УТВЕРЖДАЮ
Врио директора ФГБУ ПОО «СГУОР»

Подписано цифровой подписью: Сулимов Алексей Алексеевич
DN: E=uc_fk@roskazna.ru, S=77 Москва, INNLE=7710568760, OGRN=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Федеральное казначейство, CN=Федеральное казначейство
Причина: Я утвердил этот документ
Дата: 9 Октябрь 2026 г. 15:40:46

_____ А.А.Сулимов

«_08_» _октября_ 2026

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва» (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Положения - установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн) Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум)

олимпийского резерва» (далее - ФГБУ ПОО «СГУОР») на протяжении всего жизненного цикла ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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, если иное не предусмотрено федеральным законом.

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

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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).

Персональные данные - любая информация, относящаяся прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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.

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

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее - СЗПДн).

3.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает ФГБУ ПОО «СГУОР» или лицо, осуществляющее обработку ПДн по поручению Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва» на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между ФГБУ ПОО «СГУОР» и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе ИС.

3.4. Выбор средств защиты информации для СЗПДн осуществляется ФГБУ ПОО «СГУОР» в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее - ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее - ФСТЭК России) во исполнение Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных».

3.5. Структура, состав и основные функции СЗПДн определяются, исходя из уровня защищенности ПДн при их обработке в ИСПДн.

3.6. СЗПДн создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на создание СЗПДн.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка необходимых средств защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

3.7. Этап 1. Проведение предпроектного обследования и разработка технического задания на создание СЗПДн.

3.8.1. Назначение ответственного за организацию обработки ПДн ФГБУ ПОО «СГУОР».

3.8.2. Создание комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва».

3.8.3. Определение целей обработки ПДн ФГБУ ПОО «СГУОР».

3.8.4. Определение перечня ИСПДн ФГБУ ПОО «СГУОР» и состава ПДн, обрабатываемых в ИСПДн.

3.8.5. Определение перечня обрабатываемых ФГБУ ПОО «СГУОР» ПДн.

3.8.6. Определение сроков обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.

3.8.7. Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

3.8.8. Определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах.

3.8.9. Назначение ответственного за обеспечение безопасности ПДн в ИСПДн (далее - Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн.

3.8.10. Назначение ответственного за эксплуатацию средств криптографической защиты информации, обеспечивающего функционирование и безопасность средств криптографической защиты информации, предназначенных для обеспечения безопасности ПДн. Утверждение перечня лиц, допущенных к работе со средствами криптографической защиты информации, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей средств криптографической защиты информации).

3.8.11. Определение перечня помещений, в которых размещены ИСПДн и материальные носители ПДн.

3.8.12. Определение конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

3.8.13. Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.

3.8.14. Формирование технических паспортов ИСПДн.

3.8.15. Разработка организационно-распорядительных документов (далее - ОРД), регламентирующих процесс обработки и защиты ПДн:

- Политика в отношении обработки персональных данных;

- Инструкции (ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИСПДн, пользователя ИСПДн, ответственного за эксплуатацию средств криптографической защиты информации);

- Раздел должностных инструкций сотрудников Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва» в части обеспечения

безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

3.8.16. Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн сотрудниками Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва».

3.8.17. Утверждение форм уведомлений субъектов ПДн и форм журналов, необходимых в целях обеспечения безопасности ПДн.

3.8.18. Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с требованиями 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» (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

3.8.19. Определение типа угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных». Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

3.8.20. Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- уровень защищенности ПДн при их обработке в ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- состав и содержание работ по этапам разработки и внедрения СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации.

3.8. Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

3.9.1. Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и (или) не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

3.9.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования

информационных ресурсов Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва». Применение технических мер должно быть регламентировано локальным актом ФГБУ ПОО «СГУОР».

3.9.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.9.4. На стадии проектирования и создания СЗПДн для ИСПДн ФГБУ ПОО «СГУОР»:

- разработка технического проекта СЗПДн;
- приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;
- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;
- реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;
- подготовка эксплуатационной документации на используемые средства защиты информации;
- корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

3.9. Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.10.1. На стадии ввода в ИСПДн (СЗПДн) осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);
- контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

3.10.2. Контроль за выполнением настоящих требований организуется и проводится ФГБУ ПОО «СГУОР» (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые ФГБУ ПОО «СГУОР» (уполномоченным лицом).

4. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Проведение внутренних проверок режима обработки и защиты ПДн в ФГБУ ПОО «СГУОР» предусматривает:

- определение лиц, ответственных за осуществление внутреннего контроля соответствия

обработки ПДн в ФГБУ ПОО «СГУОР» требованиям, установленным Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

- утверждение правил осуществления внутреннего контроля соответствия обработки ПДн требованиям, установленным Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;
- утверждение на планируемый период (год) плана проведения внутренних проверок режима обработки и защиты ПДн в ФГБУ ПОО «СГУОР».

4.2. При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

4.3. В соответствии с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн ФГБУ ПОО «СГУОР» необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

5. РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

5.1. Модернизация СЗПДн для функционирующих ИСПДн ФГБУ ПОО «СГУОР» должна осуществляться в случае:

- изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменения состава угроз безопасности ПДн в ИСПДн;
- изменения уровня защищенности ПДн при их обработке в ИСПДн;
- прочих случаях, по решению ФГБУ ПОО «СГУОР».

5.2. В целях определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год ответственным за организацию обработки ПДн должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем ФГБУ ПОО «СГУОР».

5.3. Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей ПДн;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- нарушение заданного уровня безопасности ПДн (конфиденциальность/целостность/доступность).

ЛИСТ ОЗНАКОМЛЕНИЯ

с Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Федерального государственного бюджетного образовательного учреждения профессиональная образовательная организация «Смоленское государственное училище (техникум) олимпийского резерва»

№п/п	ФИО	Должность	Дата	Подпись