И. В. Андрианова

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ОРГАНИЗАЦИИ

АЛГОРИТМ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНААЛЬНЫХ ДАННЫХ

◆

ПРИМЕРЫ ДОКУМЕНТОВ

◆

НОРМАТИВНАЯ БАЗА

◆

ОБЗОР ИЗМЕНЕНИЙ В ЗАКОНОДАТЕЛЬСТВЕ ЗА 2022-2023 ГГ.

Ирина Андрианова

Персональные данные в организации

«Издательские решения»

Андрианова И.

Персональные данные в организации / И. Андрианова — «Издательские решения»,

ISBN 978-5-00-597035-0

Эта книга — практический материал, который поможет сэкономить Ваше время, быстро сориентироваться в изменениях законодательства и разработать документы по персональным данным. В книге приведен обзор законодательства, алгоритм построения системы защиты персональных данных, примеры документов (политика, приказы, инструкции, согласия, уведомления, акты и др.).Для специалистов, ответственных за работу с персональными данными,руководителей организаций и учреждений.

ISBN 978-5-00-597035-0

Содержание

Персональные данные в организации

Ирина Андрианова

ISBN 978-5-0059-7035-0
Создано в интеллектуальной издательской системе Ridero

1. ОСНОВНЫЕ ПОНЯТИЯ, КЛАССИФИКАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБЗОР ЗАКОНОДАТЕЛЬСТВА

Как организовать работу с персональными данными сотрудников, клиентов, контрагентов в организации? Какие документы по обработке и защите персональных данных должны быть разработаны и какими нормативно-правовыми актами необходимо руководствоваться?

Ответы на каждый из этих вопросов дают федеральные законы и другие нормативные правовые акты Российской Федерации, которые являются основанием для работы с персональными данными в любой организации (предприятии, учреждении).

Конституция Российской Федерации гарантирует каждому гражданину нашей страны право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства (ст. 23) и устанавливает запрет на сбор, хранение, использование информации о частной жизни человека без его согласия. На основании Конституции был создан Федеральный закон о персональных данных для обеспечения прав людей и защиты личных сведений.

1.1. Федеральный закон о персональных данных

Основной закон, регулирующий работу с персональными данными – Федеральный закон **от 27.07.2006 №152-ФЗ** «О персональных данных» (далее – ФЗ-152). В нем содержатся порядок работы с персональными данными, принципы и условия их обработки, требования к содержанию некоторых документов, например, согласий на обработку ПДн, права субъекта ПДн и обязанности оператора.

Основные понятия ФЗ-152 содержатся в статье 3.

Персональные данные (далее – ПДн) – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п.1 ст. 3 ФЗ-152). Т. е. это информация, которая относится к конкретному человеку, например, ФИО, пол, возраст, дата рождения, номер телефона, адрес электронной почты и др. Однако, некоторые данные не являются ПДн сами по себе, а становятся таковыми только в совокупности с другими сведениями. Например, сам номер телефона без ФИО не является ПДн, т. к. идентифицировать человека в этом случае невозможно. А если организация обрабатывает и хранит данные в совокупности (ФИО, номер телефона, email), то и номер телефона и адрес электронной почты являются персональными данными. Также фамилия, имя, отчество являются персональными данными только в привязке к другим данным, например, паспортным (дата и место рождения, номер паспорта и тп).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с ПДн, т. е. оператором персональных данных являются все организации, учреждения, предприятия, которые собирают, распространяют, обрабатывают и хранят ПДн работников, а также клиентов и контрагентов (п.2 ст. 3 ФЗ-152).

Субъект персональных данных – это физическое лицо, которое идентифицируется с помощью конкретных ПДн, т. е. носитель этих данных. Законодательством предусмотрено 2 основные категории субъектов ПДн – работники организации и те, кто ими не является. К субъектам ПДн относятся: работники оператора, соискатели, бывшие работники, родственники работников; контрагенты и клиенты (физ. лица); законные представители, работники юр. лиц, являющихся клиентами, контрагентами оператора.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 ФЗ 152). Т. е. обработка – это любые действия с персональными данными.

Например, сотрудник при трудоустройстве предоставил работодателю документы со сведениями о себе и своей трудовой деятельности. Сотрудник – это субъект персональных данных, работодатель – оператор, который собирает эти данные о сотруднике, хранит и анализирует, т.е. обрабатывает персональные данные конкретного работника.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения ПДн);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (п. 8 ст. 3 ФЗ-152).

Документы, содержащие персональные данные работников организации
- анкета, автобиография, личный листок по учету кадров – заполняются работником при приеме; - копии документов, предъявляемых при приеме на работу: паспорт, военный билет, диплом, ИНН, СНИЛС или другой документ персонифицированного учета, свидетельства о заключении брака, рождении детей и тп.; - личные дела работающих и уволенных работников; - трудовые книжки; - личные карточки работников по форме Т-2; - трудовые договоры и дополнительные соглашения к ним; - приказы по личному составу и их копии; - документы оплаты труда; - документы об обучении, оценке, аттестации работников; - базы данных, которые обрабатываются автоматически: таблицы Excel, базы кадровых и бухгалтерских программ и тп.; - иные документы с ПДн работников.

Когда не требуется согласие на обработку ПДн (ч.1 ст. 6 ФЗ-152)	
№ п/п	**обстоятельства**
1	Обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством РФ на оператора функций, полномочий и обязанностей;
2	Обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве (обработка осуществляется полицией, прокуратурой и тп.);
3	Обработка ПДн необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года №210-ФЗ «Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации ПДн на едином портале государственных и муниципальных услуг;
4	Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
5	Обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
6	Обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
7	Обработка ПДн необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;
8	Обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 ФЗ-152, при условии обязательного обезличивания ПДн;
9	Осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);
10	Осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1.2. Информационная система и виды обработки ПДн

Во многих организациях персональные данные обрабатываются в специальных кадровых, бухгалтерских и других программах, собираются и размещаются на сайтах компаний и др., а также обрабатываются в государственных информационных системах (ГИС).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (п.10 ст.3 ФЗ-152).

ФЗ-152 определяет следующие способы обработки персональных данных:

1) *неавтоматизированная* – обработка ПДн без использования средств автоматизации, т. е. вручную, когда сведения вносятся человеком. Особенности организации такой обработки ПДн, а также меры по защите ПДн обозначены в **Постановлении Правительства РФ от 15.09.2008 N 687** «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». В этом документе прописан порядок работы с материальными носителями ПДн и меры по обеспечению безопасности ПДн при такой обработке.

2) *автоматизированная* – обработка персональных данных с помощью средств вычислительной техники (компьютеров и других электронных устройств, баз данных, средств криптозащиты, программ, скриптов и тп. 9 (п. 4 ст.3 ФЗ-152). Состав и содержание мер по обеспечению безопасности персональных данных существенно больше, чем при неавтоматизированной обработке, и обозначены в **приказе ФСТЭК России от 18.02.2013 N 21 «**Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3) *смешанная* – обработка сведений происходит и автоматизированным и неавтоматизированным способом.

Некоторые компании (например, турагентства) в ходе своей деятельности передают персональные данные за границу, т. е осуществляют **трансграничную передачу ПДн** – передачу персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (п. 11 ст. 3 ФЗ-152).

Хранить ПДн организация может по-разному – и в электронном виде (на сервере или в облачном хранилище), и в бумажном (хранить документы в картонных папках в архиве). Бесцельно хранить и обрабатывать ПДн нельзя. Как только достигнута цель обработки, персональные данные необходимо уничтожить либо обезличить. Так, например, нельзя хранить в личном деле сотрудника копии паспорта, ИНН, СНИЛС, дипломов, военного билета и т. п. (эти документы хранят в личных делах госслужащих). При проверке инспектор может посчитать это излишнем и выпишет штраф, т. к. цель обработки этих персональных данных (трудоустройство сотрудника) уже достигнута и хранить эти сведения больше нет необходимости.

Уполномоченный орган – федеральный орган исполнительной власти, осуществляющий самостоятельно функции по контролю и надзору за соответствием обработки персональных данных (ст. 23 ФЗ-152). В Российской Федерации их 3:

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Полномочия: защита прав субъектов персональных данных, контроль и надзор за соответствием обработки ПДн требованиям законодательства РФ в области ПДн.

– Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Полномочия: контроль и надзор за организационными и техническими мерами защиты персональных данных.

– Федеральная служба безопасности (ФСБ России) осуществляет контроль и надзор за защитой биометрических персональных данных и криптографическими мерами защиты персональных данных.

1.3. Классификация персональных данных.

Категории персональных данных обозначены в пункте 5 постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – ПП №1119). Всего их 4.

1) Общедоступные персональные данные – «данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей Федерального закона „О персональных данных“». Это могут быть фамилия, имя, отчество, год и место рождения, почтовый адрес, номер телефона, сведения о профессии, месте работы, квалификации, адрес электронной почты.

2) Специальные персональные данные – «данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных», например, рост, вес пациентов, информация о наличии, отсутствии судимостей. Такие сведения находятся в закрытом доступе в отличии от общедоступных. Правила обработки специальных данных регламентированы статьей 10 ФЗ-152.

3) Биометрические персональные данные – «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных». Таковыми являются изображение лица (фото), образцы голоса человека, отпечатки пальцев, генетическая информация, рисунок радужной оболочки глаз и тп., но только в том случае, когда эти данные используются исключительно для идентификации личности. Например, если на проходной установлена камера с распознаванием лиц для идентификации сотрудников. Или в банке установлена система идентификации клиента с помощью отпечатков пальцев. Правила обработки биометрических данных прописаны в статье 11 ФЗ-152.

Также Перечень допустимых случаев обработки биометрии, используемой для идентификации, аутентификации физических лиц в информационных системах организации определен **Постановлением Правительства РФ от 23.10.2021 №1815** (срок действия 01.03.2021 по 01.03.2028).

А в 2022 году принят еще один нормативный акт, в котором обозначены случаи и сроки использования биометрических ПДн, размещенных физическими лицами в единой информационной системе ПДн – Постановление Правительства РФ **от 15.06.2022 №1067** (срок действия с 01.03.2023 по 01.03.2029). Таким образом, биометрические данные обрабатываются в единой системе при аттестации в вузах, оплате товаров и услуг на сумму до 1 000 руб., аутентификации клиентов в финансовых организациях при личном и дистанционном обслуживании, проходе на территорию госорганов и организаций, заключении договоров об оказании услуг связи через Интернет и др.

4) Иные персональные данные – остальные сведения, которые не относятся к трём другим категориям персональных данных, например, данные о заработной плате, стаже, о командировках и отпусках, о членстве в общественных организациях, клубах и тд. Объем и содержание Персональных данных должны соответствовать конкретным целям их обработки. Все персональные данные, независимо от их вида, должны обрабатываться только с согласия субъекта ПДн (его законного представителя) кроме случаев, предусмотренных законом. Контроль и защиту прав субъектов ПДн осуществляют уполномоченные органы РФ (регуляторы). Они проводят плановые и внеплановые проверки операторов (организаций, учреждений).

1.4. Другие федеральные законы в сфере защиты информации и работы с персональными данными

Требования к мерам по защите ПДн регламентирует не только ФЗ 152, но и другие нормативные акты РФ. Рассмотрим основные из них.

В ст. 86 Трудового кодекса Российской Федерации, утвержденного Федеральным законом **от 30.12.2001 N 197-ФЗ** (далее – ТК РФ) содержатся общие требования к работе с ПДн работников и гарантии их защиты. Согласно ТК РФ все персональные данные работника следует получать у него самого, при необходимости работодатель может затребовать ПДн у третьих лиц, но только если нет возможности получить их у самого работника. Перед таким запросом необходимо уведомить этого работника и разъяснить ему последствия отказа дать такое согласие. В уведомлении также обязательно указать цели, источники получения сведений и характер ПДн. Согласно ТК РФ работодатель обязан принимать меры по защите ПДн, разрабатывать соответствующие локальные нормативные акты и знакомить с ними под роспись работников.

Немаловажен в работе с информацией и Федеральный закон от **27.07.2006 №149-ФЗ** «Об информации, информационных технологиях и о защите информации» (далее – ФЗ-149). В нем обозначена основная терминология – понятие информации (конфиденциальной, общедоступной), сайта, поисковой системы и др, прописаны требования к защите информации, порядок ограничения доступа и ответственность за нарушение правил работы с ней. На этот документ ссылаются при составлении локальных нормативных актов по информационной безопасности в организации. В этом законе определяется работа всех информационных систем в российской Федерации, а в статье 14 содержится описание государственных информационных систем (ГИС).

Нельзя не отметить и Федеральный закон «Об электронной подписи» **от 06.04.2011 N 63-ФЗ** (далее – ФЗ-63), который дает ответы на вопросы о том, что такое электронная подпись, как ее использовать и какую юридическую силу она придает электронным документам. Документ определяет технические требования к каждому виду электронных подписей для подтверждения подлинности информации – простой, усиленной квалифицированной и усиленной неквалифицированной (ст. 5 ФЗ-63).

Федеральный закон **«О коммерческой тайне» от 29.07.2004 N 98-ФЗ** (далее – ФЗ-98) вводит понятие коммерческой тайны, а также определяет порядок работы с такого рода информацией и ответственность за нарушение закона.

«**Коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

ФЗ-98 обозначает, какая информация не может относится к коммерческой тайне (например, информация об учредителе или количестве работников).

Организация вправе сама определить сведения, являющиеся коммерческой тайной и должна зафиксировать это в специальном документе – перечне информации, составляющей коммерческую тайну.

Согласно ФЗ-98 уполномоченные гос. органы могут затребовать такие сведения по веским причинам. В этом случае организация обязана предоставить данные.

Обладатель коммерческой тайны обязан защищать ее и вести учет должностных лиц, которые имеют к ней доступ. Лицо, виновное в разглашении такой информации, может быть уволено, оштрафовано или привлечено к уголовной ответственности.

В процессе построения работы с ПДн необходимо учитывать вид деятельности конкретной организации, ее структуру, особенности документооборота, применяемых информационных систем и другие факторы.

Так, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от **26.07.2017 N 187-ФЗ** (далее – ФЗ-187) распространяется на работу организаций, предприятий, которые критически важны для жизни населения Российской Федерации и их простой, сбой в работе может существенно повлиять на безопасность и здоровье граждан. Сюда относятся предприятия топливной, оборонной, металлургической и химической, ракетно-космической промышленности, организации, учреждения в сфере науки, здравоохранения, энергетики транспорта и связи, банки, а также компании, которые обеспечивают работу выше перечисленных организаций (в т. ч. те, кто разрабатывает для них программное обеспечение).

В ст. 2 ФЗ-187 содержатся основные понятия:

«1) **автоматизированная система управления** – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

2) **безопасность критической информационной инфраструктуры** – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

3) **значимый объект критической информационной инфраструктуры** – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

4) **компьютерная атака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

5) **компьютерный инцидент** – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

6) **критическая информационная инфраструктура** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

7) **объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

8) **субъекты критической информационной инфраструктуры** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские

юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей».

ОСНОВНЫЕ ТЕЗИСЫ ФЕДЕРАЛЬНЫХ ЗАКОНОВ О ПЕРСОНАЛЬНЫХ ДАННЫХ И ЗАЩИТЕ ИНФОРМАЦИИ			
ФЗ-152	**ФЗ - 63**	**ФЗ-149**	**ФЗ-187**
- сбор, обработка ПДн субъекта запрещена без его согласия; - ПДн должны обрабатываться оператором только для конкретной цели; - оператор обязан принимать меры по защите персональных данных; – если субъект (владелец) ПДн требует их удалить, оператор обязан это сделать в установленные законодательством сроки; - персональные данные должны храниться и обрабатываться в базах на территории Российской Федерации. При этом данные можно передавать за границу при соблюдении определенных условий, прописанных в законе.	- для создания электронной подписи нет обязанности по использованию конкретного программного обеспечения. Можно применять любые программы и технические средства, обеспечивающие надежность подписи. - подписи бывают простые, усиленные неквалифицированные и усиленные квалифицированные. Самые надежные — усиленные квалифицированные подписи, они делают электронный документ равнозначным бумажному, подписанному собственноручно. – при работе с квалифицированной подписью необходимо держать в тайне ключ подписи; - только специальный удостоверяющий центр имеет право выдавать электронные подписи и сертификаты, подтверждающие их действительность.	- обрабатывать ПДн человека можно только с его согласия; - все информационные технологии равнозначны, у организаций нет обязанности использовать; конкретные технологии для создания информационной системы. - есть информация, ограничивать доступ к которой нельзя (например, сведения о состоянии окружающей среды; – запрещается распространять некоторую информацию (например пропаганду насилия); - тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц; – существует реестр запрещенных сайтов (доменных имен), в который Роскомнадзор может вносить сайты, содержащие информацию, запрещенную к распространению на территории РФ; – оператор (владелец) заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор, после чего его сайт разблокируют.	- существует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), функция которой - защита критической инфраструктуры; - объекты критически важной инфраструктуры обязаны подключиться к ГосСОПКА с помощью установки на предприятии специального программного обеспечения; - одна из мер предупреждения — проверка и сертификация оборудования, программного обеспечения и всей инфраструктуры, которая используется на критически важных предприятиях; - субъекты критической инф. инфраструктуры обязаны сообщать об инцидентах в своих информационных системах и выполнять предписанные требования (например, использовать только сертифицированное программное обеспечение); - все IT-системы критически важных предприятий должны быть защищены от неправомерного доступа и непрерывно взаимодействовать с ГосСОПКА; - при разработке IT-инфраструктуры критически важные предприятия должны руководствоваться требованиями приказа ФСТЭК России от 25.12.2017 № 239; - государство имеет право проверять объекты критически важной инфраструктуры, в том числе внепланово, например, после компьютерных инцидентов вроде взлома или потери информации.

2. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

2.1. Алгоритм построения системы защиты персональных данных в организации

Согласно ст. 19 ФЗ-152 оператор (организация, учреждение) должен защищать обрабатываемые им персональные данные. Важно исключить несанкционированный доступ к сведениям, их утрату или утечку. Для этого в организации необходимо правильно выстроить систему безопасности ПДн, которая зависит от многих факторов: вида деятельности компании, способа обработки данных (автоматизированной, без средств автоматизации или смешенный), категорий обрабатываемых сведений и др. Так, при обработке ПДн в информационных системах ПДн организации необходимо установить уровни защищенности ПДн в зависимости от уровней актуальных угроз с учетом категорий ПДн, выработать организационные и технические меры по их защите и провести ряд мероприятий:

1) Приказом руководителя организации назначается ответственный за обработку и защиту ПДн (его работа осуществляется на основании должностной инструкции). Также создается постоянно действующая комиссия по защите персональных данных из наиболее опытных работников в количестве 3—5 человек (порядок работы, функции и полномочия комиссии прописываются в локальном нормативном акте (положении), который утверждается приказом, также как и ее состав с указанием должностей и ФИО соответствующих работников).

2) Комиссия разрабатывает перечень лиц, допущенных к работе с ПДн, который также утверждается приказом руководителя (в приказе указываются должности и ФИО сотрудников, которые имеют доступ ПДн и обрабатывают их для выполнения своих должностных обязанностей). Эти сотрудники обязаны пройти обучение, инструктаж по работе с ПДн (проводит ответственный по ПДн).

3) Согласно ПП №1119 ответственный по ПДн проводит инвентаризацию информационных систем ПДн в организации (ИСПДн), т. е. определяет перечень оборудования и программного обеспечения (ПО) – в приказе перечисляются назначение каждой ИСПДн и основные цели обработки ПДн (например, для бухгалтерских программ целью будет автоматизация процессов бухгалтерского учета, расчета заработной платы и тп.). Также прописываются категории обрабатываемых персональных данных. В этом же приказе можно установить границы контролируемой зоны ИСПДн, где ответственные лица осуществляют контроль за ПДн и обеспечивают их защиту.

4) Комиссия формирует перечень сведений, в котором перечисляется, какие именно персональные данные обрабатываются для каждой категории субъектов ПДн – работников, клиентов, контрагентов и тд.

5) Комиссия составляет и направляет уведомление в Роскомнадзор об обработке ПДн. Есть возможность отправить документ в электронном виде через сайт ведомства. Образец заполнения и утвержденные формы также можно найти на портале персональных данных Роскомнадзора.

6) Комиссия разрабатывает типовые формы согласий на обработку, распространение ПДн (отдельно для сотрудников, клиентов, пользователей, контрагентов и тд.). Формы согласий разрабатываются на основании ст.9, ст. 10.1, ст. 11 ФЗ-152 приказа Роскомнадзора от 24.02.2021 №18. Если компания (например, интернет-магазин) планирует использовать сайт

для получения согласия на обработку ПДн от пользователей сайта, то необходимо разработать отдельную форму согласия для этой группы субъектов ПДн. В согласиях обязательно указываются сведения об операторе ПДн (организации), цель обработки ПДн, виды данных, а также наименования юр. лиц, ФИО физ. лиц, которым сведения будут передаваться.

Конец ознакомительного фрагмента.