Приложение №3
к Приказу № 9 от «19» декабря 2019 г.

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ПРО ООО ВДПО

История внесения изменений			
Порядковый номер	**Описание изменений**	**Автор**	**Дата введения**
1			

Пермь, 2019 г.

Раздел ГОСТ 27001	Контрольный номер документа	Номер версии	Дата утверждения	Срок пересмотра
А.5	ПО-03	1.0		1 год

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение об организации и обеспечении защиты персональных данных ПРО ООО ВДПО предназначено для организации и проведения мероприятий по обеспечению защиты персональных данных в соответствии с требованиями Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению защиты персональных данных в ПРО ООО ВДПО.

1.3. Положение является локальным нормативным правовым актом ПРО ООО ВДПО. Требования Положения обязательны для выполнения всеми работниками, которые допущены к обработке персональных данных.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

В Положении используются следующие основные термины и определения:

ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
КЗ	Контролируемая зона
ПДн	Персональные данные
СЗИ	Средство защиты информации
СЗПДн	Система (подсистема) защиты персональных данных
СКЗИ	Средство криптографической защиты информации

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Материальный носитель персональных данных (далее материальный носитель) – материальный объект, используемый для закрепления и хранения информации. В целях настоящего Положения под материальным носителем понимается бумажный документ, диск, дискета, флэш-карта и т.п.

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 – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств 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 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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

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

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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.

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.

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

Раздел ГОСТ 27001	Контрольный номер документа	Номер версии	Дата утверждения	Срок пересмотра
A.5	ПО-03	1.0		1 год

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или уничтожения ПДн.

3.2. Выполнение мероприятий по защите ПДн позволяет обеспечить защиту прав и свобод человека и гражданина при обработке его ПДн, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

3.3. Защита ПДн достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

3.4. Все работники, обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящим Положением под роспись.

4. НОРМАТИВНЫЕ ССЫЛКИ

4.1. Настоящее Положение разработано в соответствии с правовыми актами РФ:

- Федеральным Законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».
- Федеральным Законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановлением Правительства Российской Федерации от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн», утвержден приказом ФСТЭК России от 18.02.2013 г. № 21.
- Приказом ФСБ России от 10 июля 2014 № 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».

5. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ

5.1. ПДн, подлежащие защите, утверждаются приказом Председателя Совета ПРО ООО ВДПО в виде *«Перечня обрабатываемых персональных данных ПРО ООО ВДПО»*.

6. ОРГАНИЗАЦИОННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН

6.1. В состав организационной системы обеспечения безопасности ПДн ПРО ООО ВДПО входят:

- Председатель Совета ПРО ООО ВДПО;
- Лицо, ответственное за организацию обработки ПДн;
- Администратор безопасности ИСПДн;
- Руководители подразделений, работникам которых предоставлен доступ к ПДн;
- Работники, которым предоставлен доступ к ПДн (пользователи ИСПДн).

6.2. Общее руководство организацией работ по защите ПДн осуществляет Председатель Совета ПРО ООО ВДПО.

6.3. Лицо, ответственное за организацию обработки ПДн:

- осуществляет внутренний контроль за соблюдением ПРО ООО ВДПО и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- доводит до сведения работников ПРО ООО ВДПО положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- организации приема и обработки обращений и запросов субъектов ПДн или их представителей и осуществления контроля за приемом и обработкой таких обращений и запросов.

6.4. Администратор безопасности ИСПДн осуществляет:

- администрирование, контроль работоспособности и анализ результатов работы средств защиты информации информационных систем персональных данных;
- контроль деятельности подразделений ПРО ООО ВДПО по выполнению ими установленных требований обеспечения безопасности ПДн в информационных системах персональных данных;
- обнаружение и расследование попыток несанкционированного доступа, информирование непосредственного руководства о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным системам персональных данных;
- проведение периодических проверок защищенности информационных систем персональных данных;
- подготовка предложений по совершенствованию и реализации мероприятий по обеспечению безопасности персональных данных в информационных системах персональных данных.

6.5. Доступ работников к ИСПДн предоставляется в установленном в ПРО ООО ВДПО порядке. Руководители подразделений организуют соблюдение требований безопасности ПДн и выполнение мероприятий по защите в подразделениях ПРО ООО ВДПО. Готовят предложения в

перечень ПДн, перечень работников, допущенных к обработке ПДн, и ИСПДн ПРО ООО ВДПО, необходимые для выполнения функций подразделения.

6.6. Работники, которым предоставлен доступ к ПДн в рамках обработки без использования средств автоматизации, непосредственно реализуют организационные меры по обеспечению сохранности носителей ПДн и выполнения процедур по соблюдению требований законодательства.

6.7. Пользователи ИСПДн непосредственно реализуют требования безопасности информации, принятые для ИСПДн, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил безопасности информации.

6.8. При определении полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, рекомендуется соблюдать принцип разделения ролей.

7. ЗАЩИТА ПДН ПРИ ОБРАБОТКЕ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

7.1. Требования к обеспечению безопасности ПДн при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7.2. Порядок обработки ПДн без использования средств автоматизации устанавливается Положением об обработке персональных данных в ПРО ООО ВДПО.

7.3. Данный вид обработки ПДн (а также состав ПДн и перечень лиц, допущенных к обработке) указывается в «*Перечне обрабатываемых персональных данных*» и «*Перечне подразделений и работников, допущенных к обработке персональных данных ПРО ООО ВДПО*».

7.4. Защита ПДн, обрабатываемых без использования средств автоматизации, обеспечивается выполнением следующих мероприятий:

- определением мест хранения ПДн (материальных носителей) и перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;
- обеспечением раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях в соответствии с Положением об обработке персональных данных ПРО ООО ВДПО;
- соблюдением условий, обеспечивающих сохранность ПДн и исключающих несанкционированный доступ к ним;
- установлением порядка прекращения обработки и уничтожения или обезличивания ПДн.

8. ЗАЩИТА ПДН ПРИ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя:

- моделирование угроз безопасности ПДн при их обработке в ИСПДн, формирование на их основе частной модели угроз и нарушителя;
- определение требуемого уровня защищенности ПДн при их обработке в ИСПДн;
- разработку на основе частной модели угроз и нарушителя с учетом требуемого уровня защищенности ПДн системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- описание системы защиты ПДн;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей ПДн;
- учет лиц, допущенных к обработке ПДн в ИСПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн, включая контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения машинных носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- принятие мер в случае обнаружения фактов несанкционированного доступа к ПДн;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

8.2. Методы и способы защиты персональных данных включают в себя:

- реализацию разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрацию действий пользователей, контроль несанкционированного доступа и действий пользователей, посторонних лиц;
- учет и хранение съемных носителей информации, их обращение, исключающее хищение, подмену и уничтожение;
- управление изменениями конфигурации ИСПДн и СЗПДн;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку ПДн, только в пределах охраняемой территории (рабочие станции, серверы, коммутационное оборудование, сетевые принтеры);
- организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок с использованием средств антивирусной защиты.

8.3. Моделирование угроз безопасности и выбор уровня защищенности

8.3.1. Частная модель нарушителя и угроз безопасности ПДн при их обработке в ИСПДн разрабатывается с использованием методических документов ФСТЭК России и (или) ФСБ России. Результаты определения типа актуальных угроз безопасности ПДн при их обработке в ИСПДн ПРО ООО ВДПО и их состава утверждаются Приказом Председателя Совета ПРО ООО ВДПО.

8.3.2. Частная модель нарушителя и угроз безопасности ПДн при их обработке в ИСПДн должна включать:

- исходные данные для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;
- совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;
- тип и перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн;
- описание потенциального нарушителя;
- требуемый класс СКЗИ, позволяющих обеспечить безопасность ПДн.

8.3.3. Выявление угроз безопасности ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов по информационным технологиям, персонала ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

8.3.4. Частная модель нарушителя и угроз безопасности ПДн должна периодически пересматриваться в соответствии с Планом внутренних проверок состояния защиты ПДн.

8.3.5. Уточнение и пересмотр угроз безопасности ПДн при их обработке в ИСПДн осуществляется в случае изменения:

- технологических процессов обработки ПДн;
- состава средств защиты информации в ИСПДн;
- характеристик ИСПДн, влияющих на уровень защищенности (наличие подключений к сетям общего пользования, тип ИСПДн и т.д., кол-во субъектов, чьи ПДн обрабатываются в ИСПДн).

8.3.6. На основе определенного типа угроз безопасности ПДн и характеристик ИСПДн в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется уровень защищенности ПДн при их обработке в ИСПДн.

8.4. Порядок разработки, ввода в действие и эксплуатации СЗПДн

8.4.1. Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью СЗПДн, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

8.4.2. При формировании требований к СЗПДн должны быть учтены:

- положения законодательства РФ и руководящих документов ФСТЭК России и ФСБ России, актуальных на момент разработки требований;
- результаты разработки частной модели нарушителя и угроз, в частности, выполнение требований должно обеспечивать нейтрализацию предполагаемых актуальных угроз безопасности ПДн;
- необходимость обеспечения определенного уровня защищенности ПДн при их обработке в ИСПДн.

8.4.3. Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случаях, если:

- изменился состав обрабатываемых ПДн;
- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн) или технологический процесс обработки ПДн, вследствие которого произошли изменения в структуре ИСПДн;
- изменился состав угроз безопасности ПДн в ИСПДн.

8.4.4. В случае изменения характеристик ИСПДн, влияющих на уровень защищенности ИСПДн, проводится пересмотр уровня защищенности ПДн при их обработке в ИСПДн и повторная оценка эффективности принимаемых мер по обеспечению безопасности ПДн.

9. ФИЗИЧЕСКАЯ ЗАЩИТА ПОМЕЩЕНИЙ И ТЕХНИЧЕСКИХ СРЕДСТВ

9.1. Размещение ИСПДн и охрана помещений, в которых ведется работа с ПДн должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9.2. Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию контролируемой зоны (КЗ) ПРО ООО ВДПО.

9.3. Границами КЗ могут являться:

- периметр охраняемой территории ПРО ООО ВДПО;
- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;
- стены помещений ПРО ООО ВДПО.

9.4. В состав КЗ должны входить:

- помещения, в которых размещены рабочие станции, серверы, сетевое оборудование, входящие в состав ИСПДн;
- помещения, в которых проходят кабельные линии связи ИСПДн;
- помещения, в которых хранятся бумажные носители ПДн (архивы, помещения работников ПРО ООО ВДПО).

9.5. Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

9.6. Доступ посторонних лиц (посетителей, работников обслуживающих организаций) в контролируемую зону в рабочее время осуществляется только в сопровождении работников ПРО ООО ВДПО.

9.7. Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

9.8. Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны быть только у лиц, имеющих право доступа в них.

9.9. Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ оснащаются входными дверьми с

замками. Работники обеспечивают постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или (при наличии оборудования соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений) постановку помещения на охранную сигнализацию.

9.10. В нерабочее время доступ в КЗ должен быть исключен следующими мерами:

- заключением договора с арендодателем (охранным предприятием), обязательными условиями которого являются следующие обязанности арендодателя (охранного предприятия):
  - организация и обеспечение контроля доступа в арендуемые помещения работников и посетителей в рабочее время.
  - организация и обеспечение охраны помещений в нерабочее время, а также в выходные и праздничные дни.
  - не допускать проникновения и пребывания посторонних лиц в помещениях в нерабочее время, а также в выходные и праздничные дни. При необходимости использования помещений в указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом.
  - внос и вынос материальных ценностей в помещения и из помещений осуществляется только в присутствии ответственного лица.
- в случае отсутствия возможности заключения договора с арендодателем (охранным предприятием) для реализации мер по охране контролируемой зоны в нерабочее время необходимо выполнять следующие требования:
  - на всех остекленных проемах первого и последнего этажа должны быть установлены металлические решетки или ставни с запорами;
  - двери в помещения контролируемой зоны должны быть металлическими, с надежными замками;
  - хранение ключей осуществляется назначенным приказом ответственным работником с выдачей под роспись работникам в случае необходимости.

10. КОНТРОЛЬ ЗА ПРИНИМАЕМЫМИ МЕРАМИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Целью контроля состояния защиты является своевременное выявление и предотвращение утечки информации.

10.2. Контроль состояния защиты ПДн должен осуществляться в соответствии с утвержденным Планом внутренних проверок состояния защиты ПДн.

10.3. Проведение контроля состояния защиты включает в себя мероприятия по оценке:

- соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

10.4. Проверка проводится дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

11. ПРИНЯТИЕ МЕР В СЛУЧАЕ ОБНАРУЖЕНИЯ ФАКТОВ НАРУШЕНИЯ ТРЕБОВАНИЙ (НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ), РАЗБИРАТЕЛЬСТВО И СОСТАВЛЕНИЕ ЗАКЛЮЧЕНИЙ ПО ФАКТАМ НАРУШЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ

11.1. Лицо, обнаружившее факт нарушения требований безопасности информации, незамедлительно уведомляет *Администратора безопасности ИСПДн*.

11.2. В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

- немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;
- организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

11.3. Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

11.4. Порядок проведения расследования причин и условий возникновения нарушения требований определяется отдельными локальными нормативными актами ПРО ООО ВДПО.

11.5. В случае, если вследствие несанкционированного доступа ПДн были модифицированы или уничтожены, осуществляется восстановление ПДн из резервной копии.

12. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

12.1. При вступлении в должность нового работника непосредственный руководитель подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн (*«Положением об обработке персональных данных»*). Обучение навыкам выполнения процедур, необходимых для работы в ИСПДн ПРО ООО ВДПО и выполнения требований по защите ПДн и ознакомление под роспись с «Инструкцией работникам по обеспечению безопасности при работе с персональными данными» осуществляется в установленном порядке.

12.2. Работники должны соблюдать установленные организационно-распорядительными документами требования по режиму обработки ПДн, учету, хранению, передаче носителей информации и обеспечению безопасности ПДн.

12.3. Работники должны быть проинформированы об ответственности за нарушение требований по обеспечению безопасности ПДн в момент заключения трудового договора с ПРО ООО ВДПО.

13. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

13.1. Настоящее Положение пересматривается не реже одного раза в три года и в случае изменения законодательства в области защиты ПДн.

13.2. Все изменения отражаются в Листе изменений.

13.3. Измененное Положение утверждается в установленном порядке.

Лист изменений

№ версии	Приказ/ дата	Название документа	Лист / Статья	Содержание изменения	Характер изменения	Изменения произвел

Лист ознакомления

№	Дата	Должность/подразделение	Ф.И.О	Подпись

Приложение 1

к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

ПЕРЕЧЕНЬ

должностных лиц, допущенных к обработке персональных данных для выполнения ими служебных (трудовых) обязанностей

№ п/п	Наименование подразделения	Должность	Категория субъектов персональных данных	Перечень персональных данных
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

Приложение 2
к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

УТВЕРЖДАЮ

Председатель Совета ПРО ООО ВДПО

_____ С.Н. Ужегов

м.п.

«19» декабря 2019 г.

АКТ №___
классификации информационной системы персональных данных
ЦОК ЧС ПРО ООО ВДПО

В соответствии с п. 6 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17.11.2007 № 781 и приказом ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных», комиссия, назначенная приказом Председателя Совета ПРО ООО ВДПО от «___»_____ 2019 г.№ ___ «О приведении ПРО ООО ВДПО в соответствие с требованиями законодательства Российской Федерации в области персональных данных», в составе:

Председатель комиссии: _____
(должность назначенного лица, фамилия и инициалы)

Члены комиссии: _____
_____
_____
_____
(должность назначенного лица, фамилия и инициалы)

рассмотрев Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных ЦОК ЧС ПРО ООО ВДПО (номер Модели угроз), а также учитывая следующие исходные данные на информационную систему персональных данных:

Категория обрабатываемых в информационной системе персональных данных, ($X_{пд}$)

Объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в

информационной системе),
($X_{НПД}$)

Заданные характеристики безопасности персональных данных, обрабатываемых в информационной системе персональных данных

Структура информационной системы персональных данных

Наличие подключений информационной системы персональных данных к сетям связи общего пользования и (или) сетям международного информационного обмена

Режим обработки персональных данных

Режим разграничения прав доступа пользователей информационной системы персональных данных

Местонахождение технических средств информационной системы персональных данных

РЕШИЛ:

1. В соответствии с п. 8 приказа ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» отнести информационную систему персональных данных ЦОК ЧС ПРО ООО ВДПО к специальной информационной системе персональных данных.

2. В соответствии с п. 16 приказа ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» присвоить специальной информационной системе персональных данных «Полное название ИСПДн» ПРО ООО ВДПО класс ___ при условии выполнения организационно-технических требований, изложенных в модели угроз (номер Модели угроз).

Председатель комиссии _____ (личная подпись) _____ (фамилия и инициалы)

Члены комиссии _____ (личная подпись) _____ (фамилия и инициалы)

_____ (личная подпись) _____ (фамилия и инициалы)

Приложение 3
к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

УТВЕРЖДАЮ

Председатель Совета ПРО ООО ВДПО

_____ С.Н. Ужегов

м.п.

«19» декабря 2019 г.

ЗАКЛЮЧЕНИЕ №___
о возможности эксплуатации средства защиты информации

_____
(наименование)

В соответствии с п. 12 Постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» комиссией, назначенной приказом Председателя Совета ПРО ООО ВДПО от «___» _____ 2019 г.№ ___ «О приведении ПРО ООО ВДПО в соответствие с требованиями законодательства Российской Федерации в области персональных данных», в составе:

Председатель комиссии: _____
(должность назначенного лица, фамилия и инициалы)

Члены комиссии: _____
_____
_____
(должность назначенного лица, фамилия и инициалы)

проведена установка, настройка и проверка готовности

_____
(наименование средства защиты информации)

Прикладное программное обеспечение

_____
(наименование программного обеспечения, место установки)

Информация о настройках средств защиты информации

_____
(наименование документа, по которому проводилась настройка средства защиты информации)

Выполнение требований по сертификации средства защиты информации

_____
(реквизиты сертификата на средство защиты информации/не проводилась)

Вывод о возможности эксплуатации: установленное средство защиты информации

_____
(наименование)

готово к использованию в информационной системе персональных данных ЦОК ЧС ПРО ООО ВДПО в качестве _____
(назначение средства защиты информации)

Председатель комиссии _____ _____
(личная подпись) (фамилия и инициалы)

Члены комиссии _____ _____
(личная подпись) (фамилия и инициалы)

Приложение 4

к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

УТВЕРЖДАЮ

Председатель Совета ПРО ООО ВДПО

_____ С.Н. Ужегов

м.п.

«19» декабря 2019 г.

АКТ №____
ввода в эксплуатацию средства защиты информации

Комиссия, назначенная приказом Председателя Совета ПРО ООО ВДПО от «___»_____ 2019 г.№ ___ «О приведении ПРО ООО ВДПО в соответствие с требованиями законодательства Российской Федерации в области персональных данных», в составе:

Председатель комиссии: _____
(должность назначенного лица, фамилия и инициалы)

Члены комиссии: _____
_____
_____
(должность назначенного лица, фамилия и инициалы)

на основании Заключения от «___»_____ 2019 г.№ ___ о возможности эксплуатации средства защиты информации составила настоящий акт о том, что

_____
(наименование средства защиты информации)

информационной системы персональных данных ЦОК ЧС ПРО ООО ВДПО, установленное в соответствии с эксплуатационной и технической документацией к нему, вводится в эксплуатацию.

Председатель комиссии _____ _____
(личная подпись) (фамилия и инициалы)

Члены комиссии _____ _____
(личная подпись) (фамилия и инициалы)

_____ _____
(личная подпись) (фамилия и инициалы)

Приложение 5

к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

УТВЕРЖДАЮ

Председатель Совета ПРО ООО ВДПО

_____ С.Н. Ужегов

м.п.

«____» ноября 2019 г.

ЗАКЛЮЧЕНИЕ №____
по факту несоблюдения требований безопасности персональных данных (условий хранения носителей, использования средств защиты информации)

Комиссия, назначенная приказом Председателя Совета ПРО ООО ВДПО от «___»_____ 2019 г.№ ___ «О приведении ПРО ООО ВДПО в соответствие с требованиями законодательства Российской Федерации в области персональных данных», в составе:

Председатель комиссии: _____
(должность назначенного лица, фамилия и инициалы)

Члены комиссии: _____
_____
_____
_____
(должность назначенного лица, фамилия и инициалы)

составила настоящее заключение по факту несоблюдения условий хранения носителей персональных данных (использования средств защиты информации) работником

_____
(наименование структурного подразделения, фамилия, имя и отчество)

Комиссией установлено, что

_____
(описание инцидента нарушения безопасности персональных данных)

Вывод: комиссия считает, что вышеперечисленные нарушения стали следствием

_____
(причины нарушения, предложения о привлечении виновного к ответственности)

Председатель комиссии _____ _____
(личная подпись) (фамилия и инициалы)

Члены комиссии _____ _____
(личная подпись) (фамилия и инициалы)

(личная подпись)

(фамилия и инициалы)

Приложение 6

к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

СПИСОК

помещений, в которых обрабатываются персональные данные

№ п/п	Наименование, номер помещения	Должностные лица, имеющие право самостоятельного доступа в помещение
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		

Приложение 7

к Положению об обеспечении безопасности персональных данных при их обработке в ИСПДн ПРО ООО ВДПО

ЖУРНАЛ УЧЁТА ПОСЕТИТЕЛЕЙ

№ п/п	Дата	Ф.И.О. посетителя	Наименование и номер документа, удостоверяющего личность	Должность, ФИО лица, к которому следует посетитель	Цель посещения	Время		Ф.И.О., подпись сотрудника контроля
						входа	выхода	
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								