УТВЕРЖДЕНО
Решением Президиума
СРО Ассоциация «НАКС»
Протокол №59
от 22 января 2019 г.

Правила
«Обработка персональных данных при осуществления деятельности членами СРО Ассоциация «НАКС»

1. Термины и определения

Система обработки данных Национального Агентства Контроля Сварки (СОД НАКС) – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и получения информации для достижения целей управления аттестацией сварочного производства и оценки квалификации в области сварки и контроля.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Доступ к информации (в том числе доступ к персональным данным) – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и /или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор персональных данных (Оператор) – юридическое лицо (в контексте данного документа) независимо от организационно-правовой формы, прошедшее проверку соответствия требованиям документов Системы аттестации сварочного производства (САСв) и/или процедуру отбора для выполнения функций центра оценки квалификаций (ЦОК), организующее и/или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных

несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы и стандарты СРО НП «НАКС»:

–ПБ 03-273-99 «Правила аттестации сварщиков и специалистов сварочного производства»;

–РД 03-495-02 «Технологический регламент проведения аттестации сварщиков и специалистов сварочного производства»;

–Рекомендации по применению Правил аттестации сварщиков и специалистов сварочного производства (ПБ 03-273–99) и Технологического регламента проведения аттестации сварщиков и специалистов сварочного производства (РД 03-495–02) (Документы межотраслевого применения по вопросам промышленной безопасности и охраны недр Серия 03 Выпуск 52);

–РД 03-613-03 «Порядок применения сварочных материалов при изготовлении, монтаже, ремонте и реконструкции технических устройств для опасных производственных объектов» и Рекомендации по применению РД 03-613-03 (Документы межотраслевого применения по вопросам промышленной безопасности и охраны недр Серия 03 Выпуск 53);

–РД 03-614-03 «Порядок применения сварочного оборудования при изготовлении, монтаже, ремонте и реконструкции технических устройств для опасных производственных объектов» и Рекомендации по применению РД 03-614-03 (Документы межотраслевого применения по вопросам промышленной безопасности и охраны недр Серия 03 Выпуск 54);

–РД 03-615-03 «Порядок применения сварочных технологий при изготовлении, монтаже, ремонте и реконструкции технических устройств для опасных производственных объектов» и Рекомендации по применению РД 03-615-03 (Документы межотраслевого применения по вопросам промышленной безопасности и охраны недр Серия 03 Выпуск 55);

–Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

–Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

–Указ Президента Российской Федерации от 6 марта 1997 года N 188 «Об утверждении перечня сведений конфиденциального характера».

–Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

–Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

–Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных».

3. Общая информация

На территории Российской Федерации осуществляется государственное регулирование в области обработки и обеспечения безопасности персональных данных (далее - ПДн). Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ 152) и принятых во исполнение его нормативно-правовых актов и методических документов.

При проведении аттестации сварочного производства в соответствии с ПБ 03-273-99 «Правила аттестации сварщиков и специалистов сварочного производства», РД 03-495-02 «Технологический регламент проведения аттестации сварщиков и специалистов сварочного производства», и (или) РД 03-613-03 «Порядок применения сварочных материалов при изготовлении, монтаже, ремонте и реконструкции технических устройств для опасных производственных объектов», и (или) РД 03-614-03 «Порядок применения сварочного оборудования при изготовлении, монтаже, ремонте и реконструкции технических устройств для опасных производственных объектов», и (или) РД 03-615-03 «Порядок применения сварочных технологий при изготовлении, монтаже, ремонте и реконструкции технических устройств для опасных производственных объектов», а также при осуществлении деятельности по независимой оценке квалификации работников или лиц, претендующих на осуществление определенного вида трудовой деятельности в области сварки, Операторы осуществляют обработку персональных данных и, в терминологии Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», являются операторами персональных данных.

Настоящий документ устанавливает правила обработки персональных данных при осуществления деятельности членами СРО Ассоциация «НАКС», а также содержит методические рекомендации, разъясняющие сотрудникам и руководителям Операторов последовательность действий, направленных на обеспечение требований законодательства в области персональных данных.

Правовой основой правил являются: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее ПП 1119), иные нормативные правовые акты РФ, действующие нормативные документы ФСТЭК России, ФСБ РФ, Роскомнадзора РФ.

4. Цели и задачи

−приведение деятельности Операторов по обработке персональных данных в соответствие требованиям ФЗ 152;

−описание единого подхода к обеспечению безопасности персональных данных и приведению ИСПДн Операторов, в соответствие требованиям законодательства;

−установление требований к выполнению регулярных действий по обеспечению требований законодательства в области персональных данных при проведении аттестации сварочного производства и оценки квалификации.

5. Регуляторы, органы контроля и надзора

Государственное регулирование вопросов, связанных с обработкой и с защитой персональных данных, а так же контроль за соответствием обработки требованием законодательства осуществляют три ведомства:

−Роскомнадзор РФ - федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В соответствии с ФЗ 152 Роскомнадзор РФ является Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных». Роскомнадзор обладает правом и компетенциями для контроля исполнения всех статей ФЗ 152, за исключением ст. 19. Роскомнадзор РФ проводит плановые и внеплановые проверки организаций на предмет выполнения требований ФЗ 152.

−ФСТЭК России - федеральный орган исполнительной власти, уполномоченный в области технической защиты информации. Функции ФСТЭК РФ в сфере действия ФЗ 152 приведены в ст. 19 ФЗ 152. В части вопросов обработки ПДн функции ФСТЭК России заключаются в установлении состава и содержания мер к некриптографической защите ПДн при их обработке в ИСПДн.

−ФСБ РФ - федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности. Детально функции ФСБ РФ в сфере действия ФЗ 152 указаны в ст. 19 ФЗ 152. В части вопросов обработки ПДн функции ФСБ РФ заключаются в установлении состава и содержания мер к защите ПДн при их обработке в ИСПДн с применением криптографических средств.

Полномочия этих органов приведены на официальных сайтах этих ведомств.

6. Обязанности Операторов по выполнению требований законодательства в области персональных

Операторы, при обработке ПДн, должны принять меры, направленные на обеспечение требований ФЗ 152 (ст. 18.1 ФЗ 152). Эти меры взаимосвязаны и образуют систему мер (мероприятий), реализация которых обеспечит соблюдение установленных ФЗ 152 «О персональных данных» принципов обработки ПДн.

С точки зрения рисков для Операторов при проведении проверок контрольно-надзорными органами меры разделяются на:

−безусловно обязательные для исполнения (отсутствие мер образует состав правонарушения, с большой вероятностью влечет нарушение прав субъектов ПДн). К таким мерам относится соблюдение принципов, условий обработки, наличие лица, ответственного за обработку, факт направления уведомления в Роскомнадзор, наличие системы защиты персональных данных, ряд других;

−некритичные (отсутствие мер является нарушением нормативных документов, но такое нарушение может быть устранено в ходе проверки и не связано со значительным ущербом для Организации). К таким мерам можно отнести внедрение локальных актов (журнал учета носителей ПДн, положение об уничтожении ПДн и т.п.) либо технические недоработки (например, нарушение периодичности смены паролей доступа).

Меры (мероприятия), направленные на исполнение положений ФЗ 152, разделяют на:

−организационные и правовые меры, направленные на обеспечение надлежащей обработки ПДн;

−организационно-технические меры, направленные на обеспечение безопасности ПДн при их обработке в ИСПДн.

7. Организационные и правовые меры

В соответствии с ч.1 ст. 18.1, ст. 22.1 ФЗ 152, Оператор должен назначить ответственного за организацию обработки ПДн (далее - Ответственный). Работа по приведению деятельности оператора должна осуществляться либо самим Ответственным, либо должна быть Ответственными организована и (или) проконтролирована. Ответственный может не обладать всеми необходимыми для реализации требования ФЗ 152 компетенциями (бухгалтерский учет, кадры, информационные ресурсы, защита информации), поэтому в обязанности Ответственного, в части обеспечения требований ФЗ 152, входит координация деятельности структурных подразделений, задействованных при обработке персональных данных сварщиков и специалистов сварочного производства.

Эффективной организационно-правовой мерой является создание постоянно действующей комиссии из числа работников Оператора, в которую целесообразно включить помимо Ответственного сотрудников кадровой службы, бухгалтерии, ИТ-службы и т.д.

Деятельность Ответственного и комиссии должна быть обеспечена разработкой и внедрением следующих документов:

- Приказ «О введении в действие документов, регламентирующих мероприятия по защите персональных данных».
- Политика обработки персональных данных (далее по тексту - «Политика»).
- Положение об обработке и обеспечении безопасности персональных данных.
- Должностные или рабочие инструкции работников в части обеспечения безопасности персональных данных при их обработке.
- Регламент предоставления прав доступа к персональным данным.
- Регламент для работников по реагированию на запросы субъектов персональных данных, а также на запросы и предписания уполномоченного органа по защите прав субъектов персональных данных.
- Регламент мониторинга и контроля обработки персональных данных.
- Регламент учета съемных носителей персональных данных.
- Порядок распространения персональных данных при их обработке.
- Инструкция о порядке обеспечения конфиденциальности при работе с персональными данными.
- Инструкция по организации парольной защиты.
- Инструкция по проведению антивирусного контроля.
- Инструкция по установке, модификации и техобслуживанию программного обеспечения и аппаратных средств в информационных системах персональных данных.
- Инструкция по порядку хранения, учета и передачи средств криптографической защиты информации в информационных системах.
- Порядок ведения журнала посетителей.
- Формы согласий на обработку персональных данных.
- Форма договора поручения на обработку персональных данных.

При разработке документов, регламентирующих обработку персональных данных в АЦ, необходимо руководствоваться терминами и определениями данного стандарта СРО Ассоциация «НАКС».

7.1. Правила составления политики в отношении обработки персональных данных

В соответствии с ч.2 ст. 18.1 ФЗ 152, 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». Политика обработки персональных данных должна соответствовать рекомендациям Роскомнадзора 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» (опубликовано 27 июля 2017 года на сайте http://rkn.gov.ru).

Политика Оператора должна исключать обработку специальных категорий персональных данных и биометрических персональных данных сварщиков и специалистов сварочного производства (ст.10-11 ФЗ 152).

Политика в форме документа должна быть публичной – размещена на сайте Оператора.

7.2. Уведомление в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор РФ) «Об обработке ПДн».

Направление уведомления является обязанностью любой организации – оператора ПДн (ст.22 ФЗ 152). В законе определены (ст.22) условия, при которых организация не обязана направлять Уведомление. В отношении Операторов в контексте данного документа эти условия не применимы. Неисполнение требований ФЗ 152 в части направления Уведомления (отсутствие Уведомления) для Оператора образует состав административного правонарушения.

Подготовка и направление Уведомления осуществляется в порядке и форме, указанными в рекомендациях Роскомнадзора (см. перечень нормативной базы). Содержание Уведомления не должно противоречить соответствующим пунктам Политики в отношении обработки ПДн и Положения об обработке ПДн. Заполнение формы электронного уведомления возможно на официальном сайте Роскомнадзора. В этом случае после заполнения формы уведомления и отправки ее в информационную систему Роскомнадзора необходимо распечатать заполненную форму, после чего ее подписать и направить в соответствующий территориальный орган Роскомнадзора по месту регистрации Оператора.

Уведомление рассматривается территориальным органом Роскомнадзора РФ. На его официальном сайте обеспечена возможность для проверки состояния уведомления, поданного в электронном виде на Портале персональных данных. Результатом рассмотрения является включение Оператора в реестр операторов персональных данных. Этот реестр является открытым и доступен на сайте Роскомнадзора РФ.

7.3. Обеспечение конфиденциальности ПДн при их обработке Операторами

Обеспечение конфиденциальности ПДн является обязанностью организации (ст. 7 ФЗ 152). Оператор должен распространить требование о соблюдении режима конфиденциальности как на своих работников, имеющих отношение к обработке ПДн, так и на иных лиц, привлекаемых к обработке ПДн на основании гражданско-правовых договоров. Обеспечение конфиденциальности должно выполняться в соответствии с разработанной Оператором инструкцией о порядке обеспечения конфиденциальности при работе с персональными данными.

7.4. Передача ПДн для обработки третьему лицу

Деятельность Операторов зачастую связана с необходимостью передачи ПДн третьим лицам. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных. В этом случае возникает обязанность (ч.3 ст. 6 ФЗ 152) оператора формализовать ряд требований к третьему лицу в форме Поручения. В Поручении должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки; должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 ФЗ 152.

С момента подачи уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных, необходимо заключать соглашение о передаче ПДн для обработки третьему лицу с каждой организацией, которой Оператор передает персональные данные.

7.5. Согласие субъекта ПДн на обработку его ПДн

Получение согласия субъекта ПДн является одним из условий обработки ПДн (п.1 ч.1 ст. 6 ФЗ 152). Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным (ст. 9 ФЗ 152). Согласие должно быть дано субъектом ПДн в письменной форме при обработке заявок на бумажном носителе, в электронной форме при обработке заявок в системе документооборота ЭДО. Обязанность доказывания наличия письменного согласия возлагается на Оператора.

При подготовке форм письменных согласий персональных данных необходимо определить категории субъектов персональных данных и категории персональных данных для каждого субъекта.

К категориям субъектов ПДн относятся:

- работники Оператора, с которыми заключен трудовой договор;
- иные субъекты ПДн, которые вступили в правовые отношения с Оператором, либо субъекты ПДн, чьи ПДн Оператор намерен обрабатывать с какой-либо обоснованной законной целью.

Согласие в письменной форме может быть включено в состав уже имеющихся документов путем составления к ним дополнительного соглашения, таких как трудовой договор, гражданско-правовой договор, договор об оказании услуг и т.п., либо может быть оформлено как отдельный документ (Согласие на обработку ПДн).

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных в соответствии со ст. 9 Федерального закона №152-ФЗ должно содержать:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

−наименование Оператора, получающего согласие субъекта персональных данных;

−цель обработки персональных данных;

−перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

−перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

−срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

−подпись субъекта персональных данных либо его законного представителя.

Данные указанные в согласии в письменной форме субъекта персональных данных на обработку его персональных данных должны совпадать с данными указанными в локальных актах Оператора регламентирующих обработку персональных данных и в уведомлении об обработке персональных данных

Обработка ПДн в случаях, не предусмотренных законодательством РФ, обработка ПДн, несовместимая с целями сбора ПДн запрещена. Не допускается в одно согласие включать несколько целей обработки ПДн.

7.6. Предоставление прав доступа к информационным системам персональных данных (ИСДПн)

Предоставление прав доступа к ИСПДн является элементом политики информационной безопасности Оператора. Права доступа должны быть определены в регламенте предоставления прав доступа к персональным данным. Лицом, которое отвечает за реализацию регламента, является Администратор по информационной безопасности (Администратор ИБ - назначенный приказом Оператора сотрудник. Эту должность может совмещать Ответственный). Документ необходим Ответственному, Администратору ИБ, при расследовании инцидентов ИБ, при проведении проверок. Регламент должен содержать:

−наименование ресурсов, к которым разрешен доступ (наименование ИСПДн, элемента ИСПДн, каталога, раздела, диска, сервера, программы, устройства, базы данных и т.п.),

−тип доступа (права, полномочия на проведение операций - чтение, изменение, уничтожение и т.п.), а также субъекты доступа (указание должностей из номенклатуры Организации - Администратор №1, №2, Пользователи №№1,2,3 и т.д).

−иные условия, ограничения (время доступа, период доступа и т.п.).

7.7. Порядок действий при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Федеральный закон «О персональных данных» устанавливает (ст. 20 ФЗ 152) обязанности Организации (оператора ПДн) при обращении субъекта ПДн и при обращении Уполномоченного органа по защите прав субъекта персональных данных (Роскомнадзор РФ). Неисполнение этих обязанностей влечет за собой нарушение прав субъекта персональных данных и риск привлечения Оператора к ответственности. По этой причине должен быть разработан Регламент для работников Оператора по реагированию на запросы субъектов персональных данных, а также на запросы и предписания уполномоченного органа по защите прав субъектов персональных данных.

Регламент должен содержать детальное описание действий определенных подразделений, сотрудников Оператора при поступлении обращения (запроса, жалобы) субъектов ПДн и Роскомнадзора. С точки зрения субъекта персональных данных все эти действия будут являться действиями Оператора. Под такими действиями могут подразумеваться как действия с ПДн (уничтожение, блокирование ПДн), так и иные действия Оператора (удовлетворение жалобы, отказ в удовлетворении жалобы, отсутствие ответа на обращение, письменные разъяснения и т.п). Регламент устанавливает форму и сроки выполнения каждой процедуры при обращении субъекта ПДн. Отсутствие в установленные сроки ответа Оператора при обращении субъекта ПДн образует состав административного правонарушения. Прием и обработка запросов субъектов ПДн являются обязанностью Ответственного. Исполнение регламента реализуется Ответственным за организацию обработки ПДн, назначенным Оператором приказом.

7.8. Осуществление внутреннего контроля (аудита) соответствия обработки ПДн требованиям законодательства и политике оператора в отношении обработки ПДн.

Обязанности контроля (аудита) предусмотрены п.4 ч.1 ст. 18.1 ФЗ 152. Сферами контроля являются:

−соответствие обработки персональных данных Федеральному закону №152-ФЗ и принятым в соответствии с ним нормативным правовым актам;

−соответствие обработки ПДн требованиям к защите персональных данных;

−соответствие обработки ПДн политике оператора в отношении обработки персональных данных, локальным актам оператора.

Контрольные функции находятся в компетенции Ответственного за организацию обработки ПДн и Администратора ИБ Оператора и выполняются на регулярной основе.

7.9. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения закона «О персональных данных»

С точки зрения логики нормативно-правовых актов оценка вреда может быть проведена только после моделирования угроз безопасности ПДн и определения уровня защищенности ИСПДн. Однако, исходя из требуемых компетенций, роли и места этого документа в системе документарного обеспечения, Акт может быть отнесен к документам не технического, а организационно-правового характера, потому он рассматривается в настоящем разделе.

Обязанность по оценке вреда возложена на Оператора п.5 ч.1 ст. 18.1 ФЗ 152. Наличие оценки вреда (Акта оценки вреда) обязательно, требований к форме документа по оценке вреда не устанавливается.

При оценке вреда Оператор обязан соотнести указанный вред и принимаемые меры, направленные на обеспечение выполнения обязанностей, предусмотренных ФЗ 152. Это означает, что для каждого вида предполагаемого вреда должны быть рассмотрены компенсирующие (предотвращающие) меры (организационные, правовые, технические).

Также следует оценить достаточность этих мер. Такая работа осуществляется исключительно экспертным, а не формальным методом, и находится в компетенции постоянно действующей Комиссии Оператора или Ответственного (при отсутствии Комиссии). Для оценки вреда рекомендуется привлекать на договорной основе компетентные организации, имеющие соответствующие разрешительные документы, лицензии и сертификаты.

В Акте оценке вреда должен быть рассмотрен вред для разных категорий субъектов ПДн (например, работников Оператора, иных лиц). Должны быть рассмотрены все виды нарушений, которые могут явиться следствием неисполнения Организацией своих

обязанностей в рамках ФЗ 152, а именно:

−нарушения принципов и условий обработки ПДн;

−нарушения прав субъекта;

−нарушения обязанностей оператора.

Детализация этих нарушений выражается в:

−незаконной и несправедливой основе обработки ПДн;

−отсутствии согласия субъекта ПДн на обработку ПДн;

−нарушение требований к форме согласия субъекта ПДн;

−несоблюдение требований к согласиям субъекта ПДн в письменной форме;

−получение согласия на обработку персональных данных от представителя субъекта без проверки полномочий представителя;

−нарушении конфиденциальности при обработке ПДн;

−отсутствии ответственности третьего лица перед оператором при передаче ПДн для обработки;

−обработке специальных категорий ПДн без согласия субъекта ПДн;

−нарушении прав субъекта на получение информации, касающейся обработки его ПДн;

−нарушении прав субъекта по уточнению, блокированию, уничтожению своих ПДн;

−нарушении обязанностей оператора при сборе ПДн;

−отсутствии мер, направленных на выполнение оператором обязанностей, предусмотренных ФЗ 152;

−отсутствии мер по обеспечению безопасности ПДн.

Рассматриваются имущественный и моральный вред. Вводится оценочный показатель, который целесообразно указать как:

−высокая степень (вред выражается в значительных негативных последствиях для субъекта персональных данных);

−средняя степень (вред выражается в негативных последствиях для субъекта персональных данных);

−низкая степень (вред выражается в незначительных негативных последствиях для субъекта персональных данных);

−незначительный вред или отсутствует (вред отсутствует или его последствия для субъекта ничтожно малы).

В акте указываются члены Комиссии Оператора (или Ответственный, при отсутствии Комиссии). Подписанный Акт оценки вреда утверждается руководителем Организации.

8. Организационно-технические меры, направленные на обеспечение безопасности ПДн при их обработке в ИСПДн

Деятельность Оператора в части обеспечения безопасности ПДн осуществляется на основании постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных». Основная задача при исполнении данных требований – определение актуальных угроз безопасности ПДн с учетом оценки возможного вреда субъекту ПДн. Определение актуальных угроз осуществляется при помощи методик, изложенных в руководящих документах ФСТЭК России (см. нормативную базу) и проводится силами сотрудников Оператора или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Требования к защите информации исполняются в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Цель Приказа № 21 – обеспечить безопасность ПДн при их обработке в ИСПДн.

Таким образом, последовательность работ на этом этапе такова:

- определение актуальных угроз;
- оценка вреда;
- установление состава и содержания мер по обеспечению безопасности ПДн;
- реализация мер;
- оценка эффективности реализованных мер.

На данном этапе работы под мерами подразумевается меры организационно-технического характера. В их состав входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

В документарном смысле результатом этого этапа должны являться следующие локальные акты организации:

- Модель угроз безопасности ПДн при их обработке в ИСПДн;
- Акт оценки уровня защищенности ПДн при их обработке в ИСПДн;
- должностные или рабочие инструкции работников в части обеспечения безопасности персональных данных при их обработке Оператором;
- регламент учета съемных носителей персональных данных, обрабатываемых Оператором;
- инструкция по порядку хранения, учета и передачи средств криптографической защиты информации в информационных системах.

8.1. Модель угроз безопасности ПДн при их обработке в ИСПДн.

Модель угроз безопасности ПДн подготавливается для каждой ИСПДн Оператора в соответствии с руководящими документами ФСТЭК России (см. нормативную базу). Оценка и моделирование угроз осуществляется силами сотрудников центра (при наличии такой возможности) либо с привлечением специалистов в сфере защиты информации. Определение типа актуальных угроз проводится с учетом оценки возможного вреда субъекту ПДн. Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к

персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Содержание документа относится к сведениям ограниченного доступа.

8.2. Оценка уровня защищенности ПДн при их обработке в ИСПДн.

Уровень защищенности устанавливается в соответствии с требованиями, утвержденными Постановлением Правительства РФ № 1119 от 01.11.2012г.

Задачей Оператора является внедрение организационно-технических мер, которые будут необходимы и достаточны для нейтрализации установленных актуальных угроз и соответствовать установленному уровню защищенности. Важно понимать, что понятие «уровень защищенности» относится не к ИСПДн, а к обрабатываемым в ИСПДн ПДн.

Оценка уровня защищенности осуществляется силами Комиссии с привлечением экспертов в данной предметной области. В Акте указывается установленный уровень защищенности в отношении каждой ИСПДн.

8.3. Обеспечение безопасности персональных данных при их обработке Операторами

В соответствии с установленным уровнем защищенности, Оператор реализует технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Обеспечение безопасности, в соответствии с 152-ФЗ достигается:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных (ПП 1119 от 01.11.2012г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных");
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (в соответствии с Приказом ФСТЭК №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

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

9. Заключительные положения

Последовательность, состав и содержание перечисленных мер (мероприятий), названия, содержание, очередность внедрения организационно-распорядительных документов могут изменяться в зависимости от:

−организационно-правовой формы Организации (оператора ПДн);

−критичности обрабатываемых ПДн (сведения о состоянии здоровья, биометрические ПДн);

−объема обрабатываемых ПДн (менее 100 000 / более 100 000);

−особенностей бизнес-процессов, влияющих на обработку ПДн.

Работу по приведению деятельности Организации в соответствие с требованиями ФЗ 152 следует начинать с изучения основных положений Закона и иных нормативных актов. Практика показывает, что наиболее эффективным способом овладения необходимыми знаниями является обучение в специализированных организациях. При том необходимо помнить о двух различных компетенциях, которые потребуются Оператору:

−лицо, ответственное за обработку ПДн;

−специалист по защите информации.

Обучение Ответственного за организацию обработки ПДн необходимо проводить в лицензированных образовательных учреждениях, имеющих соответствующую образовательную программу дополнительного профессионального образования.

Обучение специалиста по защите информации необходимо в случае, если такой специалист не имеет базового высшего образования в сфере защиты информации. В этом случае достижение необходимой компетенции обеспечивается направлением такого работника в лицензированное образовательное учреждение для обучения по программам дополнительного профессионального образования. Помимо лицензии для образовательного учреждения обязательным является факт согласования такой программы со ФСТЭК России.

В случаях, когда обучение собственных специалистов Оператора невозможно, допускается привлечение на договорной основе экспертов в данной предметной области в качестве консультантов.