САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ
АССОЦИАЦИЯ
«НАЦИОНАЛЬНОЕ АГЕНТСТВО
КОНТРОЛЯ СВАРКИ»

Стандарт саморегулируемой организации

Деятельность саморегулируемой организации

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

СТО НАКС 1.2–2020

Издание официальное

Москва
2020

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Саморегулируемой организацией Ассоциация «Национальное Агентство Контроля Сварки» (СРО Ассоциация «НАКС»).

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Решением Президиума СРО Ассоциация «НАКС» от 21 января 2020 г., протокол № 63.

3 ВЗАМЕН «Методических рекомендаций по выполнению требований законодательства в области персональных данных при проведении аттестации сварочного производства» (утв. Решением НТС НАКС от 17 декабря 2014 г., протокол № 31) и Правил «Обработка персональных данных при осуществлении деятельности членами СРО Ассоциация «НАКС» (утв. Решением Президиума СРО Ассоциация «НАКС» от 22 января 2019 г., протокол № 59) .

Содержание

САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ АССОЦИАЦИЯ «НАЦИОНАЛЬНОЕ АГЕНТСТВО КОНТРОЛЯ СВАРКИ»

Деятельность саморегулируемой организации
Обработка персональных данных

Дата введения — 2020—01—21

1 Область применения

Настоящий стандарт применяется членами Саморегулируемой организации Ассоциация «Национальное Агентство Контроля Сварки» и устанавливает последовательность действий, направленных на обеспечение защиты персональных данных при осуществлении деятельности по аттестации персонала сварочного производства и оценке квалификации.

2 Нормативные ссылки

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

Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»

Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

3 Термины и определения

В настоящем стандарте применены термины и определения, приведенные в ПР НАКС 1.1 «Деятельность саморегулируемой организации. Положение о НАКС», СТО НАКС 1.1 «Деятельность саморегулируемой организации. Система обработки данных», а также следующие термины с соответствующими определениями.

3.1 **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.

3.2 **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.

3.3 **блокирование персональных данных**: Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

3.4 **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.

3.5 **информационная система персональных данных:** 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.

3.6 **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.

3.7 **несанкционированный доступ (несанкционированные действия):** Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

3.8 **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.

3.9 **оператор персональных данных:** Член НАКС, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

3.10 **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.

3.11 **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.

3.12 **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.

4 Обозначения и сокращения

НАКС - Саморегулируемая организация Ассоциация «Национальное Агентство Контроля Сварки»

ИСПДн - информационная система персональных данных

ПДн - персональные данные

ЭДО - электронный документооборот

5 Общие положения

5.1 На территории Российской Федерации осуществляется государственное регулирование в области обработки и обеспечения безопасности персональных данных. Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ 152) и принятых во исполнение его нормативно-правовых актов и методических документов.

5.2 Государственное регулирование вопросов, связанных с обработкой и защитой персональных данных, контроль за соблюдением требований законодательства осуществляют:

– 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 ФЗ 152. 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;

– Федеральная инспекция труда - федеральный орган исполнительной власти, осуществляющий надзор за соблюдением трудового законодательства, в частности контроль за требованиями главы 14 [1];

– ФСТЭК РФ - 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.

5.3 При осуществлении деятельности по аттестации или оценки квалификации, члены НАКС осуществляют обработку персональных данных и, согласно ФЗ 152, являются Операторами персональных данных.

5.4 Настоящий стандарт разработан в целях установления единого подхода к обеспечению безопасности персональных данных и приведению ИСПДн Операторов в соответствие с требованиями законодательства в области защиты персональных данных.

6 Обязанности Операторов

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

6.2 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).

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

– организационные и правовые, направленные на обеспечение надлежащей обработки ПДн;

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

7 Организационные и правовые меры

7.1 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 им 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. С целью организации работ по обеспечению безопасности персональных данных при работе с помощью средств автоматизации в ИСПДн Оператор назначает Администратора информационной безопасности (далее Администратор ИБ). Функции Администратора ИБ может выполнять внешнее гражданское лицо по договору гражданско-правового характера.

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

7.3 Деятельность Ответственного, Администратора ИБ и комиссии должна быть обеспечена разработкой и внедрением следующих документов:

– приказ о назначении ответственных лиц;

– должностные и (или) рабочие инструкции сотрудников в части обеспечения безопасности персональных данных при их обработке;

– приказ о введении в действие документов, регламентирующих мероприятия по защите персональных данных;

– политика в отношении обработки персональных данных;

– положение об обработке и обеспечении безопасности персональных данных;

– регламент предоставления прав доступа к персональным данным;

– регламент для работников по реагированию на запросы субъектов персональных данных, а также на запросы и предписания органов государственной власти по вопросам защиты и обработки персональных данных;

– регламент мониторинга и контроля обработки персональных данных;

– регламент учета съемных носителей персональных данных;

– порядок распространения персональных данных;

– инструкцию о порядке обеспечения конфиденциальности при работе с персональными данными в информационных системах;

– инструкцию по организации парольной защиты;

– инструкцию по проведению антивирусного контроля;

– инструкцию по установке, модификации и техобслуживанию программного обеспечения и аппаратных средств в информационных системах персональных данных;

– инструкцию по порядку хранения, учета и передачи средств криптографической защиты информации в информационных системах;

– порядок ведения журнала посетителей[1];

– шаблоны письменных Согласий на обработку персональных данных;

– модель угроз безопасности персональных данных в информационной системе персональных данных;

– акт оценки вреда, который может быть причинен субъектам персональных данных;

– оценка эффективности реализованных мер;

– уведомление об обработке (о намерении (о намерении осуществлять обработку) персональных данных.

7.4 Политика обработки персональных данных.

[1] Разрабатывается в случае установленного пропускного режима Оператора

7.4.1 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 ее составлению.

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

7.5 Положение об обработке и обеспечении безопасности персональных данных, разрабатывается в соответствии со ст. 18.1 ФЗ 152, определяет порядок обработки персональных данных и устанавливает общие требования к обеспечению безопасности ПДн, обрабатываемых Оператором.

7.6 Уведомление об обработке (о намерении осуществлять обработку) персональных данных (далее Уведомление) в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор РФ).

7.6.1 Направление Уведомления является обязанностью Оператора ПДн. Неисполнение требований ФЗ 152 в части направления Уведомления (отсутствие Уведомления) для Оператора образует состав административного правонарушения.

7.6.2 Подготовка и направление Уведомления осуществляется в порядке и форме, указанными в рекомендациях Роскомнадзора. 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 на официальном бланке Оператора, после чего ее подписать и направить в соответствующий территориальный орган Роскомнадзора по месту регистрации Оператора.

7.6.3 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.

7.6.4 Уведомление должно содержать достоверные, полные и актуальные сведения. Для внесения изменений в Уведомление Оператором оформляется Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных (далее Информационное письмо). Подготовка и направление Информационного письма осуществляется в порядке и форме аналогичной подаче

Уведомления, установленной п. 7.6.2 и п. 7.6.3 настоящего стандарта.

7.7 Обеспечение конфиденциальности ПДн при их обработке Операторами является обязанностью организации (ст. 7 ФЗ 152). Оператор должен распространить требование о соблюдении режима конфиденциальности как на своих сотрудников, 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.

7.8 Передача ПДн для обработки третьему лицу.

7.8.1 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. Передача персональных данных третьим лицам осуществляется в соответствии с разработанным Оператором порядком распространения персональных данных.

7.8.2 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.

7.9 Согласие субъекта ПДн на обработку его ПДн.

7.9.1 Получение согласия субъекта ПДн является одним из условий обработки ПДн (п.1 ч.1 ст. 6 ФЗ 152). Согласие на обработку ПДн должно быть конкретным, информированным и сознательным (ст. 9 ФЗ 152). Обязанность доказывания наличия письменного согласия возлагается на Оператора.

7.9.2 При подготовке форм письменных согласий ПДн необходимо определить категории субъектов ПДн и категории ПДн для каждого субъекта.

7.9.3 К категориям субъектов ПДн относятся:

– сотрудники 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.

7.9.4 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).

7.9.5 Согласие в письменной форме субъекта ПДн на обработку его ПДн в соответствии со ст. 9 ФЗ 152 должно содержать:

– фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество, адрес представителя субъекта ПДн, 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 ПДн);

– наименование Оператора, получающего согласие субъекта ПДн;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие субъекта персональных данных;

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

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов ПДн;

– срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено ФЗ 152;

– подпись субъекта ПДн либо его законного представителя.

7.9.6 Данные субъекта ПДн на обработку его ПДн, указанные в согласии в письменной форме, должны совпадать с данными, указанными в локальных актах Оператора регламентирующих обработку ПДн и в уведомлении об обработке ПДн.

7.9.7 Обработка ПДн в случаях, не предусмотренных ФЗ 152, обработка ПДн, несовместимая с целями сбора ПДн, запрещена. Не допускается в одно согласие включать несколько целей обработки ПДн.

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

7.10.1 Предоставление прав доступа к ИСПДн является элементом политики информационной безопасности Оператора. Права доступа должны быть определены в регламенте предоставления прав доступа к ПДн.

7.10.2 Регламент необходим при расследовании инцидентов ИБ, при проведении проверок. 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.).

7.11 Порядок действий при обращении либо при получении запроса субъекта ПДн или его законного представителя, а также уполномоченного органа по защите прав субъектов ПДн

7.11.1 Ст. 20 ФЗ 152 устанавливает обязанности Оператора при обращении субъекта ПДн и при обращении Уполномоченного органа по защите прав субъекта ПДн (Роскомнадзор РФ). Неисполнение этих обязанностей влечет за собой нарушение прав субъекта ПДн и риск привлечения Оператора к ответственности. По этой причине должен быть разработан Регламент для сотрудников Оператора по реагированию на запросы субъектов ПДн, а также на запросы и предписания уполномоченного органа по защите прав субъектов ПДн.

7.11.2 Регламент должен содержать детальное описание действий определенных подразделений, сотрудников Оператора при поступлении обращения (запроса, жалобы) субъектов ПДн и Роскомнадзора. С точки зрения субъекта ПДн 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.

7.12 Осуществление внутреннего контроля (аудита) соответствия обработки ПДн

требованиям законодательства и политике оператора в отношении обработки ПДн.

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

– соответствие обработки ПДн требованиям ФЗ 152 и принятым в соответствии с ним нормативным правовым актам;

– соответствие обработки ПДн требованиям к защите ПДн;

– соответствие обработки ПДн политике оператора в отношении обработки ПДн, локальным актам Оператора.

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

7.13 Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения закона ФЗ 152.

7.13.1 Обязанность по оценке вреда возложена на Оператора согласно 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.

7.13.2 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) и оценена достаточность этих мер.

7.13.3 Оценка вреда 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.

7.13.4 В Акте оценке вреда должен быть рассмотрен вред для разных категорий субъектов ПДн (например, сотрудников 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.

7.13.5 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 ПДн 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.

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

– высокая степень (вред выражается в значительных негативных последствиях для субъекта ПДн);

– средняя степень (вред выражается в негативных последствиях для субъекта ПДн);

– низкая степень (вред выражается в незначительных негативных последствиях для субъекта ПДн);

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

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

8 Организационно-технические меры

8.1 Деятельность Оператора в части обеспечения безопасности ПДн осуществляется на основании постановления Правительства Российской Федерации [2]. 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 [3] - [5], 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.

8.2 Требования к защите информации исполняются в соответствии с Приказом ФСТЭК России [3], цель которого обеспечить безопасность ПДн при их обработке в ИСПДн.

8.3 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.

8.4 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 ПДн (далее - машинные носители ПДн);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПДн;
- обеспечение целостности информационной системы и ПДн;
- обеспечение доступности ПДн;
- 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 ПДн (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты ПДн.

8.5 В документарном смысле результатом этого этапа должны являться следующие

локальные акты организации:

– модель угроз безопасности ПДн при их обработке в ИСПДн;

– акт оценки вреда, который может быть причинен субъектам персональных данных;

– оценка эффективности реализованных мер;

– должностные или рабочие инструкции сотрудников в части обеспечения безопасности ПДн при их обработке Оператором;

– регламент учета съемных носителей ПДн, обрабатываемых Оператором;

– инструкция по порядку хранения, учета и передачи средств криптографической защиты информации в информационных системах;

– 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.

8.6 Модель угроз безопасности ПДн при их обработке в ИСПДн подготавливается для каждой ИСПДн Оператора в соответствии с руководящими документами ФСТЭК [4]. Оценка и моделирование угроз осуществляется силами сотрудников Оператора (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.

8.7 Оценка уровня защищенности ПДн при их обработке в ИСПДн устанавливается в соответствии с требованиями, утвержденными Постановлением Правительства РФ [2]. Задачей Оператора является внедрение организационно-технических мер, которые будут необходимы и достаточны для нейтрализации установленных актуальных угроз и соответствовать установленному уровню защищенности. Оценка уровня защищенности осуществляется силами Комиссии или Ответственного с привлечением экспертов в данной области. В Акте указывается установленный уровень защищенности в отношении каждой ИСПДн.

8.8 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 ФЗ 152 достигается:

- определением угроз безопасности ПДн при их обработке в информационных системах ПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн [2];
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации в соответствии с [3];
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

9 Заключительные положения

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

- организационно-правовой формы 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.

Библиография

[1] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ ;

[2] Постановление Правительства Российской Федерации от 01.11.2012 № 1119 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

[3] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

[4] «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена ФСТЭК РФ 15.02.2008 года)

[5] «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена ФСТЭК 14.02.2008 года)