3**	УЗ-2	УЗ-1
• Организация режима обеспечения безопасности помещений, где обрабатываются ПДн • Обеспечение сохранности носителей персональных данных • Утверждение документа, определяющего перечень лиц, допущенных к ПДн • Использование СЗИ, прошедшие процедуру оценки соответствия			
+ Назначение должностного лица, ответственного за обеспечение безопасности персональных данных в ИСПДн			
+ Ограничение доступа к содержанию электронного журнала сообщений *доступ возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей*			
+ Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным в ИСПДн			
+ Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в ИСПДн			

Теперь зная требования для обеспечения необходимого уровня защищенности, берем Приказ ФСТЭК №21 от 18.02.2013г. "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и

- Определяем базовый набор мер;
- Проводит адаптацию базового набора мер;
- Уточняем адаптированный базовый набор мер;
- Дополняем уточненный адаптированный базовый набор мер;

- Разрабатываем иные (компенсирующие) меры.

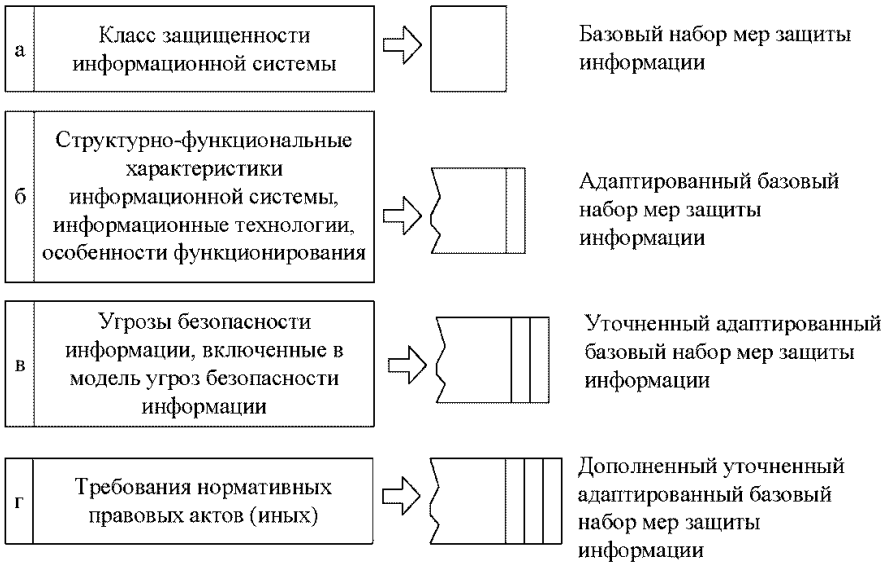
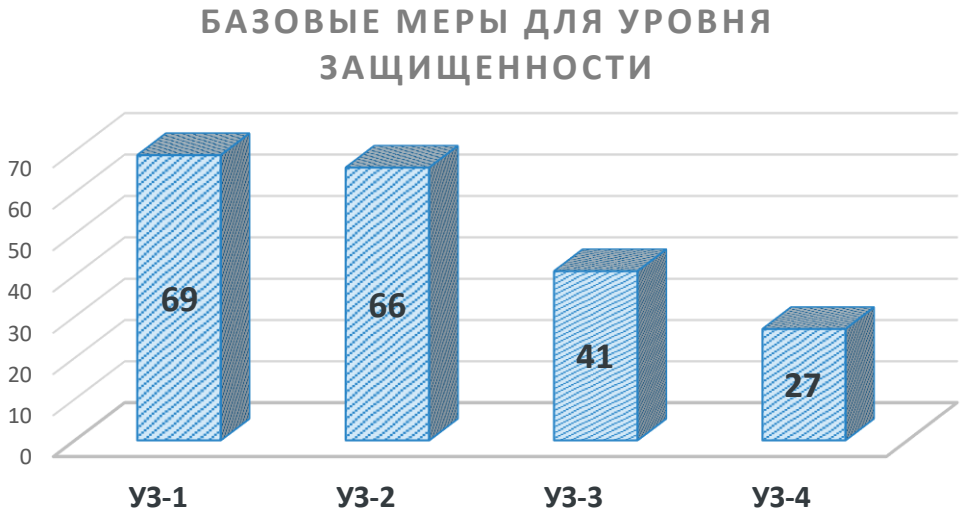


Рисунок. Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе

Состав и содержание мер для каждого из уровней защищенности приведены в приложении к приказу. Все меры не предоставляется возможным и нужным здесь описывать, документ вы можете найти в открытом доступе. Как реализовывать выбранный набор мер оператор может узнать из Методического документа «Меры защиты информации в государственных информационных системах». По применимости этого документа при построении системы защиты ПДн в организациях с частной формой собственности мы говорили ранее.

Количество базовых мер в наборе значительно возрастает между 2 и 3 уровнями защищенности.



Поэтому реализация требований по обеспечению 3 и 4 уровня защищенности является более простым и менее затратным процессом. При этом опираясь на таблицу по определению уровня защищенности, мы можем сделать вывод о том, что **УЗ-3 и УЗ-4 наиболее вероятные для большинства ИСПДн уровни защищенности, особенно при условии определении оператором актуальности только 3 типа угроз**.

Также причиной того, что для организации необходим именно УЗ-4 или УЗ-3 является то, что **многие организации обрабатывают только иные категории персональных данных**. В частности, такими данными являются многие из персональных данных, представляющих собой набор цифр (дата рождения, номер и серия паспорта, СНИЛС, ИНН, номер банковского счёта и тому подобное). Именно такие данные в сочетании с Ф.И.О. чаще всего хранятся в большинстве организаций.

При этом мнение о том, что, храня отсканированные копии паспортов и иных документов с фотографиями физических лиц, компания занимается обработкой биометрических персональных данных, неверное. Неверно это, если организация не использует особые биометрические методы идентификации личности для подтверждения личности по физиологическим параметрам.

Таким образом, если организация не занимается обработкой биометрических ПДн или ПДн специальной категории и определила для себя актуальными угрозы 3-типа, необходимо будет обеспечить 4 или реже 3 уровень защищенности ПДн. УЗ-4 необходим чаще, так как многие организации не достигли масштаба, при котором обрабатываются ПДн более 100 000 субъектов. Скорее всего УЗ-4 или УЗ-3 - именно «ваш случай».

Ниже для примера приведен состав и содержание мер для УЗ-4 из приложения 21 Приказа ФСТЭК.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ. 7	Защита информации о событиях безопасности
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Также необходимо в соответствии с Приказом ФСБ №378 применять средства криптографической защиты информации (СКЗИ) в случаях, если вы определили актуальными угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, а именно:

- передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования между филиалами организации);
- хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Для каждого из уровней защищенности ПДн должны применять СКЗИ соответствующего класса. Класс СКЗИ определяется исходя из совокупности предположений о возможностях для создания способов, подготовке и проведения атак и типа актуальных угроз безопасности ПДн.

Вкратце, для выбора СЗИ и СКЗИ для защиты ПДн необходимо предпринять следующие шаги:

1. Обследовать ИСПДн и определить какие ПДн в ней обрабатываются, кто субъекты и в каком количестве
2. Определить тип актуальных угроз
3. Определить требуемый уровень защищенности ПДн и состав и содержание мер
    - По требуемому УЗ определить классы/уровни сертификации технических СЗИ и выбрать СЗИ
4. Сформировать и утвердить совокупность предположений о возможностях для подготовки и проведения атак
    - По требуемому УЗ, типу актуальных угроз и совокупности возможностей для атак определить требуемый класс СКЗИ и выбрать СКЗИ

Обязательно ли применять сертифицированные средства защиты ПДН?

В Законе сказано, что обеспечение безопасности ПДн достигается применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Требование «оценки соответствия» есть и его необходимо выполнять. Однако, оценка соответствия проводится в формах

- *государственного контроля (надзора),*
- *аккредитации,*
- *испытания,*
- *регистрации,*
- *подтверждения соответствия,*
- *приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме*.

Таким образом, оценка соответствия может быть в различных формах. Требования закона об обязательной сертификации средств защиты, применяемых в организациях с частной формой собственности, нет. Государственный контроль и надзор – это тоже форма оценки соответствия, а значит Оператор может дожидаться проверки со стороны ФСТЭК и ФСБ, чтобы узнать верно ли спроектирована система защиты и применены СЗИ в организации.

При прохождении проверок эффективность предпринятых мер необходимо доказать, поэтому использование в своей деятельности сертифицированных средств защиты информации – это наиболее надёжное решение, минимизирующее риски.

Заключительные этапы

Заключительными этапами в реализации необходимых и достаточных мер для обеспечения выполнения обязанностей добросовестного оператора ПДн являются

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

- Согласно Приказу ФСТЭК №21 оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации **не реже одного раза в 3 года**.

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

Регистрация в реестре операторов ПДн

Также согласно ст. 22 Закона о персональных данных, 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, когда оператор вправе осуществлять без уведомления** уполномоченного органа обработку ПДн:

- обрабатываются только данные сотрудников;
- ПДн получены оператором в связи с заключением договора, стороной которого является субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и **используются оператором исключительно для исполнения указанного договора** и заключения договоров с субъектом персональных данных;
- субъект персональных данных сделал их общедоступными;
- обрабатываются только и исключительно фамилии, имена и отчества;
- для однократного пропуска субъекта персональных данных на территорию оператора;
- при обработке ПДн без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

- в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.

Причину, по которой вы решили не уведомлять Регулятора, рекомендуется отразить в ваших документах, определяющих политику в отношении обработки персональных данных.

Если обработка ПДн в вашей организации не попадает под перечисленные выше исключения об обязательном уведомлении, необходимо отправить уведомление в Роскомнадзор. В ином случае это может быть причиной наложения штрафа на организацию[16].

Подробнее об ответственности оператора и проверках регуляторов мы расскажем в следующей главе.

[16] Форму уведомления можно найти по ссылке: https://pd.rkn.gov.ru/operators-registry/notification/form/

Глава 4. Ответственность оператора и проверки регуляторов

Статья 23 федерального закона от 27.07.2006 «О персональных данных» №152-ФЗ выделяет два направления деятельности Роскомнадзора:

- защита прав субъектов персональных данных;
- контроль и надзор за соответствием обработки персональных данных требованиям законодательства.

Для выполнения этих функций указанная статья закона наделяет Роскомнадзор определенными полномочиями. Рассмотрим самые, на наш взгляд, важные из них.

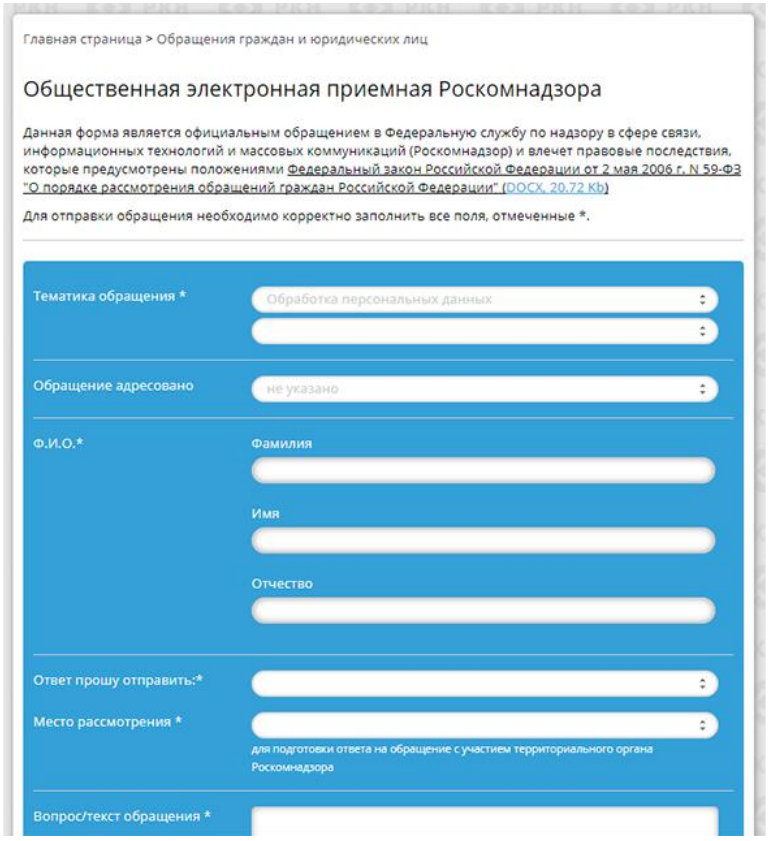
Роскомнадзор:

- проверяет сведения, указанные организацией в Уведомлении;
- может требовать от оператора уничтожения недостоверных или полученных незаконным путем персональных данных;
- может ограничивать доступ к информации, обрабатываемой с нарушением законодательства;
- вправе обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять их в суде;
- наделен полномочиями по привлечению к административной ответственности лиц, виновных в нарушении настоящего Федерального закона;
- обязан рассматривать жалобы и обращения по вопросам, связанным с обработкой персональных данных, а также принимать по ним решения в пределах своих полномочий.

На практике основные действия Роскомнадзора в соответствии с федеральным законом «О персональных данных» следующие:

- работа с обращениями и жалобами граждан;
- проведение контрольных и надзорных мероприятий;
- ведение Реестра операторов персональных данных.

Роскомнадзор рассматривает жалобы по закону от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». Жалобы могут быть направлены как в письменном виде, так и через специальную форму на сайте Роскомнадзора или портала Госуслуг.



Срок рассмотрения обращения — 30 календарных дней, за исключением случаев, установленных в законе. Сейчас в Правительстве ждет утверждения проект нового Административного регламента. Но на данный момент Роскомнадзор проводит проверочные мероприятия на основании Административного регламента, утвержденного приказом Министерства связи и массовых коммуникаций РФ № 312 от 14.11.2011 года. Соответственно, то как проводится проверка, вы можете узнать, ознакомившись с Регламентом, и в том числе, потребовать ознакомить вас с этим регламентом при проведении проверки.

В рамках деятельности по контролю и надзору за порядком обработки персональных данных Роскомнадзор осуществляет плановые и внеплановые проверки.

Плановые проверки

Плановые проверки проводятся на основании ежегодного плана, с ним можно ознакомиться по ссылке **rkn.gov.ru/plan-and-reports**, а также в ежегодных планах деятельности территориальных управлений на следующий год.

План проверок на следующий год обычно размещают на сайтах территориальных управлений в середине декабря текущего года. Так как с 1 сентября 2015 года Роскомнадзор

не согласовывает планы проверок по персональным данным с Прокуратурой, то на сайте последней в сводном плане проверок по всем органам проверок по данной тематике нет. В действующем Административном регламенте сказано, что о проведении плановой проверки территориальное управление Роскомнадзора обязано уведомить вас не позднее, чем в течение трех рабочих дней до начала ее проведения.

В уведомлении о плановой проверке, как правило, написано, что проверяемое лицо должно представить:

- копию документа о назначении должностного лица или уполномоченного представителя, которое будет представлять интересы юридического лица на проверке;
- документы, характер информации в которых предполагает или допускает включение в них персональных данных. К таким документам Роскомнадзор обычно относит заявления, анкеты, журналы и пр.;
- документы, подтверждающие уничтожение персональных данных по достижению цели обработки. К сожалению, не все операторы персональных данных понимают, что в каждом случае обработки персональных данных есть (или должна быть) цель обработки, по достижению которой данные необходимо уничтожить; письменные согласия субъектов персональных данных на обработку их персональных данных;
- документы, подтверждающие соблюдение требований законодательства РФ при обработке персональных данных, в том числе специальных категорий и биометрических персональных данных;
- документы, подтверждающие место размещения баз (информационных систем) персональных данных. Это требование появилось, когда в законодательство внесли поправки о локализации персональных данных россиян; документы, подтверждающие ознакомление работников, непосредственно осуществляющих обработку персональных данных, с законодательством и локальными актами оператора по вопросам обработки персональных данных;
- локальные акты оператора, регламентирующие порядок и условия обработки персональных данных.

Исходя из анализа данных уже размещенных и доступных на сайте Роскомнадзора, всего на 2018 год запланированы мероприятия по организации и проведению контроля (надзора) в отношении около 900 операторов ПДн. По географическому признаку — это самые различные организации «от Клининграда до Владивостока». Для выявления наиболее «проверяемых» отраслей мы воспользовались сведениями об основном виде деятельности

компаний по ОКВЭД. В планах лидируют «традиционные» для проверок РКН отрасли: образование, медицина, туризм, подбор персонала, финансовые услуги и управляющие компании.

Около 38% операторов в планах проверок — государственные организации. Соответственно на долю коммерческих организаций приходится более 62% мероприятий. Практически 99,8% — это юридические лица, а не индивидуальные предприниматели.

В план проверок включают юридических лиц, которые подали Уведомление об обработке персональных данных в реестр операторов, и тех, кто этого не сделал. Мнение о том, что, не подав уведомление об обработке ПДн в Роскомнадзор, можно избежать проверок ошибочно. Проверить могут всех. Срок проведения как плановой, так и внеплановой проверки не может превышать 20 рабочих дней.

Внеплановые проверки Роскомнадзора

Внеплановые проверки бывают документарные и выездные. Документарные проводятся в форме запроса Роскомнадзором необходимых документов и предоставления вами этих документов в срок, указанный в запросе. О проведении внеплановой проверки оператор уведомляется не позднее, чем за 24 часа до ее начала любым доступным способом. Обычно это делается по телефону или по факсу.

Такие проверки могут проводиться в большинстве случаев по следующим основаниям:

- если истек срок исполнения оператором ранее выданного предписания об устранении выявленного нарушения. Обычно после плановой проверки Роскомнадзор проводит внеплановую, чтобы выяснить, как устранено нарушение. Такая проверка редко бывает выездной. Она проводится в документарной форме, то есть Роскомнадзор запросит у вас сведения об устранении нарушений, а вы должны предоставить необходимые документы;
- если в службу или ее территориальные органы поступило обращение от граждан, юридических лиц, индивидуальных предпринимателей, информация от органов государственной власти, органов местного самоуправления, из средств массовой информации. В 2011 году в службу поступило примерно 1500 жалоб, а в 2016 году — уже примерно 33 000;
- по приказу руководителя Роскомнадзора или руководителя территориального управления.
- по факту выявления в результате систематического наблюдения нарушений обязательных требований

Мероприятия систематического наблюдения

Еще один вид контроля — мероприятия систематического наблюдения. Понятие «мероприятия по систематическому наблюдению» добавилось в 2015 году. Основное отличие - мероприятия осуществляются без взаимодействия с проверяемыми лицами. В последние годы это самый популярный вид контроля за порядком обработки персональных данных. Популярность таких мероприятий вызвана тем, что трудозатраты территориальных управлений на их проведение куда меньше плановых проверок, а эффективность намного больше. За небольшой период времени каждое территориальное управление Роскомнадзора может проверить десятки или даже сотни организаций, начав как правило с проверки их интернет-сайтов.

На сайте организации, как мы уже выяснили, должен быть опубликован документ, определяющий политику владельца сайта в отношении обработки персональных данных. Это и является самым популярным нарушением, выявляемым в ходе мероприятий систематического наблюдения, если на сайте выявлен случай сбора персональных данных (например, формы заявки, регистрации или обратной связи с определенным набором запрашиваемых сведений).

Систематическое наблюдение опасно тем, что оповещать о нём компанию никто не обязан. По результатам, если выявлены нарушения, проводится внеплановая проверка в соответствии с «Административным регламентом». Мероприятия систематического наблюдения проводятся на основании приказа руководителя территориального органа и закрепляются в ежегодном плане деятельности территориального управления на следующий год.

Также Роскомнадзор может запросить правовые основания для размещения чьих-либо персональных данных. Такие запросы уже поступали, например, в образовательные организации, когда на их сайте размещали персональные данные о школьниках и их успехах в олимпиадах. Так что, размещая персональные данные своих работников или иных лиц на сайте, проконтролируйте соблюдение требований закона.

Проверки Государственной инспекции труда

В Трудовом Кодексе РФ 14 глава называется: «Защита персональных данных работника». Государственная инспекция труда проводит контрольно-надзорные мероприятия по поводу выполнения требований всего Трудового кодекса и, соответственно, не может обойти стороной главу 14. На проверках обращают внимание на требование пункта 8 статьи 86:

«работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области».

Таким образом, проверяют наличие такого документа и факт ознакомления с ним всех работников.

Административная ответственность за нарушение этих требований предусмотрена статьей 5.27. КоАП — штраф в размере от 30 000 до 50 000 рублей.

Проверки ФСТЭК и ФСБ

Статья 19 федерального закона «О персональных данных» устанавливает меры по обеспечению безопасности персональных данных при их обработке.

В части 4 статьи 19 установлено, что состав и содержание необходимых для выполнения установленных Правительством требований, организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в ИСПДн устанавливают ФСТЭК и ФСБ в рамках их полномочий.

В части 8 статьи 19 федерального закона «О персональных данных» закреплен важный момент:

«Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных».

Выходит, ФСБ и ФСТЭК могут проверять организации, эксплуатирующие государственные информационные системы. Для остальных информационных систем контроль в законе не закреплен. Сказано лишь, что ФСТЭК И ФСБ «решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер…, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных…».

Проверки ФСТЭК и ФСБ могут быть как плановыми, так и внеплановыми.

На что обратить внимание

Обработка персональных данных — это каждодневная деятельность любого юридического лица. Мы постоянно работаем с данными наших работников и клиентов (пациентов, студентов, покупателей, заявителей, пользователей сайта, заемщиков, страхователей, посетителей, зрителей и пр.). Одни и те же данные одного и того же человека мы обрабатываем в разных случаях. И взятое в одном случае согласие — на другой может не распространяться.

Соответственно, чтобы предотвратить негативные последствия, мы должны обратить внимание на правовую основу обработки персональных данных в каждом конкретном случае обработки, т. е. понять, есть ли у нас договоры, согласия или даже нормативные акты, которые Роскомнадзор признает при проверке законным основанием для обработки персональных данных. А проверка может возникнуть в любой момент.

Например, у вас есть сайт. Вы собираете на нем данные через различные формы. Соответственно, вас могут проверить в ходе мероприятий систематического наблюдения, или в случае, если какой-нибудь посетитель вашего сайта подаст на вас жалобу. Также вами может быть недоволен ваш клиент или работник (бывший тоже может), которые имеют возможность пожаловаться в Роскомнадзор, и тот в свою очередь обязан на такие жалобы реагировать. Так что ваша задача — обеспечить правовую основу для каждого случая обработки.

Вкратце повторив требования закона, описанные ранее в этой книге, оператору следует:

- Получать письменное согласие у каждого субъекта ПДн для определенных целей, если это необходимо по закону, и запрашивать только такие данные, которые нужны для этих конкретных целей;
- Публиковать или иным образом обеспечить неограниченный доступ к документу, определяющему политику в отношении обработки персональных данных и к сведениям о реализуемых требованиях к защите персональных данных;
- Использовать данные только для заявленных в документах целей, о которых предупрежден человек;
- Не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных;

- Немедленно прекратить по требованию субъекта персональных данных при обработке его персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации;
- Устранять нарушения законодательства, допущенные при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных;
- Организовать прием и обработку обращений и запросов субъектов ПДн и сообщать по запросу субъекта ПДн информацию, касающеюся обработки его персональных данных, в том числе содержащей:
    - подтверждение факта обработки ПДн оператором;
    - правовые основания и цели обработки персональных данных;
    - цели и применяемые оператором способы обработки ПДн;
    - 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;
    - обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
    - сроки обработки персональных данных, в том числе сроки их хранения;
    - порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
    - информацию об осуществленной или о предполагаемой трансграничной передаче данных;
    - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- Принимать необходимые и достаточные меры для обеспечения выполнения обязанностей Оператора в соответствии с законом;
- Ознакомить и/или обучить сотрудников законодательству России в сфере защиты прав субъектов ПДн, ознакомить под роспись с локальными документами организации;
- Подать уведомление об обработке ПДн в Роскомнадзор.

Ответственность, риски и штрафы

Учитывая интенсивное развитие информационно-коммуникационных технологий, растет объем и масштаб правонарушений в области персональных данных.

7 февраля 2017 года Президент России подписал Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», которые вступили в силу с 1 июля 2017 года.

Прежняя редакция статьи 13.11 КоАП РФ не позволяла в полной мере обеспечить эффективную защиту прав и интересов субъектов персональных данных и не учитывала тяжесть негативных последствий совершенных правонарушений.

В целях повышения эффективности реализации мер административной ответственности в области персональных данных Федеральным законом дифференцируются составы административных правонарушений в области персональных данных с учетом ущерба, причиненного нарушением, и устанавливаются дополнительные составы административных правонарушений в области персональных данных, а также усиливается ответственность за их нарушение, значительно (в разы) увеличиваются размеры административных штрафов.

Суммируя, отметим, что вместо единственного вида административной ответственности, описанного в статье 13.11 КоАП РФ, появилось семь. За различные нарушения в сфере персональных данных можно будет применять разные штрафы. **Если нарушение по разным составам выявят несколько, то, соответственно, количество штрафов может увеличиваться кратно.**

Одним из самых ярких случаев в прошлом является плановая выездная проверка в отношении Департамента здравоохранения Ивановской области 1 декабря 2011 года. По окончании проверки выданы 14 предписаний[17]. Таким образом после наложения штрафа в размере установленном текущей редакцией КоАП, суммарное наказание может превысить сотни тысяч рублей.

Рассмотрим новые составы правонарушений детально.

1. Обработка персональных данных в случаях, не предусмотренных законодательством, либо **обработка, несовместимая с целями сбора** персональных данных влечет

   a. предупреждение или

[17] 37.rkn.gov.ru/news/news31219.htm

b. наложение штрафа на граждан в размере от 1000 до 3000 рублей;
c. на должностных лиц - от 5000 до 10000 рублей;
d. на юридических лиц - от 30000 до 50000 рублей.

2. Обработка персональных данных **без согласия в письменной форме** субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено**, либо обработка ПДн с нарушением** требований **к составу сведений, включаемых в согласие в письменной форме** субъекта ПДн на обработку его ПДн, влечет

a. штраф на граждан в размере от 3000 до 5000 рублей;
b. на должностных лиц - от 10000 тысяч до 20000 тысяч рублей;
c. на юридических лиц - от 15000 до 75000 тысяч рублей.

3. Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных -

a. предупреждение или
b. штраф на граждан от 700 до 1500 рублей;
c. на должностных лиц - от 3000 до 6000 рублей;
d. на индивидуальных предпринимателей - от 5000 до 10000 рублей;
e. на юридических лиц - от 15000 до 30000 рублей.

4. Невыполнение оператором обязанности по предоставлению субъекту ПДн информации, касающейся обработки его персональных данных, -

a. предупреждение или
b. штраф на граждан от 1000 до 2000 рублей;
c. на должностных лиц - от 4000 до 6000 рублей;
d. на индивидуальных предпринимателей - от 10000 до 15000 рублей;
e. на юридических лиц - от 20000 до 40000 рублей.

5. Невыполнение оператором в сроки, установленные законодательством, требования субъекта ПДн или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, -

a. предупреждение или
b. штраф на граждан в размере от 1000 до 2000 рублей;
c. на должностных лиц - от 4000 до 10000 рублей;
d. на индивидуальных предпринимателей - от 10000 до 20000 рублей;
e. на юридических лиц - от 25000 до 45000 рублей.

6. Невыполнение оператором при обработке ПДн без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих сохранность персональных данных при хранении материальных носителей ПДн и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния -

a. штраф на граждан от 700 до 2000 рублей;
b. на должностных лиц - от 4000 до 10000 рублей;
c. на индивидуальных предпринимателей - от 10000 до 20000 рублей;
d. на юридических лиц - от 25000 до 50000 рублей.

7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных -

a. предупреждение или
b. наложение штрафа на должностных лиц в размере от 3000 до 6000 рублей.

Кроме того, внесены изменения и дополнения в КоАП РФ, касающиеся наделения Роскомнадзора полномочиями в области административного производства в рамках осуществления государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

До 1 июля 2017 года возбуждать дела по административным делам, связанным с персональными данными, по статье 13.11 КоАП РФ был вправе исключительно прокурор. Это предусмотрено частью 1 ст. 28.4 КоАП РФ.

С 1 июля 2017 года **участие прокурора стало необязательным**. С указанной даты **дела по статье 13.11 КоАП будут вправе возбуждать должностные лица Роскомнадзора**. Такая поправка внесена комментируемым законом в пункт 58 части 2 статьи 28.3 КоАП РФ. Следовательно, **процедура привлечения к ответственности по делам о персональных данных стала проще**.

Ранее проблема заключалась в длительном процессе сбора материалов, направлении их в органы прокуратуры, рассмотрении органами прокуратуры представленных материалов. Характер правонарушений по статье 13.11 КоАП РФ, который не является длящимся и для которых установлен 3-х месячный срок давности, делал затруднительным привлечение операторов к установленной законом административной ответственности.

В сложившейся ситуации наделение Роскомнадзора полномочиями по возбуждению дел об административных правонарушениях по статье 13.11 КоАП РФ позволит в значительно большей мере обеспечить соблюдение принципа неотвратимости наказания за совершенное правонарушение.

Из-за существенного увеличения штрафов изменится подход организаций к выполнению требований закона и к подготовке к проверкам. Если раньше организации считали, что проще ничего не делать и можно ждать вероятную проверку, по ее итогам заплатив небольшой штраф (до 10 000 рублей), то теперь компании будут бороться за свои права, а значит, это положительно повлияет на довольно неоднозначную судебную практику по данным вопросам.

Кроме штрафов в пользу государства за нарушение правил обработки ПДн по решению суда может быть взыскана компенсация морального вреда.

В случае, если несоблюдение требований к обработке ПДн привело также к нарушению неприкосновенности частной жизни может быть применено наказание в соответствии со ст. 137 УК РФ: от штрафа до лишения свободы на срок до 2 лет. Если те же деяния совершены лицом с использованием своего служебного положения, законом установлено более суровое наказание.

Работникам и работодателям также следует помнить о том, что в соответствии со статьей 81 ТК РФ разглашение охраняемой законом тайны, в том числе разглашение персональных данных другого работника, является грубым нарушением трудовых обязанностей и может быть законной причиной расторжения трудового договора работника по инициативе работодателя.

В заключении этой главы, хотелось бы отметить, что при несоблюдении требований законодательства в сфере персональных данных, кроме риска серьезных штрафов необходимо помнить о возможном ущербе деловой репутации компании и снижении стоимости её нематериальных активов. В случае с крупными компаниями, обрабатывающими данные тысяч клиентов, подобные потери могут значительно превысить размер штрафов и снизить устойчивость её функционирования.

Курс на защиту прав субъектов персональных данных взят в России относительно недавно, однако ждать отмены требований этого закона бессмысленно. В будущем ожидается повышение осведомленности граждан о правах субъектов персональных данных и ужесточение законодательства, а значит риск жалоб в случае нарушения требований закона будет только расти.

Организациям, выбирающим стратегию клиентоориентированности и социально ответственного бизнеса, ориентированным на непрерывность деятельности и долгосрочное развитие, чтобы избежать критичных рисков, следует, не дожидаясь проверок, привести процесс обработки персональных данных в соответствии с законом. Начать заниматься защитой персональных данных нужно как можно раньше, так как процесс оформления полного комплекта документов, обучения сотрудников и принятия комплекса необходимых и достаточных организационных и технических мер для всех ИСПДн организации может занять значительно время.

Стоит помнить, что обработка ПДн также может осуществляться лицом по поручению оператора. При автоматизированной обработке можно обратиться к облачному провайдеру и избавить себя хотя бы от части головной боли по вопросу соответствия и сократить свои издержки.

Глава 5. Обработка персональных данных как услуга

Право оператора поручить обработку персональных данных другому лицу с согласия субъекта персональных данных закреплено в части 3 статье 6. «Условия обработки персональных данных» Федерального закона №152.

Постановление Правительство №1119 также сообщает о том, что безопасность персональных данных при их обработке в информационной системе может обеспечивать лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. **Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.**

Приказ ФСТЭК № 21 повторяет норму ПП-1119 о возможности обеспечения безопасности ПДн лицом по поручению оператора. При этом для выполнения этих работ могут привлекаться на договорной основе **юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации**.

Популярным решением, освобождающим оператора ПДн от капитальных затрат на создание и владение защищенной IT-инфраструктурой для выполнения требований 152-ФЗ и 242-ФЗ стало размещение ИСПДн в облаке.

Иными словами, многие российские компании воспользовались правом поручить облачному провайдеру обязанности по обеспечению безопасности ПДн и принятию всех необходимых и достаточных организационно-технические мер для защиты персональных данных от несанкционированного и неправомерного доступа.

Для читателей незнакомых с облачной моделью потребления услуг, вкратце поясним, что при таком подходе клиенты получают доступ к любым IT-ресурсам удаленно через сеть. Это могут быть универсальные серверные мощности, специализированные элементы облака, реализующие функции защиты или просто готовая 1С как услуга. Клиент имеет возможность самостоятельно и оперативно изменять объем и состав ресурсов, защищенных и изолированных для использования только им. Оплата при этом происходит в строгом соответствии с тем сколько и в течении какого периода использовал клиент.

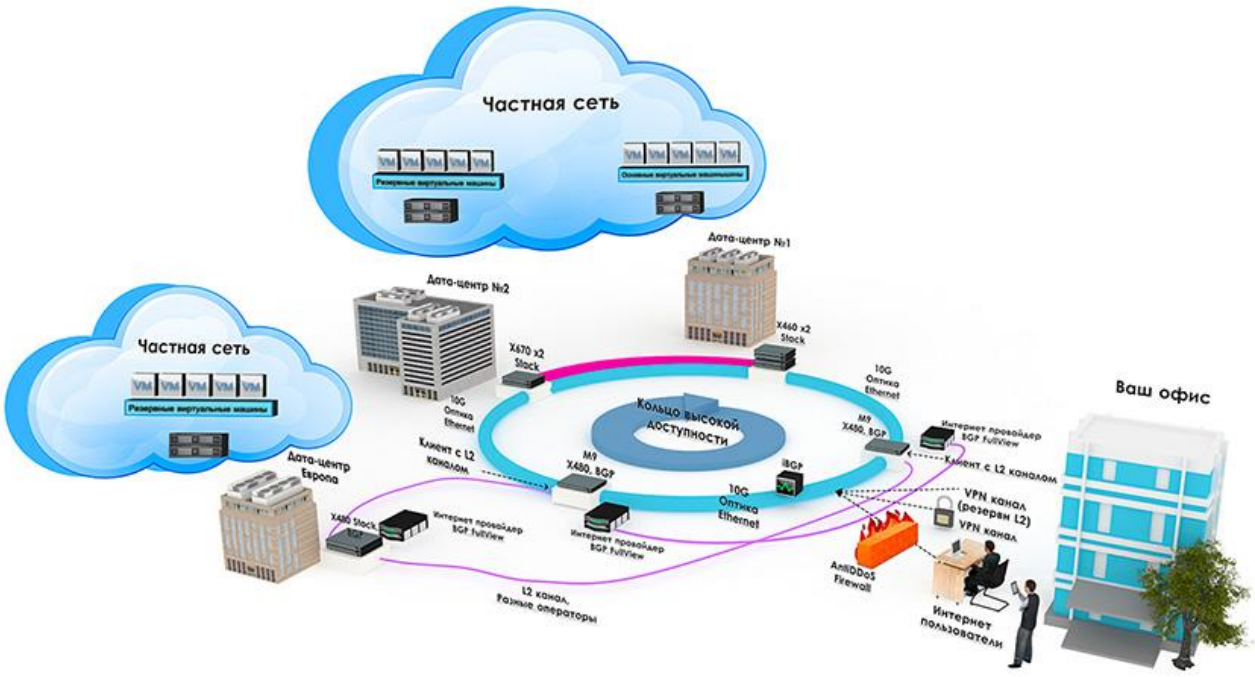
«Настоящее» облако объединяет в себе пул всех необходимых IT-ресурсов и обладает полезными свойствами

- эластичности,
- масштабируемости,
- доступности в любом месте, где есть Интернет,
- с удобным самообслуживанием и
- гибким биллингом
- позволяет стабильно получать качественные услуги, полностью соответствующие актуальным потребностям бизнеса.

Такой потребностью, как мы выяснили, является передача с целью экономии денег и времени части обязанностей оператора ПДн на лицо, которое может профессионально их выполнять.

Немного об авторах книги

Корпоративный облачный провайдер Cloud4Y с момента основания в 2009 году ориентирован на удовлетворение высоких требований бизнеса к IT-услугам. Мы предлагаем программно-конфигурируемые дата-центры (vDC) на базе кластерных решений VMware vSphere с управлением посредством портала самообслуживания VMware vCloud Director.



Помимо модели IaaS (инфраструктура как услуга), мы разработали и успешно предоставляем множество актуальных и популярных SaaS-продуктов (1С в облаке, удаленные рабочие столы, корпоративная почта, антиспам и многое другое).

Используемый стек технологий VMware, надежное оборудование, расположенное в сети безопасных дата-центров TIER III, объединенных оптическим кольцом высокой доступности с дублированием каналов связи, обеспечивают должное качество услуг и отказоустойчивость необходимые для Enterprise-клиентов.

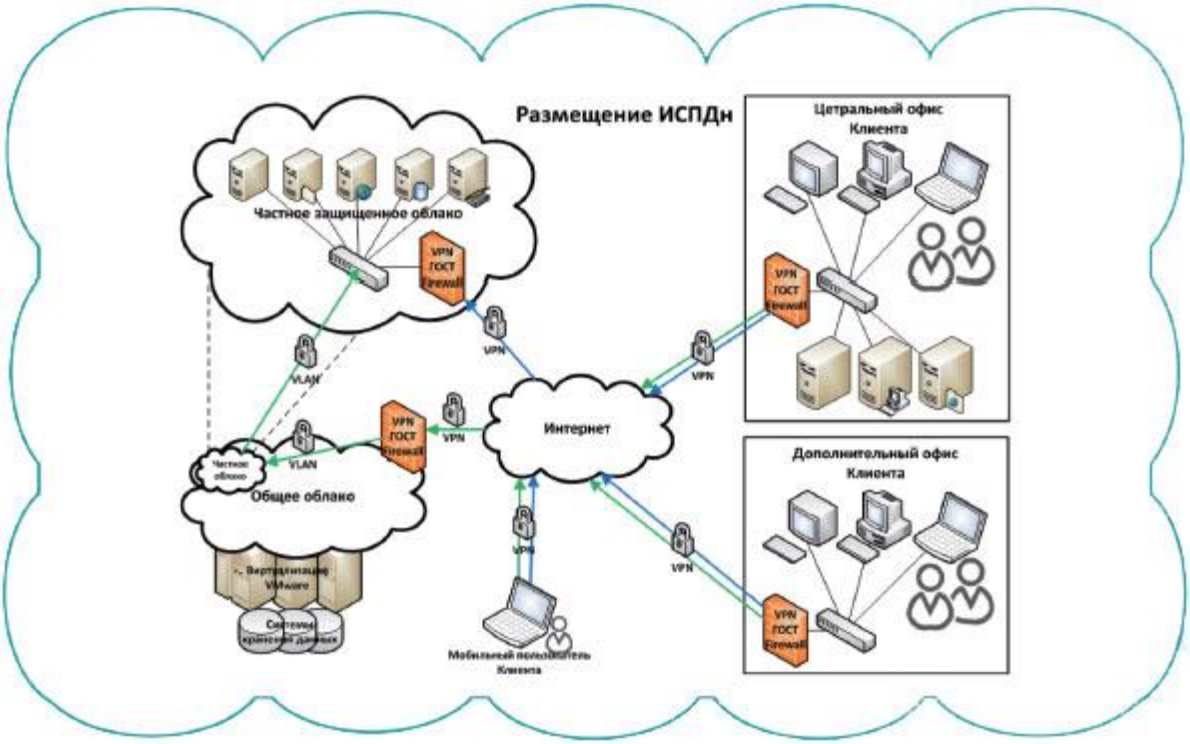
Центры обработки данных, расположены в России, что полностью соответствует норме права о локализации хранения баз и отдельных процессов обработки персональных данных российских граждан на территории России.

Среди наших клиентов: Спасибо от Сбербанка, MODIS, «Федерация гандбола России», ФБУН Центральный НИИ Эпидемиологии Роспотребнадзора, Администрация Костромской области и прочие. Все перечисленные клиенты используют нашу защищенную в соответствии с требованиями законодательства инфраструктуру «Облако ФЗ 152» в том числе для размещения своих ИСПДн.

Особенности размещения ИСПДн в облаке

- Обеспечение безопасности ПДн предоставляется как услуга, то есть, заказчик не имеет капитальных затрат.
- Комплекс необходимых и достаточных организационно-технических мер защиты, позволяет обеспечить клиентам невозможность реализации угроз безопасности ПДн, в том числе со стороны обслуживающего персонала провайдера и со стороны других клиентов, расположенных "по соседству" в облаке. По решению клиента базовый набор мер для установленного УЗ ПДн может быть адаптирован, уточнен и дополнен.
- На различные элементы облака, реализующие функции защиты (гипервизор, средства защиты, интегрированные в облако, средства защиты, предлагаемые клиентам как сервисы безопасности) имеются сертификаты, выданные соответствующими органами ФСТЭК и ФСБ России. Это даёт гарантию того, что применяемые средства защиты прошли в установленном порядке оценку соответствия.
- Система прошла аттестацию лицензиатами ФСТЭК, что подтверждает её соответствие требованиям безопасности в целом.

- Размещение ИСПДн в облаке позволяет использовать общесистемное и специальное ПО провайдера в аренду и получать сопровождение IT-инфраструктуры высококвалифицированным персоналом в режиме 24x7.



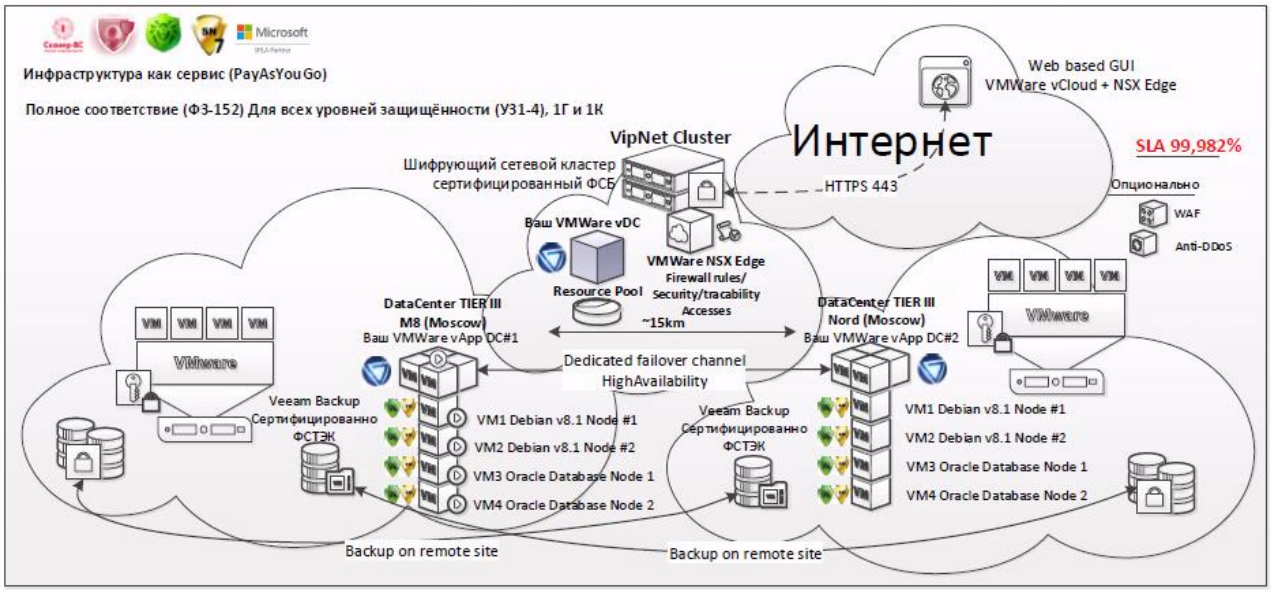
Следовательно, в рамках процесса организации обработки и обеспечения безопасности персональных данных в организации, облачный провайдер готов взять на себя обязанности по защите ПДн, предоставив для размещения ИСПДн заказчика свою инфраструктуру с реализованным комплексом мер, которые необходимы и достаточны для обеспечения установленного для ПДн уровня защищенности.

Реализация взаимодействия оператора ПДн и облачного провайдера может быть реализована двумя подходами. Мы готовы

1. осуществлять обработку ПДн по поручению оператора;
2. предоставить готовое отдельное облако с реализованным комплексом необходимых и достаточных организационно-технических мер для обеспечения нужного клиенту уровня защищенности ПДн.

При выборе второго варианта и использовании такого защищенного облака клиент сам решает, что в нем размещать и обрабатывать, а доступ сотрудников провайдера к размещаемым данным полностью запрещен с помощью сертифицированных ФСТЭК средств (vGate R2). Обмен данными происходит по защищенным каналам связи. Для возможности оценки клиентом и регуляторами мер по информационной безопасности, предпринятых

Cloud4Y, по запросу предоставляются необходимые сертификаты и аттестаты соответствия, а также лицензии ФСТЭК и ФСБ на осуществление соответствующих видов деятельности.



Пример реализации облачной инфраструктуры

Помимо этого, специалисты Cloud4Y при необходимости консультируют компании в рамках организации обработки и обеспечения безопасности ПДн по вопросам:

- организации обработки ПДн;
- проведения обследования информационных систем;
- разработки Политики в отношении обработки персональных данных, других необходимых локальных актов;
- выбора и применения СЗИ и СКЗИ;
- проведения оценки эффективности реализованных в рамках системы защиты мер;
- сопровождают клиентов при проведении проверок.

Если для вас актуальна тема обеспечения безопасности персональных данных в вашей организации, вы можете проконсультироваться, обратившись к любому менеджеру Cloud4Y по телефону +7 (495) 268-04-12 или любым другим удобным вам способом.