

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 1 из 13
---	---	--

УТВЕРЖДАЮ
Директор
АНО ДПО «УКЦАСФ им. В.В. Никулина»

С.С. Левенчик
3 февраля 2025 г.



**Положение
по организации и проведению работ по обеспечению безопасности
персональных данных при их обработке
в информационных системах персональных данных**

Разработал
Заместитель директора по АР

К.О. Безрукова
30 января 2025 г.

Проверил
Первый заместитель директора

А.М. Колмыков
31 января 2025 г.

г. Новомосковск - 2025 г.

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 2 из 13
---	---	---

Содержание

1 Общие положения	3
2 Термины и определения	3
3 Порядок организации и проведения работ по обеспечению безопасности персональных данных	5
4 Проведения работ по обеспечению безопасности персональных данных	8
5 Порядок резервного копирования и восстановления информации в информационных системах	9
6 Решение вопросов обеспечения безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты	11
Приложение № 1	13

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 3 из 13
---	---	--

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 АНО ДПО «УКЦАСФ им. В.В. Никулина» (далее по тексту - Положение, Учебный центр) 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», 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 по тексту - ПДн) в информационных системах персональных данных (далее по тексту - ИСПДн) Учебного центра 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.

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,

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 4 из 13
---	---	--

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 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.

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 5 из 13
---	--	---

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 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 по тексту - 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 Учебный центр или лицо, осуществляющее обработку ПДн по поручению Учебного центра на основании заключаемого с этим лицом договора (далее по тексту - Уполномоченное лицо). Договор между Учебным центром 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 Учебным центром в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее по тексту - ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее по тексту - 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 ИСПДн.

3.6 СЗПДн создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн.

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.

3.7.1 Назначение ответственного за организацию обработки ПДн.

3.7.2 Создание комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн.

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 6 из 13
---	--	--

3.7.3 Определение целей обработки ПДн.

3.7.4 Определение перечня ИСПДн и состава ПДн, обрабатываемых в ИСПДн.

3.7.5 Определение перечня обрабатываемых 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 (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

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

3.7.9 Назначение Администратора безопасности информационной системы персональных данных (далее по тексту - Администратор ИБ) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн.

3.7.10 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).

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

3.7.12 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.

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

3.7.14 Формирование технических паспортов ИСПДн.

3.7.15 Разработка организационно-распорядительных документов (далее по тексту - ОРД), регламентирующих процесс обработки и защиты ПДн:

- Политика в отношении обработки персональных данных;
- Инструкции (ответственного за организацию обработки ПДн, Администратора ИБ, пользователя ИСПДн, ответственного за эксплуатацию средств криптографической защиты информации).

3.7.16 Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн работниками Учебного центра.

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

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 7 из 13
---	---	--

3.7.18 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).

3.7.19 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» от 27 июля 2006 г. № 152. Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

3.7.20 Формирование требований к разработке 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.

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 ИСПДн и (или) не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

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 Учебного центра. Применение технических мер должно быть регламентировано локальным актом Учебного центра.

3.8.3 Средства защиты информации, применяемые в ИСПДн, 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 ИСПДн проводятся следующие мероприятия:

- 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;

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 8 из 13
---	---	--

- 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.

3.9.1 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.

3.9.2 Контроль за выполнением настоящих требований организуется и проводится Учебным центром (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 Учебным центром (Уполномоченным лицом).

4 Проведение работ по обеспечению безопасности персональных данных

4.1 Проведение внутренних проверок режима обработки и защиты ПДн в Учебном центре предусматривает:

- определение лиц, ответственных за осуществление внутреннего контроля соответствия обработки ПДн требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

- утверждение правил осуществления внутреннего контроля соответствия обработки ПДн требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

- утверждение на планируемый период (год) приказом директора Учебного центра плана проведения внутренних проверок режима обработки и защиты ПДн.

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

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 9 из 13
---	---	--

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 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 Порядок резервного копирования и восстановления информации в информационных системах

5.1 Настоящий порядок определяет правила проведения резервного копирования данных, обрабатываемых в ИСПДн Учебного центра.

5.2 Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

5.3 Резервному копированию подлежит информация, обрабатываемая в ИСПДн Учебного центра.

5.4 Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

5.5 Перед выполнением процедур резервного копирования или восстановления информации и программного обеспечения средств защиты необходимо провести проверку:

- доступности резервного носителя, достаточности свободного места в хранилище для записи или восстановления данных;
- работоспособности средств резервного копирования и восстановления;
- готовности информационных ресурсов к осуществлению их резервного копирования или восстановления;
- завершения работы ПО и процессов, способных повлиять на процесс создания или восстановления копий.

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 10 из 13
---	---	---

5.6 Расписание проведения резервного копирования определяется Администратором ИБ.

5.7 Резервное копирование проводится Администратором ИБ и регистрируется в Журнале резервного копирования и восстановления информации (приложение № 1).

5.8 Перечень информационных ресурсов, подлежащих резервному копированию, время и дата создания копии, пометки об успешном/неуспешном завершении, а также, при необходимости, комментарии Администратором ИБ заносятся в Журнал резервного копирования и восстановления информации.

5.9 В случае выявления нарушений Администратором ИБ необходимо в кратчайшие сроки устранить неисправности в системе резервного копирования и восстановить работоспособность подсистем в штатный режим работы.

5.10 О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, Администратор ИБ сообщает директору Учебного центра немедленно.

5.11 Администратор ИБ должен контролировать проведение резервного копирования в целях выполнения требований по защите информации.

5.12 В случае обнаружения ошибки резервного копирования Администратор ИБ выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями Учебного центра, в Журнал резервного копирования и восстановления информации заносятся соответствующие отметки.

5.13 Хранение резервных копий данных осуществляется на сменных носителях информации (CD/DVD, внешние жесткие диски и т.п.), промаркированных Администратором ИБ в соответствии с расписанием резервного копирования. Маркировка должна содержать номер копии, дату ее создания, наименование ИСПДн.

5.14 Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

5.15 Срок хранения резервных копий определяется Администратором ИБ.

5.16 Очистка устаревших резервных копий из хранилища должна производиться Администратором ИБ регулярно по мере заполнения выделенной области памяти или по истечении предусмотренного срока хранения.

5.17 Удаление резервных копий для повторного использования носителя информации либо окончательное удаление производится Администратором ИБ.

5.18 Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях. Восстановление данных производится Администратором ИБ.

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 11 из 13
---	---	---

5.19 Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

5.20 В зависимости от характера и уровня повреждения информационных ресурсов, Администратор ИБ восстанавливает либо весь архив копии данных, либо отдельные потерянные части или технические средства из соответствующих хранилищ.

5.21 После завершения процесса восстановления Администратором ИБ проверяется целостность информационных ресурсов и корректная работа технических средств информационных систем, также заполняются соответствующие поля в Журнале резервного копирования и восстановления информации.

6 Решение вопросов обеспечения безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты

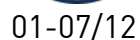
6.1 Модернизация СЗПДн для функционирующих ИСПДн Учебного центра должна осуществляться в случае:

- 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 Учебного центра.

6.2 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 директором Учебного центра.

6.3 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).



Положение по организации и проведению работ по
обеспечению безопасности персональных данных при их
обработке в информационных системах персональных данных
Автономной некоммерческой организации
дополнительного профессионального образования
«Учебно-консультационный центр
аварийно-спасательных формирований им. В.В. Никулина»

Редакция 2
Дата
03.02.2025
стр. 12 из 13

С настоящим положением ознакомлен(а):

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

(подпись)

(расшифровка подписи)

(дата)

 01-07/12	Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Автономной некоммерческой организации дополнительного профессионального образования «Учебно-консультационный центр аварийно-спасательных формирований им. В.В. Никулина»	Редакция 2 Дата 03.02.2025 стр. 13 из 13
---	---	--

Приложение № 1

Форма

Журнал резервного копирования/восстановления данных

№ п/п	Схема резервного копирования/ восстановления данных	Копируемые/ восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/ восстановления	ФИО	Подпись	Результат резервного копирования/во сстановления данных	Комментарий