САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ
АССОЦИАЦИЯ
«НАЦИОНАЛЬНОЕ АГЕНТСТВО
КОНТРОЛЯ СВАРКИ»

Стандарт саморегулируемой организации

Деятельность саморегулируемой организации

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

СТО НАКС 1.2–2023

Издание официальное

Москва
2023

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 31 мая 2023 г., протокол № 82.

3 ВЗАМЕН СТО НАКС 1.2-2020 Обработка персональных данных (утв. Решением Президиума СРО Ассоциация «НАКС» от 21 января 2020 г., протокол № 63).

Содержание

САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ АССОЦИАЦИЯ «НАЦИОНАЛЬНОЕ АГЕНТСТВО КОНТРОЛЯ СВАРКИ»

Деятельность саморегулируемой организации Обработка персональных данных

Дата введения — 2023—06—01

1 Область применения

Настоящий стандарт применяется членами Саморегулируемой организации Ассоциация «Национальное Агентство Контроля Сварки» и устанавливает перечень мер, направленных на обеспечение защиты персональных данных при осуществлении деятельности по аттестации, сертификации и оценке квалификации.

2 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.

2.1 **персональные данные:** Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

2.2 **персональные данные, разрешенные субъектом персональных данных для распространения:** Персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3 **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.

2.4 **специальные персональные данные**: Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

2.5 **оператор:** 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.

2.6 **обработка персональных данных:** Действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7 **распространение персональных данных:** Действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.8 **предоставление персональных данных:** Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.9 **блокирование персональных данных:** Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.10 **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.

2.11 **обезличивание персональных данных**: Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.12 **информационная система персональных данных:** Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

2.13 **трансграничная передача персональных данных:** Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.14 **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.

2.15 **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.

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

2.17 **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.

2.18 **уровень защищенности персональных данных:** Комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3 Обозначения и сокращения

НАКС - Саморегулируемая организация Ассоциация «Национальное Агентство Контроля Сварки»;

ИСПДн - информационная система персональных данных.

4 Общие положения

4.1 На территории Российской Федерации осуществляется государственное регулирование вопросов, связанных с обработкой и защитой персональных данных, в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации от 30.12.2001 г. №197-ФЗ (далее – ТК РФ) [1], Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) [2], иными нормативными правовыми актами Российской Федерации и нормативными правовыми актами федеральных органов исполнительной власти Российской Федерации [3] - [11].

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

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В соответствии с Законом о персональных данных Роскомнадзор является Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Закона о персональных данных. Роскомнадзор обладает правом и компетенциями для контроля исполнения всех статей Закона о персональных данных. Роскомнадзор проводит плановые и внеплановые проверки организаций на предмет выполнения требований Закона о персональных данных, а так же имеет иные права, установленные Законом о персональных данных;

– Федеральная служба по труду и занятости (Роструд) - федеральный орган исполнительной власти, осуществляющий надзор за соблюдением трудового законодательства, в частности контроль за требованиями главы 14 ТК РФ [1];

– Федеральная служба по техническому и экспортному контролю (ФСТЭК) - федеральный орган исполнительной власти, уполномоченный в области технической защиты информации. ФСТЭК осуществляет контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных ст. 19 Закона о персональных данных, в рамках своей компетенции;

– Федеральная служба безопасности (ФСБ) - федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности. ФСБ осуществляет контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных ст. 19 Закона о персональных данных, в рамках своей компетенции.

4.3 При осуществлении деятельности по аттестации, сертификации или оценки квалификации члены НАКС осуществляют обработку персональных данных и, согласно Закону о персональных данных, являются Операторами персональных данных.

4.4 При осуществлении деятельности по аттестации, сертификации или оценки квалификации Операторы не осуществляют обработку биометрических персональных данных субъектов персональных данных.

4.5 Настоящий стандарт разработан в целях установления единого подхода к обеспечению безопасности персональных данных Операторов в соответствии с

требованиями законодательства Российской Федерации в области защиты персональных данных.

5 Обязанности Оператора

5.1 При обработке персональных данных, осуществляемой без использования средств автоматизации, Оператор обязан исполнять требования, установленные Правительством Российской Федерации [11].

5.2 Оператор, при сборе персональных данных, обязан исполнять требования, установленные ст. 18 Закона о персональных данных.

5.3 Оператор, при обработке персональных данных, должен принять меры, направленные на обеспечение требований, установленных ст. 18.1, ст.19 Закона о персональных данных. Эти меры взаимосвязаны и образуют систему мер (мероприятий), реализация которых обеспечит соблюдение установленных Законом о персональных данных принципов обработки персональных данных.

5.4 Меры (мероприятия), направленные на исполнение положений Закона о персональных данных, разделяют на:

– меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

– меры, направленные на обеспечение безопасности персональных данных.

5.5 Оператор при обращении субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных обязан выполнять требования, установленные ст. 14, ст. 20 Закона о персональных данных.

5.6 В случае нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных Оператор обязан принять меры, установленные ст. 21 Закона о персональных данных.

5.7 Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Требования к уведомлению об обработке персональных данных установлены ст. 22 Закона о персональных данных.

5.8 В случае трансграничной передачи персональных данных Оператор обязан исполнять требования ст. 12 Закона о персональных данных.

6 Меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных

6.1 В соответствии с пунктом 1 части 1 статьи 18.1 Закона о персональных данных, Оператор должен назначить ответственного за организацию обработки персональных данных (далее - Ответственный). Обязанности Ответственного установлены ст. 22.1 Закона о персональных данных. Работа по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области обработки и защиты персональных данных должна осуществляться либо самим Ответственным, либо должна быть им организована и проконтролирована.

6.2 В соответствии с пунктом 2 части 1 ст. 18.1 Закона о персональных данных, Оператор должен издать документы, определяющие политику в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

6.3 В соответствии с пунктом 4 части 1 ст. 18.1 Закона о персональных данных, Оператор должен осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

6.4 В соответствии с пунктом 5 части 1 ст. 18.1 Закона о персональных данных, Оператор должен провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.

6.5 С целью исполнения требований, указанных в п. 5, п. 6.1-6.4 Оператор обязан издать следующие локальные акты:

6.5.1 Приказ о назначении ответственного лица за организацию обработки персональных данных.

6.5.2 Должностная или рабочая инструкция ответственного лица за организацию обработки персональных данных.

Должностная или рабочая инструкция ответственного лица за организацию обработки персональных данных должна устанавливать права, обязанности, в том числе обязанности,

установленные ст. 22.1 Закона о персональных данных, и ответственность ответственного лица за организацию обработки персональных данных.

6.5.3 Приказ о создании комиссии по обеспечению защиты персональных данных.

6.5.4 Положение о комиссии по обеспечению защиты персональных данных.

Положение о комиссии по обеспечению защиты персональных данных должно устанавливать права, обязанности ответственность членов комиссии по обеспечению защиты персональных данных, в соответствии с внутренними локальными актами Оператора.

6.5.5 Политика в отношении обработки персональных данных.

Политика в отношении обработки персональных данных должна соответствовать рекомендациям Роскомнадзора по ее составлению. В соответствии с частью 2 ст. 18.1 Закона о персональных данных, Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к Политике в отношении обработки персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, Политику в отношении обработки персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети. Требования к содержанию Политики в отношении обработки персональных данных представлены в Приложении 1.

6.5.6 Положение об обработке и обеспечении безопасности персональных данных.

Положение об обработке и обеспечении безопасности персональных данных должно устанавливать принципы и условия обработки персональных данных, для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки, определять перечень информационных систем персональных данных, определять правовые, организационные и технические меры по обеспечению безопасности персональных данных Оператором. Положение об обработке и обеспечении безопасности персональных данных должно быть информативным и содержать ссылки на иные локальные акты Оператора. Требования к содержанию Положения об обработке и обеспечении безопасности персональных данных представлены в Приложении 2.

6.5.7 Регламент для работников Оператора по реагированию на запросы и обращения субъекта персональных данных, его законного представителя и органов государственной власти по вопросам защиты и обработки персональных данных.

Регламент для работников Оператора по реагированию на запросы и обращения субъекта персональных данных, его законного представителя и органов государственной власти по вопросам защиты и обработки персональных данных должен устанавливать обязанности Оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных, в соответствии со ст. 20 Закона о персональных данных, и обязанности Оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных в соответствии со ст. 21 Закона о персональных данных. Требования к содержанию Регламента по реагированию на запросы и обращения субъекта персональных данных, его законного представителя и органов государственной власти по вопросам защиты и обработки персональных данных представлены в Приложении 3.

6.5.8 Порядок распространения и передачи персональных данных третьим лицам.

Порядок распространения и передачи персональных данных третьим лицам должен быть разработан в соответствии со ст. 6, ст. 10.1 Закона о персональных данных и устанавливать порядок и условия передачи персональных данных третьим лицам и порядок распространения персональных данных, разрешенных субъектом персональных данных для распространения. Требования к содержанию Порядка распространения и передачи персональных данных третьим лицам представлены в Приложении 4.

6.5.9 Порядок хранения и уничтожения персональных данных.

Порядок хранения и уничтожения персональных данных должен устанавливать требования к хранению, порядку подготовки к уничтожению, способам уничтожения персональных данных и требования к подтверждению уничтожения персональных данных, обрабатываемых Оператором, в соответствии с требованиями Роскомнадзора [7]. Требования к содержанию Порядка хранения и уничтожения персональных данных представлены в Приложении 5.

6.5.10 Регламент внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации.

Регламент внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации должен определять периодичность и состав мероприятий по проведению внутреннего контроля соответствия обработки

персональных данных требованиям законодательства Российской Федерации. Требования к содержанию Регламента внутреннего контроля соответствия обработки персональных данных представлены в Приложении 6.

6.5.11 Порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» должен быть разработан в соответствии с требованиями Роскомнадзора [6]. Требования к содержанию Порядка оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» представлены в Приложении 7.

6.5.12 Регламент обработки персональных данных без использования средств автоматизации.

Регламент обработки персональных данных без использования средств автоматизации должен устанавливать особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации и меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации в соответствии с требованиями Правительства Российской Федерации [11]. Требования к содержанию Регламента обработки персональных данных без использования средств автоматизации представлены в Приложении 8.

6.6 Одним из условий обработки персональных данных, установленных ст. 6 Закона о персональных данных, является получение согласия на обработку персональных данных. Согласие на обработку персональных данных необходимо в случае отсутствия оснований обработки персональных данных, установленных пунктами 2-11 части 1 ст. 6 Закона о персональных данных.

Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой, позволяющей подтвердить факт его получения, форме, если иное не установлено законодательством Российской Федерации.

Письменная форма согласия на обработку персональных данных обязательна в случаях:

– обработки специальных персональных данных за исключением случаев, предусмотренных пунктами 2-10 части 2, части 2.1 ст. 10 Закона о персональных данных;

– обработки биометрических персональных данных за исключением случаев, предусмотренных частью 2 статьи 11 Закона о персональных данных;

– включения персональных данных в общедоступные источники в соответствии со ст. 8 Закона о персональных данных;

– осуществления трансграничной передачи, в случаях и при выполнении условий, установленных ст. 12 Закона о персональных данных.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных в соответствии со ст. 9 Закона о персональных данных 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 Законом о персональных данных;

– подпись субъекта персональных данных либо его законного представителя.

Форма согласия в письменной форме субъекта персональных данных на обработку его персональных данных, применяемая Операторами представлена в Приложении 9.

6.7 Распространение персональных данных, в соответствии со ст. 10.1 Закона о персональных данных, осуществляется с Согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, установлены Роскомнадзором [3], данное согласие должно содержать следующую информацию:

– фамилия, имя, отчество (при наличии) субъекта персональных данных;

– контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);

– сведения об Операторе - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);

– сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;

– цель (цели) обработки персональных данных;

– категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

- персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту персональных данных);

- специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, сведения о судимости);

- биометрические персональные данные;

– категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта персональных данных);

– условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников,

либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);

– срок действия согласия.

Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ Оператора в установлении субъектом персональных данных запретов и условий не допускается.

Форма согласия субъекта персональных данных на обработку его персональных данных, разрешенных субъектом персональных данных для распространения, применяемая Операторами, представлена в Приложении 10.

Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

1) непосредственно Оператору в письменной форме;

2) с использованием информационной системы Роскомнадзора.

6.8 Оператор обязан ознакомить своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, указанными в п. 6.5, п. 7.3 настоящего Стандарта и (или) провести обучение указанных работников.

7 Меры, направленные на обеспечение безопасности персональных данных

7.1 Оператор, в соответствии со ст.19 Закона о персональных данных, при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2 Обеспечение безопасности персональных данных достигается, в частности:

– 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 обеспечивают установленные Правительством Российской Федерации уровни защищенности персональных данных [4, 8, 10]

– применением прошедшей в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

– 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.

7.3 С целью исполнения требований ст. 19 Закона о персональных данных Оператором издаются следующие локальные акты:

7.3.1 Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее ИСПДн) должно осуществляться в соответствии с методическим документом ФСТЭК России [6]. По результатам оценки, проведенной в соответствии с данной Методикой, должны быть выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей. Результаты оценки угроз безопасности информации отражаются в модели угроз. Рекомендуемая структура модели угроз безопасности информации приведена в Приложении 11.

7.3.2 После определения угроз безопасности персональных данных при их обработке в ИСПДн Оператор должен составить Акт классификации информационной системы персональных данных, который предусматривает установление уровней защищенности персональных данных при их обработке в ИСПДн в зависимости от угроз безопасности этих данных, в соответствии с требованиями, установленными Правительством Российской Федерации [10]. Форма Акта классификации информационной системы персональных данных приведена в Приложении 12.

7.3.3 Регламент предоставления прав доступа к персональным данным, содержащимся в информационных системах персональных данных.

Регламент предоставления прав доступа к персональным данным, содержащимся в информационных системах персональных данных, должен устанавливать перечень лиц, имеющим доступ к ИСПДн, правила предоставления, изменения и прекращения прав доступа в ИСПДн. Требования к содержанию Регламента предоставления прав доступа к персональным данным, содержащимся в информационных системах персональных данных, представлены в Приложении 13.

7.3.4 Регламент обращения с машинными носителями персональных данных субъектов персональных данных.

Регламент обращения с машинными носителями персональных данных субъектов персональных данных должен определять порядок регистрации, учета, хранения и уничтожения машинных носителей персональных данных субъектов персональных данных. Требования к содержанию Регламента обращения с машинными носителями персональных данных субъектов персональных данных представлены в Приложении 14.

7.3.5 Инструкция по учету и эксплуатации средств криптографической защиты в информационных системах.

Инструкция по учету и эксплуатации средств криптографической защиты в информационных системах разрабатывается в соответствии с требованиями ФСБ России [8] и должен определять требования к учету и эксплуатации средств криптографической защиты, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Требования к содержанию Инструкции по учету и эксплуатации средств криптографической защиты в информационных системах представлены в Приложении 15.

7.3.6 Инструкция по антивирусной защите информации в информационных системах персональных данных.

Инструкция по антивирусной защите информации в информационных системах персональных данных должна определять требования к организации антивирусной защиты серверов и персональных компьютеров, входящих в состав информационных систем персональных данных, от воздействий компьютерных вирусов и другого вредоносного программного обеспечения, устанавливать порядок применения средств антивирусной защиты информации. Требования к содержанию Инструкции по антивирусной защите информации в информационных системах персональных данных представлены в Приложении 16.

7.3.7 Инструкция по организации парольной защиты.

Инструкция по организации парольной защиты должна определять требования к генерации, смене и прекращению действия паролей в информационных системах персональных данных, а также контроль за действиями пользователей при работе с паролями. Требования к содержанию Инструкции по организации парольной защиты представлены в Приложении 17.

7.3.8 Регламент резервного копирования и восстановления персональных данных субъектов персональных данных.

Регламент резервного копирования и восстановления персональных данных субъектов персональных данных должен определять правила и объемы резервного копирования, порядок восстановления персональных данных субъектов персональных данных субъектов персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним. Требования к содержанию Инструкции по организации парольной защиты представлены в Приложении 18.

7.3.9 Регламент по реагированию на инциденты информационной безопасности.

Регламент по реагированию на инциденты информационной безопасности должен определять порядок реагирования на инциденты информационной безопасности, порядок проведения внутреннего расследования инцидента информационной безопасности, порядок взаимодействия с Национальным координационным центром по компьютерным инцидентам, в соответствии с требованиями ФСБ России [5] и порядок уведомления уполномоченного органа по защите прав субъектов персональных данных о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных в соответствии с требованиями, установленными пунктом 3.1. части 3 ст. 31 Закона о персональных данных. Требования к содержанию Регламента по реагированию на инциденты информационной безопасности представлены в Приложении 19.

7.3.10 Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных должна проводиться Оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7.3.11 В зависимости от уровня защищенности персональных данных при их обработке в ИСПДн Оператор обязан принимать дополнительные меры по защите персональных данных, в том числе:

– назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе;

– организация доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

– организация автоматической регистрации в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

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

7.4 В соответствии с ч.2 ст. 18.1 Закона о персональных данных, Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей,

обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

8 Заключительные положения

8.1 Операторы обязаны соблюдать положения настоящего Стандарта и иные требования, установленные Законом о персональных данных, принятыми в соответствии с ним нормативными правовыми актами Российской федерации и нормативными правовыми актами федеральных органов исполнительной власти Российской Федерации.

8.2 В случае изменения законодательства Российской Федерации о персональных данных Операторы обязаны актуализировать локальные акты Оператора в соответствии с новыми требованиями.

Библиография

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

[2] Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»

[3] Приказ Роскомнадзора от 24.02.2021 г. № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»

[4] Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 г. № 28375)

[5] Приказ ФСБ России от 13.02.2023 г. № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» (Зарегистрировано в Минюсте России 20.02.2023 N 72404)

[6] Приказ Роскомнадзора от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (Зарегистрировано в Минюсте России 28.11.2022 N 71166)

[7] Приказ Роскомнадзора от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» (Зарегистрировано в Минюсте России 28.11.2022 N 71167)

[8] Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 N 33620)

[9] «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021 г.)

[10] 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»

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

Приложение 1

Политика в отношении обработки персональных данных
(содержание)

Приложение 2

Положение об обработке и обеспечении безопасности персональных данных
(содержание)

8.7. Обнаружение фактов несанкционированного доступа к персональным данным субъектов персональных данных и принятие мер по реагированию на несанкционированный доступ к персональным данным субъектов персональных

8.8. Восстановление персональных данных субъектов персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

8.9. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации

8.10. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

8.11. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных субъектов персональных данных

9. Заключительные положения

10. Ответственность

Приложение 3

Регламент по реагированию на запросы и обращения субъекта персональных данных, его законного представителя и органов государственной власти по вопросам защиты и обработки персональных данных (содержание)

Приложение 4

Порядок распространения и передачи персональных данных третьим лицам
(содержание)

Приложение 5

Порядок хранения и уничтожения персональных данных (содержание)

Приложение 6

Регламент внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации (содержание)

Приложение 7

Порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (содержание)

Приложение 8

Регламент обработки персональных данных без использования средств автоматизации (содержание)

Приложение 9

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных (форма)

СОГЛАСИЕ
на обработку персональных данных

Я, субъект персональных данных:

Фамилия Имя Отчество (при наличии)	
Адрес	
Наименование документа, удостоверяющего личность	
Номер документа, удостоверяющего личность	
Дата выдачи документа, удостоверяющего личность	
Орган, выдавший документ, удостоверяющего личность	

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», действуя по своей воле и в своих интересах, даю свое согласие на обработку моих персональных данных _____
_____,
(наименование Оператора, ИНН Оператора, юридический адрес Оператора)
далее Оператор, с целью _____.
(указать цель обработки персональных данных Оператором)
Перечень моих персональных данных, на обработку которых Оператору дается согласие: _____
_____.
(указать категории и перечень персональных данных)

Перечень действий с моими персональными данными, на совершение которых Оператору дается согласие: _____.
(указать перечень действий с персональными данными)

Я предоставляю Оператору право осуществлять обработку моих персональных данных_____.
(указать способ обработки персональных данных)
Я даю право Оператору передавать мои персональные данные _____
_____
(указать наименование третьего лица, ИНН, юр. адрес)

в соответствии с законодательством Российской Федерации, в рамках заключенного поручения, существенным условием которого является обеспечение безопасности персональных данных при их обработке и предотвращение разглашения моих персональных данных.

Настоящее согласие предоставляется мной с момента его подписания и действует до _____.
(указать срок согласия)

Настоящее согласие может быть отозвано мной при предоставлении Оператору заявления в форме, установленной Политикой в отношении обработки персональных данных Оператора, размещенной на сайте Оператора - _____.
(сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы)
либо в свободной форме, в соответствии с требованиями Законодательства Российской Федерации.

«_____»_____20_____г._____ /_____/

Дата *Личная подпись* *Расшифровка личной подписи*

Приложение 10

Согласие субъекта персональных данных на обработку его персональных данных, разрешенных субъектом персональных данных для распространения (форма)

СОГЛАСИЕ
на обработку персональных данных, разрешенных
субъектом персональных данных для распространения

Я, субъект персональных данных:

Фамилия *Имя* *Отчество (при наличии)*	
Контактная информация (номер телефона, адрес электронной почты или почтовый адрес)	

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» и Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 г. №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения», действуя по своей воле и в своих интересах, даю свое согласие на обработку моих персональных данных, разрешенных мной для распространения,

_____,
(наименование Оператора, ИНН Оператора, ОГРН Оператора, юридический адрес Оператора)

далее Оператор, с целью _____.
(указать цель обработки персональных данных Оператором)

Категории и перечень персональных данных, на распространение которых дается настоящее согласие:

Категория персональных данных	*Перечень персональных данных*	*Разрешаю к распространению (да/нет)*	*Разрешаю к распространению неограниченному кругу лиц (да/нет)*	*Условия и запреты, перечень условий и запретов*	*Дополнительные условия**

* Условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных.

В рамках достижения целей обработки моих персональных данных, разрешенных мной для распространения, даю право Оператору передавать мои персональные данные в _____.
(наименование третьего лица, получающего персональные данные, ИНН, ОГРН, юридический адрес)

Настоящее согласие дается для распространения моих персональных данных с помощью информационного ресурса_____.
(сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы)

Настоящее согласие предоставляется мной с момента его подписания и действует до _____.
(указать срок согласия)

Распространение моих персональных данных должно быть прекращено при предоставлении Оператору требования в форме, в форме, установленной Политикой в отношении обработки персональных данных Оператора - _____.
(сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы)

либо в свободной форме, в соответствии с требованиями Законодательства Российской Федерации.

«_____»_____20_____г._____ /_____/

Дата *Личная подпись* *Расшифровка личной подписи*

Приложение 11

Структура модели угроз безопасности информации (содержание)

1. Общие положения
2. Описание систем и сетей и их характеристика как объектов защиты
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
4. Возможные объекты воздействия угроз безопасности информации
5. Источники угроз безопасности информации
6. Способы реализации (возникновения) угроз безопасности информации
7. Актуальные угрозы безопасности информации

Приложение 12

Акт классификации информационной системы персональных данных (форма)

АКТ
ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАНЫХ
«_____»
(наименование информационной системы)
от « ____ » _____ 20____ г.

Комиссия в составе:

Председатель комиссии:
_____ _____
должность *Фамилия Имя Отчество*
Члены комиссии:
_____ _____
должность *Фамилия Имя Отчество*
_____ _____
должность *Фамилия Имя Отчество*

1. ОПРЕДЕЛИЛА основные характеристики информационной системы персональных данных
«_____»
(наименование информационной системы)

Основные характеристики представлены в Таблице №1

Таблица № 1 – Основные характеристики информационной системы персональных данных «НАКС»

№ п\п	Показатели	Значение показателя
1	Характеристики ИСПДн	
2	Типы актуальных угроз	

2. Исходя из основных характеристик информационной системы персональных данных «_____»,
(наименование информационной системы)
представленных в Таблице №1, в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства РФ от 01 ноября 2012 г. № 1119, комиссия **УСТАНОВИЛА** _____
(уровень защищенности)
уровень защищенности персональных данных при их обработке в информационной системе персональных данных «_____».
(наименование информационной системы)

Председатель комиссии:
_____ _____ /_____/
должность *подпись* *расшифровка*

Члены комиссии:
_____ _____ /_____/
должность *подпись* *расшифровка*
_____ _____ /_____/
должность *подпись* *расшифровка*

Приложение 13

Регламент предоставления прав доступа к персональным данным, содержащимся в информационных системах персональных данных (содержание)

Приложение 14

Регламент обращения с машинными носителями персональных данных субъектов персональных данных (содержание)

Приложение 15

Инструкция по учету и эксплуатации средств криптографической защиты в информационных системах (содержание)

Приложение 16

Инструкция по антивирусной защите информации в информационных системах персональных данных (содержание)

Приложение 17

Инструкция по организации парольной защиты (содержание)

Приложение 18

Регламент резервного копирования и восстановления персональных данных субъектов персональных данных (содержание)

Приложение 19

Регламент по реагированию на инциденты информационной безопасности
(содержание)