

## **Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах ЧУ ДПО «СГТИ»**

### **1. Общие положения**

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах ЧУ ДПО «СГТИ» (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 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», [постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»](#), постановления Правительства Российской Федерации от 21 марта 2012 г. № 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 2013 г. № 21 «Об утверждении Составы 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 (далее – ИС) ЧУ ДПО «СГТИ» на протяжении всего жизненного цикла ИС.

### **2. Термины и определения**

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

**Информационная система** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

**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.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**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), обезличивание, 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 к прямо или косвенно определенному 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.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**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.

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

**Целостность информации** – способность средства вычислительной техники или 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 ИС 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 ИС обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

3.4. Выбор средств защиты информации для СЗПДн осуществляется оператором 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 «О персональных данных».

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

3.6. СЗПДн создается в три этапа:

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

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

Этап 3. Ввод ИС с СЗПДн в эксплуатацию.

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

3.7.1. Назначение ответственного за организацию обработки ПДн ЧУ ДПО «СГТИ».

3.7.2. Создание комиссии по определению уровня защищенности ПДн при их обработке в ИС ЧУ ДПО «СГТИ».

3.7.3. Определение целей обработки ПДн ЧУ ДПО «СГТИ».

3.7.4. Определение перечня ИС ЧУ ДПО «СГТИ» и состава ПДн, обрабатываемых в ИС.

3.7.5. Определение перечня обрабатываемых ЧУ ДПО «СГТИ» ПДн.

3.7.6. 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.

3.7.7. Определение перечня используемых в ИС (предлагаемых к использованию в ИС) общесистемных и прикладных программных средств.

3.7.8. Определение режимов обработки ПДн в ИС в целом и в отдельных компонентах.

3.7.9. Назначение ответственного за обеспечение безопасности ПДн в ИС (далее – Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИС. Для каждой ИС может быть назначен

отдельный Ответственный.

3.7.10. Назначение ответственного пользователя криптосредств, обеспечивающего функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждение перечня лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИС (пользователей криптосредств).

3.7.11. Определение перечня помещений, в которых размещены ИС и материальные носители ПДн.

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

3.7.13. Определение технических средств и систем, используемых в ИС, включая условия их расположения.

3.7.14. Формирование технических паспортов ИС.

3.7.15. 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 ИС, пользователя ИС, ответственного пользователя криптосредств);
- Раздел должностных инструкций сотрудников ЧУ ДПО «СГТИ» в части обеспечения безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

3.7.16. Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн сотрудником ЧУ ДПО «СГТИ».

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

3.7.18. Определение уровня защищенности ПДн при их обработке в ИС в соответствии с «Требованиями к защите ПДн при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИС).

3.7.19. 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 «О персональных данных». Определение угроз

безопасности ПДн в конкретных условиях функционирования ИС (разработка моделей угроз безопасности ПДн при их обработке в ИС).

3.7.20. 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 ИС.

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИС в техническом, программном, информационном и организационном аспектах;
- уровень защищенности ПДн при их обработке в ИС;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИС;
- 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.

3.8.1. 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 ИС и/или не нейтрализуют всех угроз безопасности ПДн для данной ИС.

3.8.2. 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 ЧУ ДПО «СГТИ». Применение технических мер должно быть регламентировано нормативным актом ЧУ ДПО «СГТИ».

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

3.8.4. На стадии проектирования и создания СЗПДн для ИС ЧУ ДПО «СГТИ» проводятся следующие мероприятия:

- 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 ИС к обрабатываемой в ИС информации;
- подготовка эксплуатационной документации на используемые средства защиты информации;
- корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

### 3.9. Этап 3. Ввод ИС с СЗПДн в промышленную эксплуатацию.

#### 3.9.1. На стадии ввода в ИС (СЗПДн) осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИС (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).

3.9.2. Контроль за выполнением настоящих требований организуется и проводится оператором (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 оператором (уполномоченным лицом).

## **4. Проведение работ по обеспечению безопасности персональных данных**

4.1. Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных (Приложение № 1). Внутренние проверки режима защиты ПДн ЧУ ДПО «СГТИ» проводятся в соответствии с Планом внутренних проверок режима защиты персональных данных (Приложение № 2).

4.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в

разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИС ЧУ ДПО «СГТИ» требованиям безопасности ПДн.

4.3. 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.

## **5. Решение вопросов обеспечения безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты**

5.1. Модернизация СЗПДн для функционирующих ИС ЧУ ДПО «СГТИ» должна осуществляться в случае:

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

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 ИС, состава угроз безопасности ПДн в ИС и уровня защищенности ПДн при их обработке в ИС, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем ЧУ ДПО «СГТИ».

5.3. Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должно 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).



Приложение № 1

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах ЧУ ДПО «СГТИ»

от «12»июля 2019 г.

**План мероприятий по защите персональных данных  
в ЧУ ДПО «СГТИ»**

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИС)	В случае создания ИС, а также приведения имеющихся ИС в соответствие с требованиями закона необходимо разграничить доступ сотрудников Оператора к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
6.	Ведение журналов учета	Постоянно	

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
	отчуждаемых электронных носителей персональных данных, средств защиты информации		
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИС)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Оператором устанавливаются сроки обработки ПДн, которые документально подтверждаются в нормативных документах Оператора. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных»
11.	Определение уровня защищенности ПДн при их обработке в ИС	При необходимости	Определение уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИС
13.	Аттестация (сертификация) СЗПДн или декларирование соответствия по требованиям безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
14.	Эксплуатация ИС и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по защите ПДн путем сегментирования ИС, отключения от сетей общего пользования, обеспечения обмена между ИС с помощью сменных носителей, создания автономных ИС на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИС, а также приведения имеющихся ИС в соответствии с требованиями закона

Приложение № 2  
к Положению по организации и проведению  
работ по обеспечению безопасности  
персональных данных при их обработке в  
информационных системах ЧУ ДПО «СГТИ»  
от «12»июля 2019 г.

**План внутренних проверок режима защиты персональных данных  
в ЧУ ДПО «СГТИ»**

<b>№</b>	<b>Мероприятие</b>	<b>Периодичность</b>	<b>Дата, подпись исполнителя</b>
1.	Контроль соблюдения правил обработки ПДн	Ежемесячно	
2.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
3.	Контроль соблюдения режима парольной защиты	Ежемесячно	
4.	Контроль выполнения антивирусной защиты	Еженедельно	
5.	Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС	Еженедельно	
7.	Контроль за обеспечением резервного копирования	Ежемесячно	
8.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
9.	Поддержание в актуальном состоянии нормативно-организационных документов	Ежеквартально	
10.	Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями (при наличии)	Ежемесячно	
11.	Тестирование всех функций СЗИ НСД с помощью специальных программных средств	Ежегодно	